PROCEDIMIENTOS DE SEGURIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA GOBERNACIÓN DEL CAUCA

YOLI ALEXANDRA CAMPO MARTÍNEZ

Trabajo de grado en Modalidad de Practica Profesional en Ingeniera Electrónica y Telecomunicaciones

Director
Mg. Siler Amador Donado

Asesor
Daniel Fernando Valencia Viteri

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Tecnologías de la Información-GTI
Línea de investigación Seguridad de la Información

Popayán, 2019

YOLI ALEXANDRA CAMPO MARTÍNEZ

PROCEDIMIENTOS DE SEGURIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA GOBERNACIÓN DEL CAUCA

Trabajo de grado presentado a la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca para la obtención del Título de Ingeniera en Electrónica y Telecomunicaciones

Director
Mg. Siler Amador Donado

Asesor
Daniel Fernando Valencia Viteri

Popayán, 2019

Agradecimientos

Agradecer se convierte en el gesto más valioso cuando consigues algo por lo que luchaste tanto.

Decir gracias a Dios y a todos aquellos que fueron participes de este gran trabajo, se queda corto con el sentimiento de saber que el esfuerzo siempre será recompensado.

Es por eso, que doy gracias a mi familia, especialmente a mis padres y hermana, quienes, con su apoyo y aliento constante, me motivaron cada día a ser mejor, crecer de manera integral y sobre todo amar cada labor que desarrollo.

A mi director de trabajo de grado, que siempre se lleva todo el cariño con el carisma que contagia a los estudiantes; y al ingeniero Daniel Valencia por darme la oportunidad de desempeñarme en la Gobernación del dpto. del Cauca, contribuir con la entidad y crecer en el ámbito profesional.

Hoy soy consciente de la tarea que desempeñare, ser ingeniera es un trabajo de todos los días, que requiere de un crecimiento constante en todos los campos tanto personal como laboral. Ahora espero poder contribuir a la sociedad, ya que como bien dicen, "quien vive para servir, sirve para vivir".

Yoli Alexandra Campo Martínez

Popayán, febrero 2019

"LA GRATITUD ES UNA CUALIDAD SIMILAR A LA ELECTRICIDAD: DEBE PRODUCIRSE, DESCARGARSE Y AGOTARSE PARA PODER EXISTIR".

William Faulkner

RESUMEN

Procedimientos de Seguridad del Modelo de Seguridad y Privacidad de la Información para la Gobernación del Cauca

Gobernación del Departamento del Cauca-Universidad del Cauca

Actualmente las entidades del estado se encuentran en un proceso de aplicación de distintos Modelos de Gestión que permiten digitalizar, y controlar el funcionamiento de las mismas. Por tal razón, la Gobernación del Departamento del Cauca en consonancia con el Ministerio de Tecnologías de la Información y las comunicaciones, se encuentra en proceso de implementación del Modelo Integrado de Planeación y Gestión (MIPG). MIPG se soporta en el cumplimiento de las distintas políticas que el MinTIC estableció para soportar el mismo. En ese sentido la política de Gobierno Digital establece dos componentes: TIC para Estado y TIC para sociedad. Estos componentes a su vez contienen 3 factores transversales: Arquitectura TI, Servicios Ciudadanos Digitales y Seguridad de la Información. Este último componente, es el objetivo del presente trabajo de grado; eso, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información a través de la generación de los procedimientos de Seguridad de la Información.

Por lo anterior el Modelo de Seguridad de la Información brinda la Guía N° 3 Procedimientos de Seguridad y Privacidad de la Información, con los lineamientos necesarios para el establecimiento de los mismos. En ese sentido los procedimientos de seguridad de la Información son establecidos con base en la herramienta de Evaluación del MSPI donde se evidencian los indicadores que ilustran la madurez y avance del modelo.

De esta forma, se generan los procedimientos de seguridad de la información para la Gobernación del Departamento del Cauca, con los debidos controles establecidos por las normas, en cumplimiento de los requisitos de tecnologías de la información.

ABSTRACT

Security Procedures of Security and Information Privacity and Security Model for Governation of Cauca

Governation Department of Cauca-University of Cauca

Currently, entities are in process of applying different Management Models that allow digitizing, and control their operation. For this reason, the Government of the Department of Cauca and the Ministry of Information Technology and communications, is in the process of implementing the Integrated Planning and Management Model (MIPG). MIPG is supported in complying with the different policies that the MinTIC established to support it. In this sense, the Digital Government policy establishes two components: TIC for the State and TIC for society. These components, in turn, contain three transversal factors: TI Architecture, Digital Citizen Services and Information Security. This last component, is the objective of the present work of degree; that, in order to guarantee the confidentiality, integrity and availability of information through the generation of Information Security procedures.

Therefore, the Information Security Model provides Guide No. 3 Security Procedures and Information Privacy, with the necessary guidelines for establishing them. In this sense, information security procedures are established based on the MSPI Evaluation tool, where the indicators that illustrate the maturity and progress of the model are evidenced.

In this way, information security procedures are generated for the Government of the Department of Cauca, with the appropriate controls established by the regulations, in compliance with the requirements of information technology.

CONTENIDO

Índice de Figuras

Índice de Tablas

Glosario de Términos

IEC *International Electrotechnical Commission*, Comisión Electrotécnica Internacional.

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

NTC Norma Técnica Colombiana.

AENOR Asociación Española de Normalización y Certificación.

ITIL Information Technology Infrastructure Library

Lista de Acrónimos

GD Gobierno Digital.

MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones.

MPSI Modelo de Privacidad y Seguridad de la Información.

PM *Project Management*, Gestión de Proyectos.

PSI Procedimientos de Seguridad de la Información.

Glosario

Actividad. El menor objeto de trabajo identificado en un proyecto. [1]

Activos 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. [2]

Acuerdo con proveedor. Un acuerdo de nivel de servicio (service level agreement, SLA) es un contrato entre un proveedor de servicios y sus clientes internos o externos que documenta qué servicios proporcionará el proveedor y define los estándares de servicio que el proveedor está obligado a cumplir [4].

Auditoria. Proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría. [1]

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

Capacitación. La capacitación es un proceso a través del cual se adquieren, actualizan y desarrollan conocimientos, habilidades y actitudes para el mejor desempeño de una función laboral o conjunto de ellas [5].

Cifrado de datos. El cifrado es el elemento fundamental de la seguridad de datos y es la forma más simple e importante de impedir que alguien robe o lea la información de un sistema informático con fines malintencionados [6]. Es el proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes. El cifrado de activos de información en redes se utiliza para proteger los datos que pasan por las complejas topologías de red que se utilizan en la actualidad al interior de las entidades. La protección de datos en movimiento, en tiempo real, requiere una gestión del cifrado de alto rendimiento y robustos algoritmos, a fin de evitar problemas de latencia o de sincronización.

Clasificación. 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 [7].

Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados [8]**.**

Contrato. Acuerdo vinculante [1].

Control. Medio para mantener el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras, organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal [9].

Control de acceso. Abarca únicamente la aprobación de acceso, por lo que el sistema adopta la decisión de conceder o rechazar una solicitud de acceso de un sujeto ya autenticado, sobre la base a lo que el sujeto está autorizado a acceder [10].

Criptografía. Es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad, y provee las herramientas idóneas para ello [11].

Custodio del activo de información. 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 [7].

Dato Abierto. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6) [2].

Dato personal. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3) [2].

Dato público. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3) [2].

Dato sensible. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos

humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3) [2].

Disponibilidad. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada [8]**.**

Eficiencia. Relación entre el resultado alcanzado y los recursos utilizados [1].

Encriptación. La encriptación de datos o cifrado de archivos es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes. Así, cualquier persona que no disponga de las claves correctas no podrá acceder a la información que contiene [12].

Gestión. Actividades coordinadas para dirigir y controlar una organización [1].

Grupo Ocupacional. Agrupación de personal describe cargos comprendidos en la misma rama o actividad de trabajo [13].

Identificación. La identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema [4].

Incidente en seguridad de la información. Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la entidad [8].

Información pública clasificada. Aquella información que estando en poder o custodia, de un sujeto, 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 de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18, de la ley 1712 de 2014 [14]; y su acceso pudiere causar un daño a los siguientes derechos:

- ✓ El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.
- ✓ El derecho de toda persona a la vida, la salud o la seguridad.
- ✓ Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la ley 1474 de 2011, teniendo una duración ilimitada y no deberán aplicarse a cuando la persona natural o jurídica ha

consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo régimen de publicidad aplicable (artículo 6, literal c y 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 de manera motivada y por escrito, por año a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014. Se podrá negar el acceso a esta información cuando concurra una de las siguientes circunstancias y siempre que dicho acceso estuviere expresamente prohibió por una norma legal o constitucional [14].

- ✓ La defensa y seguridad nacional
- ✓ La seguridad pública
- ✓ Las relaciones internacionales
- ✓ La prevención, investigación y persecución de los delitos y las faltas disciplinarias. mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.
- ✓ El debido proceso y la igualdad de partes en los procesos judiciales
- ✓ La administración efectiva de la justicia
- ✓ La estabilidad macroeconómica y financiera del país
- ✓ La salud pública
- ✓ Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos (artículo 6, literal d y artículo 19 de la ley 1712 de 2014).

Integridad. Propiedad de salvaguardar la exactitud y estado completo de los activos [8].

Llaves criptográficas. Es el proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes. El cifrado de activos de información en redes se utiliza para proteger los datos que pasan por las complejas topologías de red que se utilizan en la actualidad al interior de las entidades. La protección de datos en movimiento, en tiempo real, requiere una gestión del cifrado de alto rendimiento y robustos algoritmos, a fin de evitar problemas de latencia o de sincronización [15].

Malware. Es la abreviatura de Malicious Software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de Malwares podemos encontrar términos como, por ejemplo, Virus, Troyanos, Gusanos (Worm), keyloggers, Botnets, entre otros [16].

Organización. Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos [1].

Perfiles de usuario. Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él [17].

Privacidad. En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente [2].

Política. Intenciones y dirección de una organización, como las expresa formalmente su alta dirección [1].

Procedimiento. Forma especificada de llevar a cabo una actividad o un proceso [1].

Proceso. Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto [1].

Registro. Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas [1].

Riesgo. Efecto de la incertidumbre [1].

Seguridad de la información. Preservación de la confidencialidad, integridad, y disponibilidad de la información. [8].

Sensibilización. Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular [18].

Servicio. Salida de una organización con al menos una actividad, necesariamente llevada a cabo entre la organización y el cliente [1].

Sistema. Conjunto de elementos interrelacionados o que interactúan [1].

Sistemas de información. Un sistema de información es un conjunto de datos que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización [1].

Spam. Los términos correo basura y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido, habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor [19].

Registro. Un log ("registro", en español) es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado [8].

Registro de auditoria. Archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Entidad. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas [8].

Requisito. Necesidad o expectativa establecida, generalmente implícita u obligatoria [1].

Trazabilidad. Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad [8].

Validación. Confirmación, mediante la aportación de evidencia objetiva, de que se han cumplido los requisitos para una utilización o aplicación específica prevista [1].

Verificación. Confirmación mediante la aportación de evidencia objetiva, de que se han cumplido los requisitos especificados [1].

Vulnerabilidad. Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Entidad (amenazas), las cuales se constituyen en fuentes de riesgo [8].

Capítulo 1.
Inicio y Planificación

1.1 Introducción

Dentro del marco legal, existen normas y decretos que reglamentan el sistema de gestión pública. Actualmente, el MinTIC proporciona a las diferentes entidades del sector público como la Gobernación del Departamento del Cauca, el Modelo Integrado de Planeación y Gestión (MIPG).

MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos. MIPG recoge en siete dimensiones los aspectos más importantes de las prácticas y procesos que adelantan las entidades públicas. Las políticas de gestión y desempeño proveen los lineamientos bajo los cuales se asegura una gestión y desempeño adecuado y el mejoramiento continuo aplicable a todas las entidades del Estado, donde la seguridad de la información actúa como componente transversal en la implementación de las dimensiones (Figura 1).

Figura 1. Relación: MIPG, GD y Seguridad de la Información. Fuente: propia.

A su vez, las políticas: Gobierno Digital y Seguridad Digital, aparecen como los lineamientos fundamentales en el desarrollo del MSPI (Figura 2) [20]. La implementación de la política se hará a través de la adopción e implementación de las metodologías dispuestas para tal fin. Estas son: el modelo de seguridad y privacidad de la información (MSPI) del MinTIC o un sistema de gestión de seguridad de la información (SGSI) de acuerdo con estándares como: NTC-ISO/IEC27001:2013 o NTC-ISO 27005:2011 entre otras.

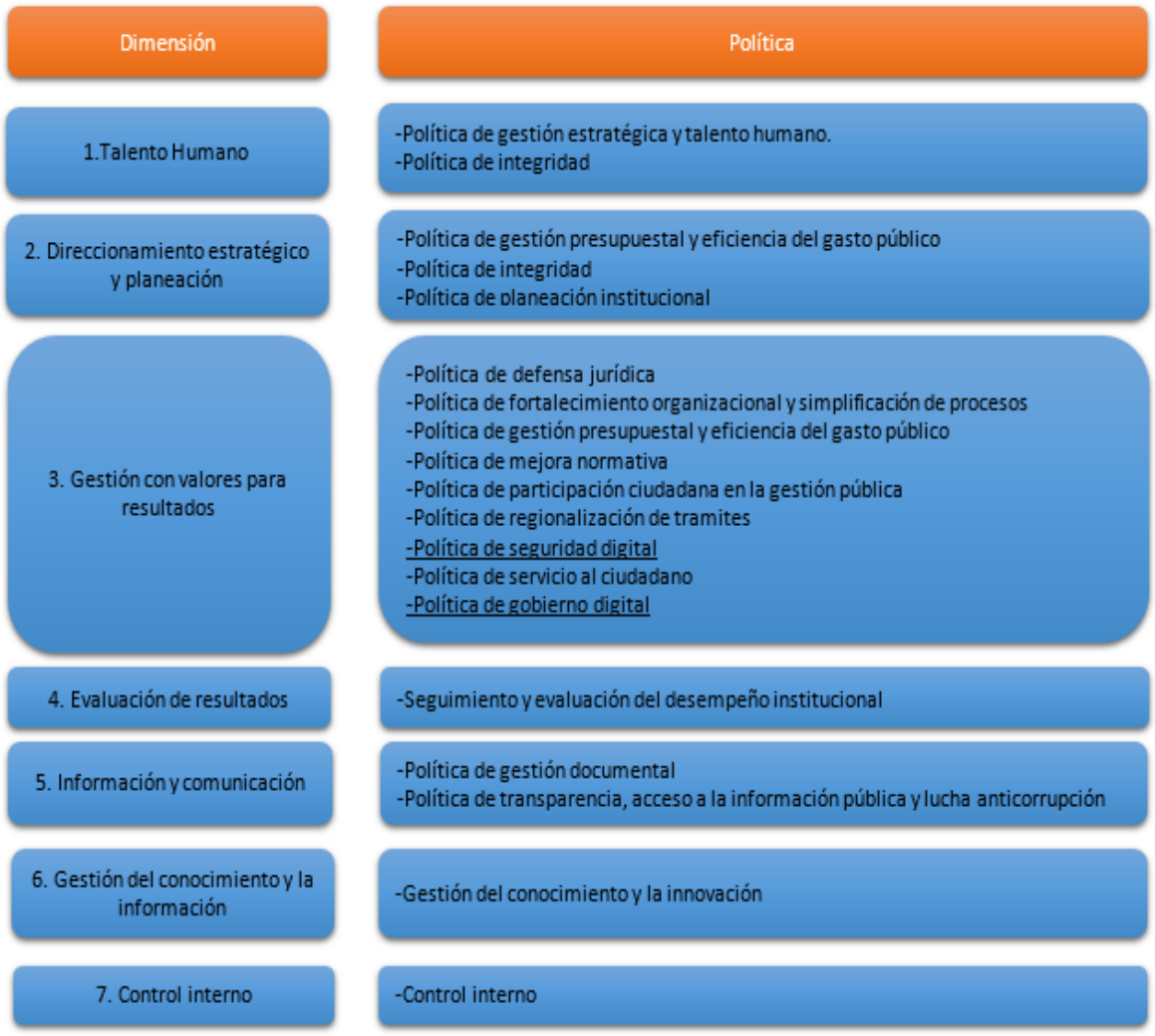


Figura 2. Relación entre dimensiones MIPG y políticas de soporte [21].

Una vez se adoptada el MSPI, el presente trabajo de grado, definirá los procedimientos de seguridad de la información de la Guía N° 3-Procedimientos de seguridad de la información para la gobernación del departamento del Cauca.

Por lo anterior se hace necesario un análisis previo de los procedimientos vigentes de la Gobernación del departamento del Cauca con los cuales laboran actualmente las divisiones de recursos humanos, gestión de tecnologías, proveedores, criptografía y demás, encontrando que se encuentran activos 4 procedimientos formalizados para la seguridad de la información con los cuales los funcionarios de la entidad mantienen un control decadente sobre la información que está siendo manipulada y quien tiene acceso a ella; por tal motivo la gestión de activos y de riesgos no es clara ocasionando confusión entre empleados y usuarios como también que los datos circulantes estén expuestos a interrupción, interceptación o modificación, lo que en consecuencia genera que no se cumpla con la confidencialidad, integridad, disponibilidad y autenticación de la información que se está desplegando.

1.2 Marco Teórico

En el entorno de Seguridad y Privacidad de la Información deben ser de total claridad los instrumentos al alcance de las actividades que se realizarán, por tal motivo es necesario definir los términos involucrados en el desarrollo de la guía de definición de procedimientos para la seguridad y privacidad de la información.

- **AENOR ISO/IEC 27002.**

La norma 27002 especifica los parámetros y controles que deben tenerse en cuenta en los controles de procedimientos de la Gobernación del Departamento del Cauca. Los controles que proporciona la norma establecen de manera específica las normativas que tanto los activos de información como los activos de instalación deben cumplir para garantizar la confidencialidad, disponibilidad e integridad de la información. A su vez brindar la identificación de las vulnerabilidades de la entidad, con los numerales puntuales de los aspectos que deben tenerse en cuenta para generar los procedimientos de seguridad. Lo anterior debe ser implementado de

manera transversal en la entidad, resaltando que las actividades que conforman los procedimientos deben generar un registro, formato o formulario con el fin de llevar el respectivo control del procedimiento en cuestión [22].

- **Gobierno Digital.**

GD se hace necesaria para dar paso a una evolución que permitirá a las entidades públicas adaptarse más fácilmente a las necesidades de la ciudadanía, se basa en dos pilares fundamentales: TIC para servicios, TIC para el gobierno abierto, TIC para la gestión y TIC para la seguridad de la información. GD, se plasma en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015 que comprende cuatro propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información [23].

- **Manual de Gobierno Digital-Implementación de Política de Gobierno Digital.**

Este documento conocido tradicionalmente como “Manual de Gobierno en Línea” y que ahora evoluciona para ser el “Manual para la implementación de la política de Gobierno Digital”, muestra la ruta de acción que deben seguir las entidades públicas para adoptar la política. A partir de ello, su proceso de implementación consta de cuatro grandes actividades: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política, las cuales incorporan acciones que permitirán desarrollar la política en cada una de las entidades públicas [24].

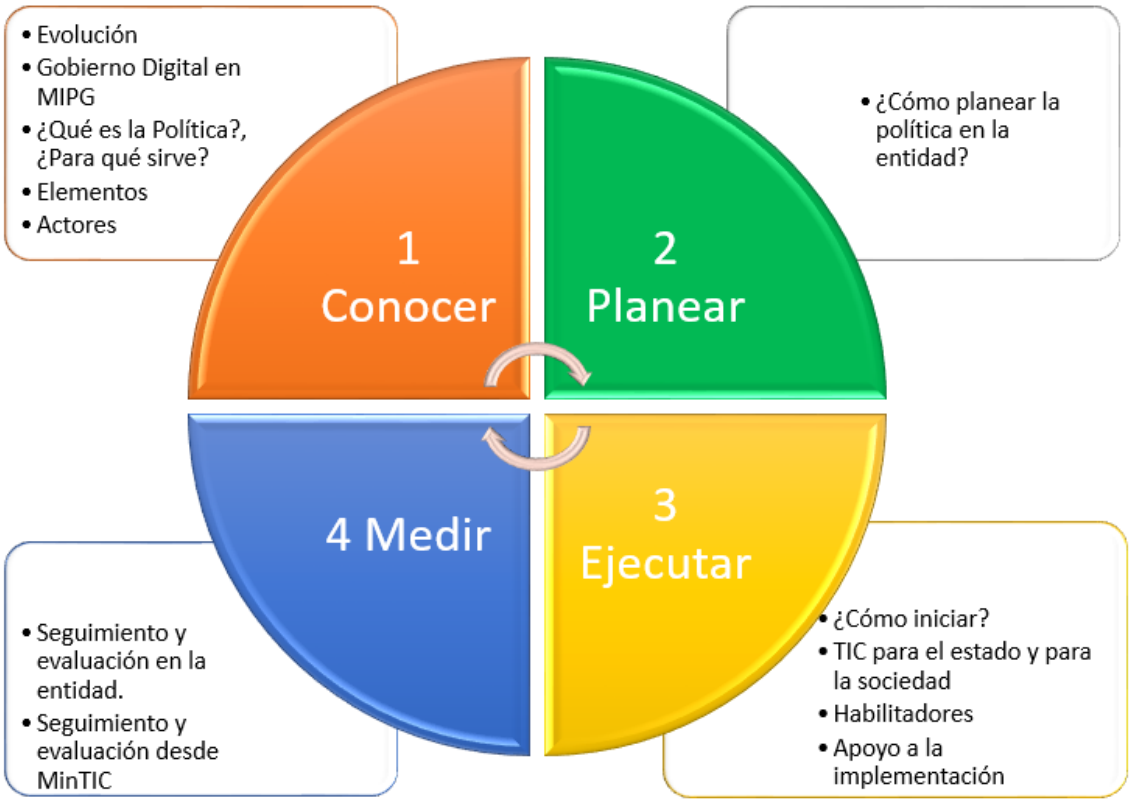


Figura 3. Ciclo PHVA adaptado a política de Gobierno Digital [24].

- **Manual de Política, Uso y Administración de Recursos Tecnológicos de la Gobernación del Departamento del Cauca.**

Las políticas de seguridad son directrices que orientan las actividades tendientes a proteger y administrar correctamente los recursos informáticos y tecnológicos de entidades como la Gobernación del Cauca. Para ello, el Grupo de Gestión Tecnológica y TICs emprendió la tarea de estructurar el Manual de políticas de seguridad de la Gobernación del Cauca, con el fin de reglamentar el uso de la información y recursos tecnológicos y su protección al interior de la entidad.

El objetivo principal del Grupo de Gestión Tecnológica y TICs, es brindar a los usuarios los recursos informáticos con la cantidad y calidad que demandan; esto es que se garantice la continuidad en el servicio los 365 días del año de manera confiable. Así, la cantidad de recursos de cómputo y de telecomunicaciones con que

se cuentan son de consideración y es imprescindible que se protejan para garantizar su funcionamiento.

La política de seguridad, administración y uso informático de la Gobernación del Cauca emerge como el instrumento para concientizar a los servidores públicos sobre la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permitan cumplir con los objetivos propuestos en miras de beneficiar a los ciudadanos del Departamento.

En éste documento se analizarán las políticas de Gestión Informática, Administración de Red, Seguridad de la Red, Correo Electrónico, Servicio de Internet, Sitio Web, Intranet, Recursos Informáticos, Adquisición de nuevas tecnologías, Desarrollo de Software y usuarios finales.

La realización de éste documento, permitirá a los funcionarios tanto administradores del sistema como usuarios finales, tener claridad en el manejo y aplicación de políticas de seguridad informática y administración de los recursos tecnológicos [25].

- **Marco Referencia-Arquitectura TI**.

El Marco de Referencia es el instrumento principal, la carta de navegación, para implementar la Arquitectura TI de Colombia. Esta última, a su vez, habilita o permite hacer realidad la Estrategia de Gobierno Electrónico del Estado colombiano. El objetivo principal del Ministerio de Tecnologías de la Información y las Comunicaciones con estas tres herramientas, la Estrategia, la Arquitectura y el Marco, es apoyar a las instituciones en la eficacia de la gestión de Tecnologías de la Información (TI) [26].

- **Modelo Integrado de Planeación y Gestión-MIPG.**

MIPG es un marco de referencia diseñado para que las entidades identifiquen problemáticas, planeen, ejecuten y hagan seguimiento a su gestión para el beneficio del ciudadano. No pretende generar nuevos requerimientos, sino facilitar la gestión sistémica de las organizaciones a través de la integración de la normatividad vigente en materia de gestión y desempeño, guías para fortalecer el talento humano, agilizar

las operaciones, fomentar el desarrollo de una cultura organizacional sólida y promover la participación ciudadana, entre otros.

El mensaje detrás de este gran esfuerzo es muy claro: la administración pública pretende mejorar la capacidad del Estado para cumplirle a la ciudadanía y a los grupos de valor. Fortalecer MIPG, se traduce en un incremento de la confianza ciudadana en las entidades públicas y sus servidores, y no solo aumenta la gobernabilidad, sino también la legitimidad de nuestro aparato público. Significa también generar resultados con valores, mayor coordinación interinstitucional, servidores públicos comprometidos, un Estado con mayor presencia en el territorio, aumento de la capacidad institucional y un mejor aprovechamiento y difusión de información confiable y oportuna. Además, para el Gobierno será una mejor manera de hacer seguimiento y ofrecer ayuda en los frentes que realmente las entidades territoriales necesitan fortalecer.

MIPG se desarrolla a través de 7 dimensiones operativas, cada dimensión corresponde al conjunto de políticas prácticas, elementos e instrumentos con un propósito común, que permiten desarrollar un proceso de gestión estratégica que se adapta a las características particulares de cada entidad pública [27].

- **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 de la adecuada gestión de riesgos” [2].

- **NTC ISO/IEC 27000.**

La norma NTC ISO/IEC 27000 plantea los conceptos básicos sobre el Sistema de Gestión de Seguridad de la Información (SGSI), es decir, el concepto central sobre el cual se generó NTC ISO/IEC 27001.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la

seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías [8].

- **NTC ISO/IEC 27001.**

La norma NTC ISO/IEC 27001 suministra los requisitos para establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información. La presente norma se implementa para establecer las actividades pertinentes para cumplir los requisitos de seguridad de la Gobernación del Departamento del Cauca.

En ese sentido la norma NTC ISO/IEC 27001 plantea la importancia del Sistema de Gestión de Seguridad de la información, que se ve influenciado por las necesidades, y objetivos de la Gobernación del Departamento del Cauca, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño de la entidad.

En este caso la adopción de éste sistema es una decisión estratégica para la entidad. El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad, de la información, mediante la aplicación del proceso denominado de Modelo de Seguridad y Privacidad de la Información que trae consigo la identificación de las principales falencias y riesgos, lo que brinda confianza a la Gobernación del Departamento del Cauca acerca de los procesos y procedimientos y su óptima gestión. En consecuencia, el presente trabajo de grado satisface la planificación, implementación y control de los procedimientos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones orientadas de la Guía N°3 Procedimientos de Seguridad de la Información. Por tal motivo, todos los procedimientos deben mantener la información documentada en la medida necesaria para tener la confianza en que los procedimientos se han cumplido de manera satisfactoria [28].

- **Procedimientos de Seguridad de la Información.**

La guía denominada PSI contiene las instrucciones para la ejecución de las actividades o tareas determinadas para garantizar el cumplimiento de la misma sobre los métodos específicos para las plataformas, sistemas de información o los puntos clave donde el buen manejo de la información es de primordial importancia independientemente de si es pública o privada [29].

- **Information Technology Infrastructure Library ('Biblioteca de Infraestructura de Tecnologías de Información') ITIL.**

Es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI [30].

1.3 Metodología

Con el fin de desarrollar el trabajo de grado propuesto, se estableció el uso de la Metodología de Marco Lógico que involucra la identificación del problema y las posibles soluciones a lo largo del trabajo de grado, por lo cual se definen fases dentro de las que se enmarcan las diferentes actividades a desarrollar.

De acuerdo a la metodología de Marco Lógico, se llevan a cabo las actividades propias a la Identificación del problema, Análisis del Problema y Análisis de Soluciones acorde con el estado de la Gobernación del Departamento del Cauca [31].

1.3.1 Identificación del Problema.

¿Qué está sucediendo?. Actualmente la Gobernación del Departamento del Cauca lleva a cabo los procesos y procedimientos sin ninguna serie de pasos, motivo por el cual, el personal contratado a nivel institucional, no comprende ni ejecuta medidas necesarias en seguridad de la información [31]. El hecho de no tomar esas precauciones, ocasiona que se generen consecuencias, como:

- Mal manejo de los recursos de red.

- Pérdida de información de la entidad.
- Libre acceso a zonas y sistemas de información que únicamente deben ser manipuladas por personal autorizado.
- Inexistencia de registros de cualquier tipo de acceso, modificación, e implementación de activos de información.
- Ping Pong: no hay comunicación entre las diferentes oficinas ya que se trocan los procesos debido a la falta de procedimientos que proporcionen actividades puntuales para realizarlos.

1.3.2 Análisis del Problema.

¿Por qué está sucediendo?. Por lo anterior se debe analizar la causa por la cual se generan los inconvenientes en las distintas oficinas de la Gobernación del Departamento del Cauca. Puntualmente se realizó la recolección de la información involucrada que se hace necesaria; el resultado: carencia de procedimientos con un marco de referencia valido para implementación, falta de estructuración de mesas de trabajo para socializar avances, cambios y modificaciones que afecten a la entidad en general, falta de asignación de roles y responsabilidades en temas de seguridad de la información, tiempos demasiado extensos para dar respuesta ante solicitudes de información que deben estar al alcance de todo funcionario. Lo anterior, resumido en que no se implementa la Política de Seguridad de la Información y que no existen los procedimientos de Seguridad de la Información para la Gobernación del Departamento del Cauca.

En consecuencia, de lo anterior no hay procedimientos que generen controles sobre los datos que se generan en la entidad, exponiendo la confidencialidad, integridad y disponibilidad de la información.

Las 3 características: confidencialidad, integridad y disponibilidad, deben garantizarse para cada activo relacionado con la oficina de Gestión Tecnológica de la Gobernación del Departamento del Cauca con el fin de dar cumplimiento a la ley 1753, artículo 53 del aprovechamiento de las TIC.

En ese sentido la figura 5 resume, cuáles son los problemas principales, por qué se están generando, y las consecuencias que acarrea la entidad.

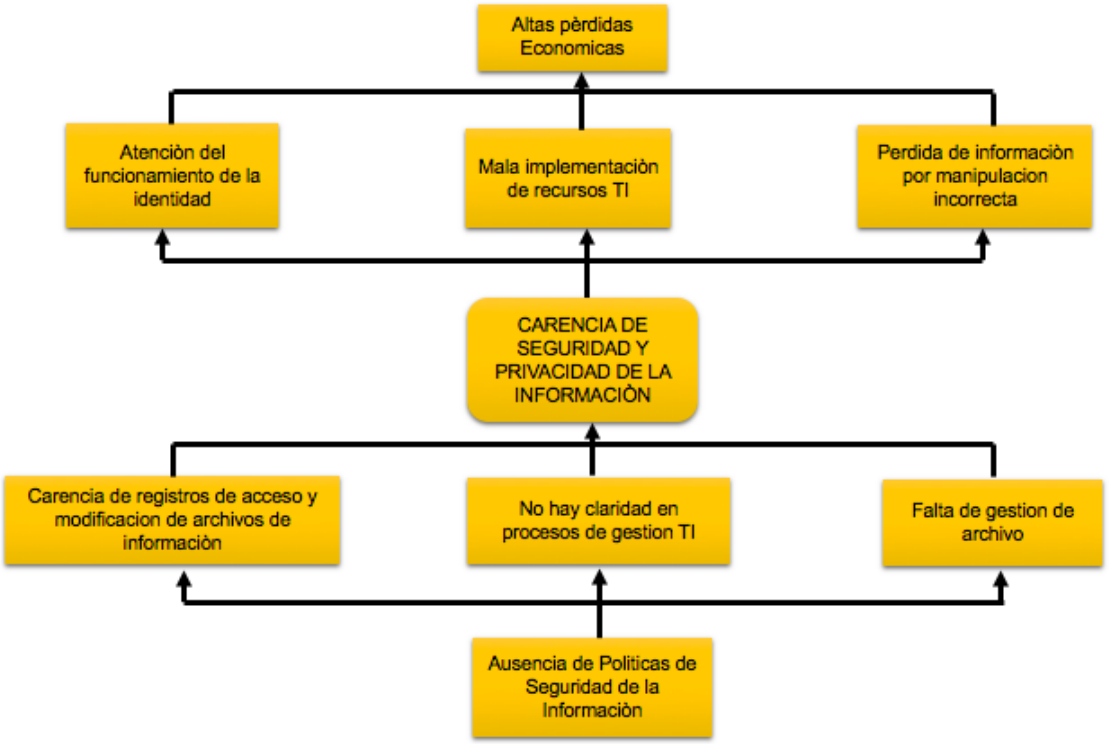


Figura 4. Relación: causa-problema-consecuencia. Fuente: propia

1.3.3 Análisis de Soluciones

¿Qué se puede realizar para garantizar la seguridad de la información y mitigar los riesgos?

Teniendo en cuenta los inconvenientes que se generan y la pérdida de información por la falta de procedimientos y de la política de Seguridad de la Información, debe analizarse como modelar la solución a la situación actual de la Gobernación del Departamento del Cauca para garantizar que los servicios que presta esta misma sean de satisfacción para los ciudadanos y cumplan con los estándares de calidad proporcionados por la respectiva normatividad colombiana. En ese sentido se proyecta la Figura 6, donde se involucran los procedimientos de seguridad de la información como solución a los inconvenientes anteriormente descritos.

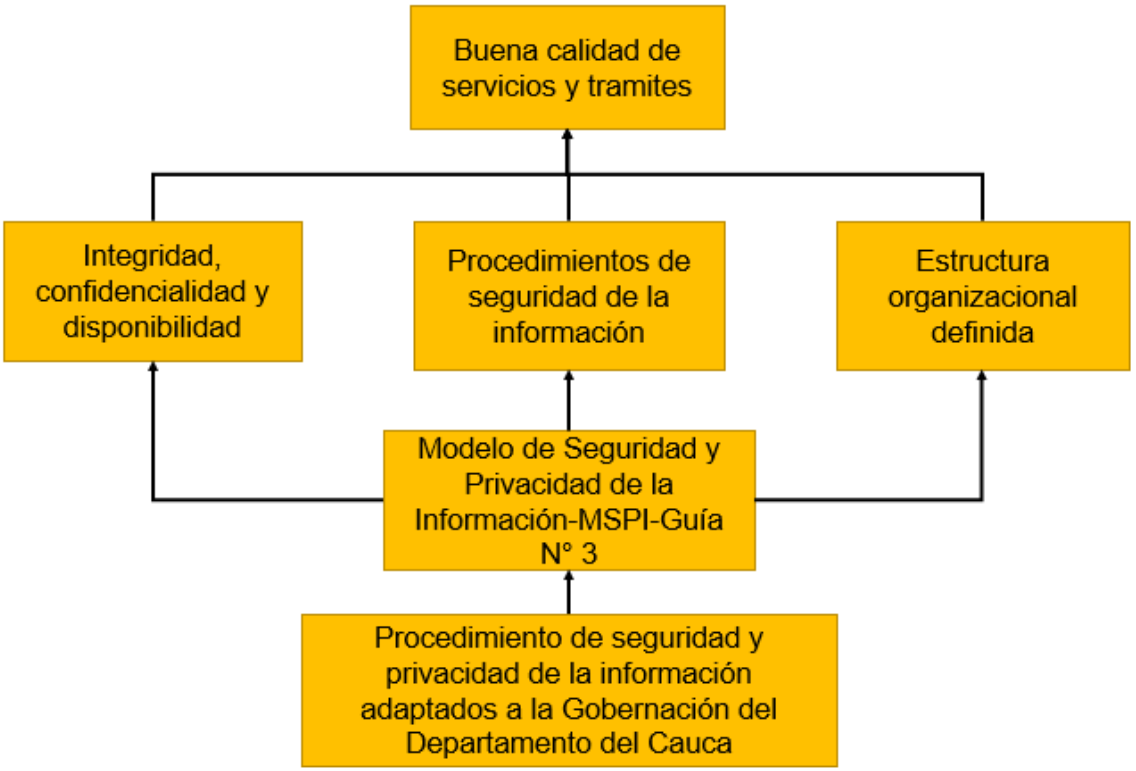


Figura 5. Análisis de soluciones. Fuente: propia

1.4 Recolección de la Información

1.4.1 Procedimientos Existentes.

La revisión de antecedentes del presente trabajo de grado se basa en la recolección de información de todos los aspectos que involucren el componente de Seguridad de la Información, y de esta manera conocer el estado actual de La Gobernación del Departamento del Cauca. La recolección de información se realiza de parte de las oficinas y secretarias involucradas y que influencian ese proceso de avance a medida que se requieran datos cruciales en el desarrollo de las actividades.

De manera cronológica la oficina de gestión tecnológica estipuló cuatro procedimientos de seguridad de la Información en el año 2016, dentro de los cuales se contemplan las

actividades relacionadas a Copias de Seguridad, Gestión de Administración de Sistemas de Información y Soporte Técnico. Estos procedimientos vigentes en la Gobernación del Departamento del Cauca se acogen a un formato estipulado por la Oficina de Gestión Organizacional, con una estructura de explicación completa de los aspectos del procedimiento.

En consecuencia, el formato a implementar tanto en los procedimientos anteriores como en los actuales, es el siguiente:

	PROCEDIMIENTO DE SEGURIDAD DE INFORMACIÓN	Código: Versión: 01 Fecha : Página

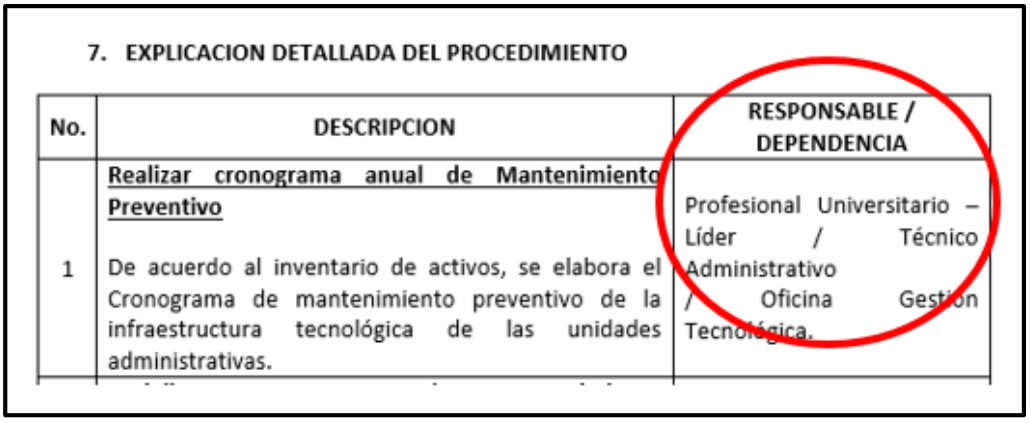
Versión	Fecha (D-M-A)	Apoyo a la elaboración	Elaborado por	Razón de la actualización
02	31-08-2018	Firma:	Firma:	

Revisado por:	Aprobado por:
JAIME ALBERTO DORADO ZUÑIGA Profesional Universitario Administrador del SIG Oficina de Gestión Organizacional	GUIDO ALBERTO GARZÓN Secretario General

1. **INTRODUCCIÓN**
2. **OBJETIVO**
3. **INVOLUCRADOS**
4. **ALCANCE**
5. **NORMATIVAS**
6. **POLÍTICAS**
7. **DEFINICIONES**
8. **SIGLAS**
9. **EXPLICACIÓN DETALLADA DEL PROCEDIMIENTO**
10. **MESA DE TRABAJO**

Figura 6. Formato de generación de procedimientos-
Oficina de Gestión Organizacional.
Fuente: Gobernación del departamento del Cauca

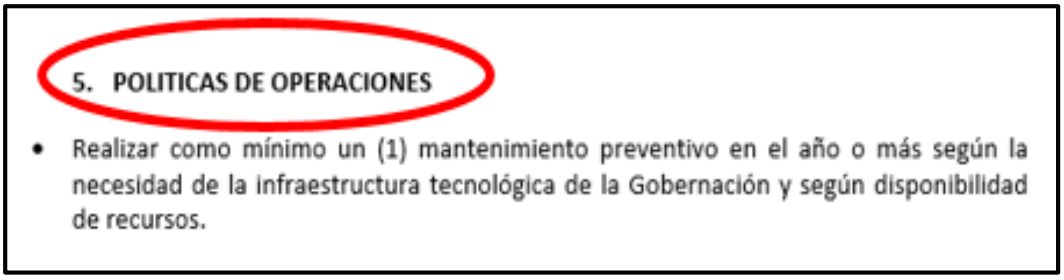
En ese sentido los procedimientos, contienen la definición de: Objetivo a cumplir, alcance del procedimiento (actividad que da inicio y actividad que lo finaliza), responsables (quien lo implementa), políticas de operación, definición de términos implementados a lo largo del procedimiento, explicación detallada del procedimiento, registros, documentos internos y documentos externos (Figura 7, Figura 8 y Figura 9).



7. EXPLICACION DETALLADA DEL PROCEDIMIENTO

No.	DESCRIPCION	RESPONSABLE / DEPENDENCIA
1	**Realizar cronograma anual de Mantenimiento Preventivo** De acuerdo al inventario de activos, se elabora el Cronograma de mantenimiento preventivo de la infraestructura tecnológica de las unidades administrativas.	Profesional Universitario – Líder / Técnico Administrativo / Oficina Gestion Tecnológica.

Figura 7. Responsable de la Actividad. Fuente: Gobernación del departamento del Cauca



5. POLITICAS DE OPERACIONES

- Realizar como mínimo un (1) mantenimiento preventivo en el año o más según la necesidad de la infraestructura tecnológica de la Gobernación y según disponibilidad de recursos.

Figura 8. Políticas de operación de procedimientos. Fuente: Gobernación del departamento del Cauca

En ese proceso, la explicación detallada del procedimiento contiene las actividades y su descripción detallada, así:

7. EXPLICACION DETALLADA DEL PROCEDIMIENTO

No.	DESCRIPCION
1	**Realizar cronograma anual de Mantenimiento Preventivo** De acuerdo al inventario de activos, se elabora el Cronograma de mantenimiento preventivo de la infraestructura tecnológica de las unidades administrativas.

Figura 9. Descripción de actividad. Fuente: Gobernación del departamento del Cauca

En ese sentido, los roles definidos para los procedimientos vigentes antes del MSPI, se presentan en la siguiente relación, donde se evidencian los que se desempeñan en estos procedimientos, teniendo en cuenta los cargos que otorga la Gobernación del Departamento del Cauca, tales como profesional universitario y técnico administrativo en las distintas categorías:

Gobernación del Cauca	**Relación de roles y procedimientos de seguridad de la información-modelo de seguridad y privacidad de la información.**			
Cargo	Gestión de administración de sistemas de información	Mantenimiento preventivo y correctivo	Copias de seguridad	Soporte técnico
Profesional universitario-02				
Profesional universitario-02				
Técnico administrativo-06				
Técnico administrativo-05				
Técnico administrativo-01				

Tabla 1. Relación roles y responsabilidades de procedimientos existentes. Fuente: propia

En el transcurso de la recolección de información se toma como un referente importante MIPG ya que cuenta con 4 componentes de la política de GD para su funcionamiento y de los cuales extraeremos únicamente Seguridad de la Información como parte fundamental del trabajo a desarrollar. Por lo tanto, MIPG presenta como antecedentes del presente trabajo de grado, 3 aspectos de evaluación: autodiagnóstico, plan de acción

y gráficas; que se relacionan como se indica en la figura 10, donde el estado rojo y naranja es crítico, amarillo representa un nivel medio de avance y verde el avance optimo que se pretende en las entidades del estado como la Gobernación del Departamento del Cauca.

1.4.2 Herramienta de Autodiagnóstico MIPG

La herramienta de autodiagnóstico realizó la evaluación a criterio de experto en manos de la oficina de Gestión Tecnológica acompañada por la oficina de Gestión Organizacional; donde se analizaron 4 indicadores de proceso: definición del marco de seguridad y privacidad de la información, plan de seguridad y privacidad de la información, monitoreo y mejoramiento continuo y el indicador de resultado: seguridad y privacidad de la información, reflejado en la Figura 10.

De ese análisis, se obtiene el balance total del componente completo de seguridad de la información en la política de Gobierno Digital, con un balance de 31 puntos, como se observa en la Figura 11, calificándose como un nivel precario en la implementación del componente en cuestión [32]. (Ver anexo A)

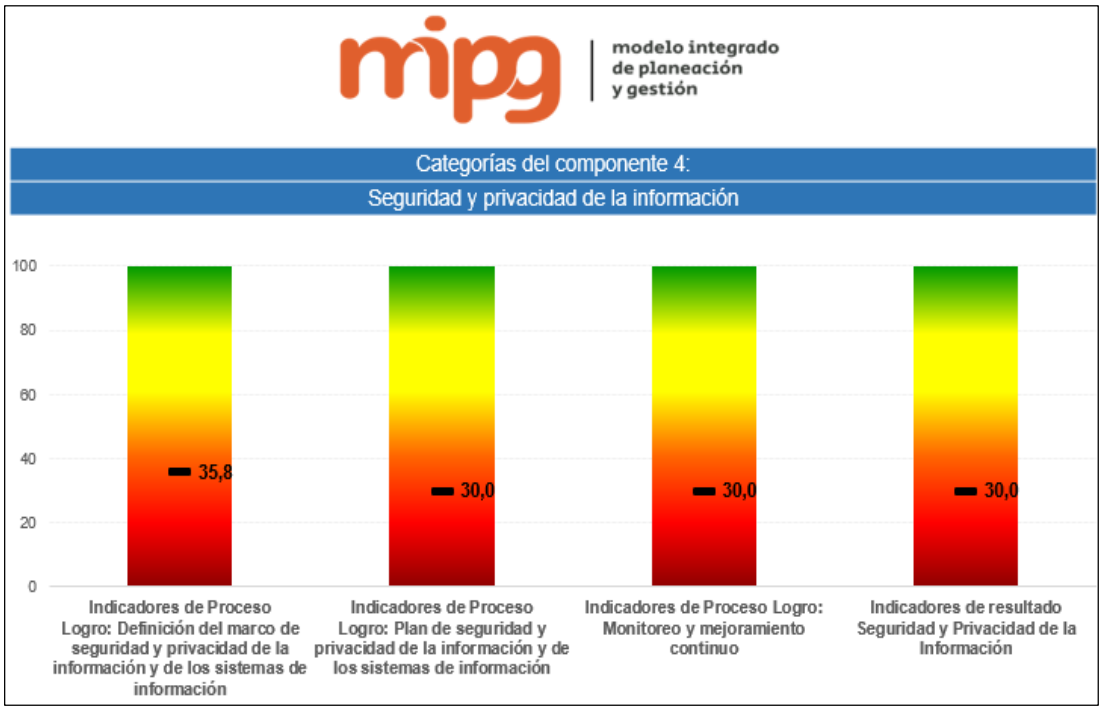


Figura 10. Resultado-componente 4: seguridad de la información.
Fuente: Gobernación del Departamento del Cauca.

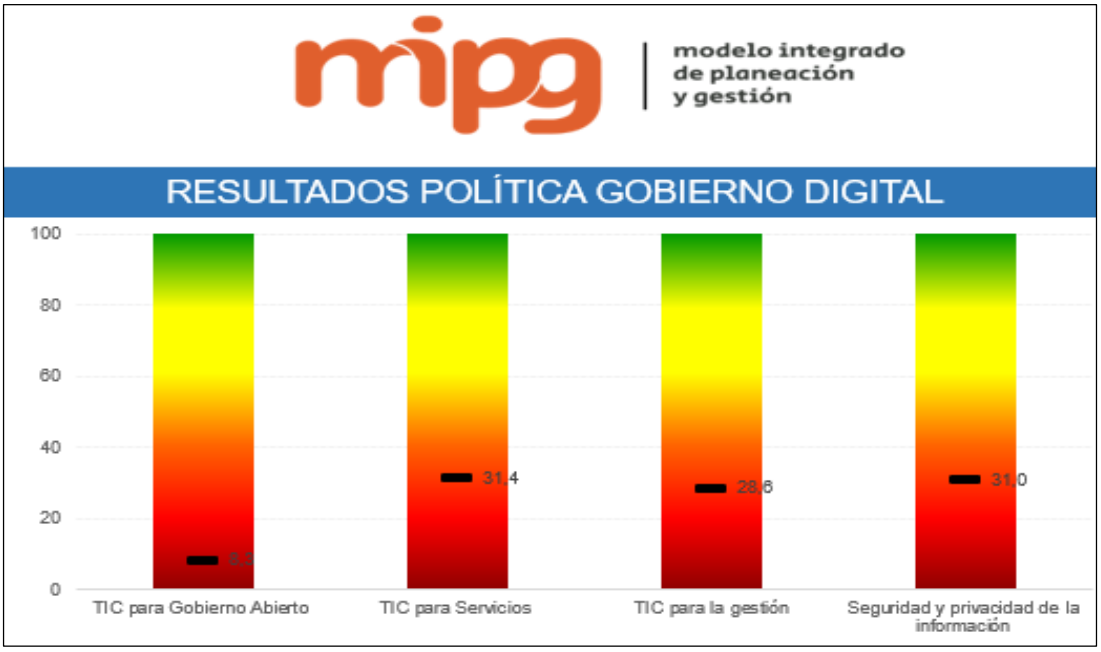


Figura 11. Autodiagnóstico- política Gobierno Digital

Fuente: Gobernación del departamento del Cauca.

1.5.3 Herramienta de Evaluación del MSPI

Por otra parte, la evaluación de avance del MSPI se ejecuta con la herramienta de evaluación del mismo teniendo en cuenta los criterios proporcionados por el MinTIC, establecidos en la tabla 1 [33]; describiendo el campo criterio como argumento para asignar la calificación y la descripción, de la siguiente manera:

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
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.

Tabla 2. Criterios de evaluación controles-MSPI [34].

Como primera pauta el instrumento de evaluación del MSPI presenta varios aspectos que permiten identificar las necesidades y el avance de la entidad respecto a la implementación del Manual de Gobierno Digital en la Gobernación del Departamento del Cauca. En este caso el MSPI abarca una gran cantidad de aspectos que lo hacen funcional, uno de los principales es Procedimientos de Seguridad de la Información donde se definen los pasos para cumplir a satisfacción los controles mínimos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los activos de información de la Gobernación del Departamento del Cauca.

La Tabla 2 presenta el levantamiento inicial del instrumento de identificación de la línea base de seguridad, donde se ilustra la brecha entre la implementación del MSPI y la evaluación de la efectividad de los controles NTC ISO/IEC 27001 al interior de la Gobernación del Departamento del Cauca, ya que se toma la norma como referente de calidad respecto a estándares de seguridad de la información [33]. Lo anterior se recoge como resumen de la evaluación realizada en la entidad (Ver Anexo B).

La evaluación se realiza en consideración con el instructivo de uso de la herramienta de evaluación del modelo de seguridad y privacidad de la Información [34].

En consecuencia, al implementar la herramienta de evaluación, se evidencia que el MSPI está en su etapa inicial encontrándose en un rango entre 0 y 20% de avance, índice crítico en seguridad. La inexistencia de casi todos los procedimientos con que debe contar la Gobernación del Departamento del Cauca, por lo cual se observa que únicamente cuenta con la Políticas de Seguridad de la Información [33]

.

Gobernación del Cauca

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

ENTIDAD EVALUADA	**Gobernacion del Departamento del Cauca**
FECHAS DE EVALUACIÓN	
CONTACTO	
ELABORADO POR	Oficina de Gestión Tecnológica y Gestión Organizacional

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	INEXISTENTE
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	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	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
PROMEDIO EVALUACIÓN DE CONTROLES		**1**	**100**	INICIAL

Tabla 3. Evaluación de efectividad de controles [34].

Por otro lado, la herramienta de evaluación del MSPI proporciona el resultado del avance de ciclo de funcionamiento del modelo de operación PHVA, a través de los años mostrando el porcentaje de avance actual y el porcentaje de avance esperado en la entidad, con un total de 2% desde el año 2015 hasta el año 2018.

En ese sentido y con las categorías anteriormente presentadas, el nivel de madurez de seguridad de la información se establece con los criterios basados en el cumplimiento de los controles y procedimientos al interior de la Gobernación del departamento del Cauca al final de la evaluación, cuyo resultado es de un nivel crítico [33].

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

Tabla 4. Total, de requisitos con calificaciones de cumplimiento [34].

En la misma evaluación se realiza una breve descripción de los criterios que se implementan a la hora de evaluar el nivel de madurez en que se encuentra la entidad, es decir, que criterio evaluativo de desarrollo e implementación del MSPI se asigna (Tabla 5) [33].

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
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.

Tabla 5. Nivel de madurez del Modelo de seguridad y privacidad de la información [34].

Una vez comprendidos por la entidad los criterios anteriormente mencionados, se lleva a cabo la evaluación del nivel de madurez respecto a la Gobernación del Departamento del Cauca, ilustrado en la Tabla 6, donde se califica el nivel inicial como intermedio, es decir, en pleno arranque de su planificación y desarrollo, donde el personal aun no aprueba los documentos en seguridad de la información y tampoco los divulgan [34].

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Gobernación del Cauca		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	INTERMEDIO
	Repetible	CRÍTICO
	Definido	CRÍTICO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

Tabla 6. Evaluación de nivel de madurez-MSPI [34]

Capítulo 2.
Ejecución y Control

2.1 Generación de Procedimientos de Seguridad y Privacidad de la Información para la Gobernación del Departamento del Cauca.

Una vez analizados los antecedentes que contextualizan el estado de la Gobernación del Departamento del Cauca respecto al nivel de madurez del MSPI, y dando cumplimiento al formato para estipular los mismos, se procede a establecer los procedimientos de seguridad y privacidad de la información, según la Guía No. 3 del MSPI proporcionada por el MinTIC. En ese sentido se realiza de manera general para todos los procedimientos lo siguiente:

- Clasificación del personal involucrado en las actividades de cada control aplicado.
- Establecimiento de Roles, responsables de control y funciones para los procedimientos de seguridad.
- Definir objetivos y políticas de operación para los procedimientos.
- Determinar los controles y actividades aplicables en la entidad.
- Establecer mesas de trabajo para una mejora continua de los procedimientos.

2.1.1 Personal involucrado en los procedimientos

El personal involucrado en los procedimientos, se clasifico conforme a los grupos ocupacionales a los que pertenecen dependiendo de su cargo en la Gobernación del Dpto. del Cauca (Tabla 7). Lo anterior con el fin de ligar de manera directa a quien va dirigida cada actividad en los procedimientos de seguridad de la información.

La clasificación se realiza de manera transversal a la entidad y de esa misma forma se adopta en todos los procedimientos [35].

Grupo Ocupacional	Nombre	Personal involucrado
I	Servicios Generales	▪ Mensajeros externos ▪ Chofer ▪ Personal de limpieza
II	Apoyo administrativo	▪ Recepcionista ▪ Secretaria ▪ Auxiliar ▪ Digitador
III	Técnico	▪ Técnico administrativo.
IV	Profesionales	▪ Profesional universitario
V	Dirección y supervisión	▪ Gobernador del Dpto. del Cauca. ▪ Líderes de oficina.

Tabla 7. Clasificación del personal de la entidad

Ahora bien, el personal que implemente las actividades ligadas a los controles, debe estar sujeto a un rol, responsabilidad de control y función a desempeñar (Tabla 8).

Lo anterior sujeto a ITIL [36], la cual se refiere al conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información en pro de mejorar los procesos de la entidad, para llevar a cabo el proceso de asignación de roles y responsabilidades estará a cargo de la mesa de trabajo conformada y liderada por la Oficina de Gestión tecnológica de la Gobernación del Cauca, Oficina de Recursos Humanos, Oficina de Gestión Organizacional, Archivo Central, Oficina Asesora Jurídica, Oficina de Planeación entre otras.

ROLES – RESPONSABLES DE CONTROL –FUNCIONES			
N°	**Roles (ITIL-4.4)**	**Responsable de Procesos (ITIL-4.4)**	**Funciones (ITIL-4.2, NTC ISO/IEC 27001-5.3)**
1	Propietario del proceso, responsable de la información. (Altos ejecutivos: Gobernador del Dpto del Cauca, Responsable de Secretaria, Líder de Oficina)	Es el área, dependencia o grupo que creo la información, encargado de impulsar diseñar y realizar gestión del proceso de gestión de seguridad y privacidad de la Información.	• Tomar decisiones sobre el buen uso de la información y Comunicar información del proceso o cambios cuando se apropiado • Garantizar que se cumplan los controles de protección dela información, gestionar recursos al proceso para soportar sus actividades. • Garantizar que la información se encuentre disponible, integra y que solo personal autorizado tenga acceso a ella. • Hacer manteamiento periódico y evaluar su clasificación y valoración.
2	Gestor del proceso (líderes de oficinas o dependencias)	Es el área o dependencia o grupo encargado de la protección y control para el efecto de permitir su acceso, además trabaja con el propietario del proceso para planear y coordinar todas las actividades	• Asegurar que todas las actividades son llevadas a cabo como es requerido • Nombrar a las personas para los roles requeridos • Gestionar los recursos asignados al proceso • Trabajar con los dueños y otros gestores de procesos para asegurar la correcta ejecución de los servicios • Monitorear y reportar el rendimiento del proceso • Identificar oportunidades de mejora y registrarlas • Proteger la información de los activos. • Acatar los controles de seguridad establecidos para la protección de la información. • Ejecutar las actividades propias de su cargo de acuerdo a la custodia de la información .
3	Ejecutor del proceso, usuario final (Funcionario)	Personal que hace uso de los activos de información.	• Hacer buen uso de los activos de información asignados • Garantizar la confidencialidad, integridad, y disponibilidad del activo de información, también llevar a cabo una o más actividades del proceso. • Entender cómo contribuye a la entrega del servicio y a la creación de valor al negocio. • Asegurar que sus acciones son efectivas • Asegurar que las entradas, salidas e interfaces son correctas. • Crear o actualizar registros relacionados al proceso • Reportar cualquier evento que atente contra la seguridad de la información.

Tabla 8. Roles, responsables de control y funciones. Fuente propia.

2.1.2 Objetivos y Políticas de operación de los procedimientos de Seguridad de la información.

Los procedimientos de seguridad de la información deben tener un enfoque específico y un soporte brindado por la organización en el cual basar sus pautas; para establecer los controles y actividades propias de los mismos. En ese sentido la Tabla 9 presenta los objetivos y la política de operación empleada en cada procedimiento [25], [29].

	OBJETIVOS Y POLÍTICAS DE OPERACIÓN-PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN			
	Nombre	**Objetivo General**	**Objetivos Específicos**	**Políticas de Operación**
PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN	Procedimiento de Seguridad del Recurso Humano	Definir responsabilidades relacionadas con la seguridad y privacidad de la información antes, durante y después del empleo.	**1.** Garantizar que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran. **2.** Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información. **3.** Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.	La política general de seguridad y privacidad de la información de la Gobernación del Departamento del Cauca, dentro de los procedimientos de vinculación y desvinculación al igual que la capacitación y sensibilización del personal activo en la entidad, constituye la base del presente procedimiento a partir del numeral 10. Seguridad Personal. "Todos los empleados de la Gobernación del Departamento del Cauca y cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la Organización. Esto comprende los requerimientos de seguridad, las responsabilidades legales y controles de la Gobernación, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, servicios y recursos por ej. El procedimiento de entrada al sistema ("log-on") y el uso de paquetes de software, antes de que se le otorgue acceso a la información o a los servicios."
	Procedimiento de Gestión de Activos	Establecer la manera en que los activos de información son identificados e inventariados por la Gobernación del Departamento	**1.** Identificar los activos de información de la organización en conjunto con las responsabilidades de protección adecuadas.	Procedimiento se basa en los numerales 9.1, 9.2, 9.3 de la Política de seguridad de la información de la Gobernación del Cauca.

	OBJETIVOS Y POLÍTICAS DE OPERACIÓN-PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN			
	Nombre	**Objetivo General**	**Objetivos Específicos**	**Políticas de Operación**
		del Cauca, de acuerdo a su nivel de confidencialidad o criticidad.	**2.** Asegurar que los activos de información reciban un nivel apropiado de protección, de acuerdo con el nivel de criticidad e importancia.	
	Procedimiento de Control de Acceso	Limitar el acceso a los recursos de tratamiento de información y a la información.	1. Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios. 2.Responsabilizar al usuario de salvaguardar la información de autenticación. 3. Prevenir el acceso no autorizado a los sistemas y aplicaciones.	Con el propósito de estipular el procedimiento de Control de Acceso a los Sistemas de Información se toma como referente la política general de control de acceso donde se encuentran los lineamientos necesarios para gestionar el acceso por parte de los funcionarios y/o contratistas a los mismos. Para conservar una línea de cumplimiento de las políticas de seguridad de la Información se resalta el siguiente enunciado: ✓ Los accesos a las áreas críticas deberán ser restringidos de acuerdo a las políticas que emite el Grupo de Tecnología, Conectividad y Comunicaciones. ✓ El acceso de los usuarios será únicamente a los recursos informáticos que requiera para desarrollar su trabajo. ✓ Se debe llevar registro de altas, bajas y cambios de usuarios con acceso a los sistemas informáticos y a la red. ✓ Se deben crear y mantener perfiles de seguridad para todos los usuarios con base en sus roles y responsabilidades.
	Procedimiento de Criptografía	Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.	**1.** Establecer el procedimiento con base a la política sobre el uso de los controles criptográficos para protegerla información. **2.** Describir la manera en que se gestionan las llaves criptográficas con base a la política sobre el uso de las llaves a lo largo de su ciclo de vida.	De acuerdo a la política de uso de controles criptográficos y gestión de llaves criptográficas propuestas por la Auditoria General de la Republica en los numerales 4.1, 4.2, y de manera simultánea la Política de seguridad de la Red del numeral 13. de políticas de Seguridad de la Gobernación del Cauca, se propone aplicarlas con el objetivo de mantener las características de confidencialidad, integridad,

	OBJETIVOS Y POLÍTICAS DE OPERACIÓN-PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN			
	Nombre	**Objetivo General**	**Objetivos Específicos**	**Políticas de Operación**
				disponibilidad y no repudio vinculadas a la norma [ISO/IEC 27002] que busca proteger la autenticidad e integridad de los activos de información y datos circulantes.
	Procedimiento de Seguridad Física y del Entorno	Definir la manera de prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.	**a.** Establecer los perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información. **b.** Evitar la pérdida, daño, robo, o el compromiso de los activos y la interrupción de las operaciones de la organización.	La política de seguridad que brinda la Gobernación del Departamento del Cauca señala en los numerales 11. Política de Seguridad y Ambiente y 12. Política de Administración de la Red, los cuidados que se hacen necesarios en el uso de las instalaciones y áreas vulnerables de la entidad. Estos numerales resumen los controles que son necesarios para asegurar el uso apropiado y eficaz de las zonas vulnerables, como también prevenir el acceso físico no autorizado, daño e interferencia en instalaciones o equipos contenedores de información de la entidad. Agregado. La política involucra todo el numeral 12 de tratado del cableado para la Gobernación del Departamento del Cauca, regido por los estándares necesarios.
	Procedimiento de Seguridad de las Operaciones	Asegurar el correcto funcionamiento y seguro de las instalaciones de tratamiento de la información para su procesamiento	**1.** Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware. **2.** Evitar perdida de datos. **3.** Registrar eventos y generar evidencia. **4**. Asegurar la integridad del software en explotación. **5.** Reducir riesgos resultantes de la explotación de las vulnerabilidades técnicas.	La política de seguridad de la Gobernación del Departamento del Cauca, documento que articula la filosofía, los requerimientos reglamentarios que tiene en relación con la protección de los recursos de información, tecnológicos y telecomunicaciones. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la administración central.
	Procedimiento de Seguridad de las Comunicaciones	Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.	**1.** Identificar los mecanismos de seguridad, niveles de servicio, y los requisitos de gestión de todos los servicios de red. **2.** Mantener la seguridad en la información	Procedimiento de seguridad de las comunicaciones toman como referente los numerales 13, 14, 15 y 16 de la política de seguridad y privacidad de la información de la Gobernación del Departamento del Cauca que se

	OBJETIVOS Y POLÍTICAS DE OPERACIÓN-PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN			
	Nombre	**Objetivo General**	**Objetivos Específicos**	**Políticas de Operación**
			que se transfiere dentro de una organización y con cualquier entidad externa.	encuentran en proceso de validación, por medio de las cuales se llevará a cabo el cumplimiento del procedimiento de gestión de activos de información enmarcado en el proceso de procedimientos de seguridad de la información y el macro proceso Modelo de Seguridad y Privacidad de la Información (MSPI).
	Procedimiento de Seguridad en Relaciones con Proveedores.	Asegurar la protección de los activos de información de la Gobernación del Departamento del Cauca que sean accesibles a los proveedores.	Definir acuerdos apropiados con proveedores de servicios y/o productos	la protección de los recursos de información, tecnológicos y telecomunicaciones establece en el numeral 8.3 del mismo especificaciones del manejo de la relaciones con los proveedores. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la administración central.
	Procedimiento de Adquisición y Mantenimiento.	Garantizar que la seguridad de la información relacionada a la adquisición, desarrollo y mantenimiento de sistemas de información sea parte integral de los sistemas de información a través de todo el ciclo de vida.	**1.** Garantizar la seguridad de la información que ha diseñado e implementado en el ciclo de desarrollo de información. **2.** Asegurar la protección de los datos de prueba. **3.** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores. **4.** Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores. **5.** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluida la comunicación de eventos de seguridad y debilidades. **6.** Asegurar la disponibilidad de los recursos de tratamiento de la información.	La política de seguridad de la Gobernación del Departamento del Cauca, documento que articula la filosofía, los requerimientos reglamentarios que tiene en relación con la protección de los recursos de información, tecnológicos y telecomunicaciones. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la administración central.

	OBJETIVOS Y POLÍTICAS DE OPERACIÓN-PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN			
	Nombre	**Objetivo General**	**Objetivos Específicos**	**Políticas de Operación**
	Procedimiento de Gestión de Incidentes	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.	1. Definir roles y responsabilidades en gestión de incidentes con personal apropiado.	Como base el numeral 10.3 de la política de seguridad de la información de la Gobernación del Cauca, donde se entabla la concienciación que debe realizarse a los empleados en reportaje de incidentes y la gestión de los mismos.
	Procedimiento de Gestión de Continuidad del Negocio	Definir la continuidad de la seguridad de la información como parte de los sistemas de gestión de continuidad de negocio de la Gobernación del Departamento del Cauca.	1. Definir un plan de continuidad en caso de incidentes. 2. Definir roles y responsabilidades en gestión de soluciones para garantizar continuidad del negocio	La política de seguridad de la Gobernación del Departamento del Cauca, es el documento que articula la filosofía, los requerimientos reglamentarios que tiene en relación con la protección de los recursos de información, tecnológicos y telecomunicaciones. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la administración central.

Tabla 9. Relación de objetivos y políticas de operación.

Fuente propia.

2.2 Seguridad relativa a los recursos humanos-A.7 ISO 27001

El procedimiento de seguridad de la información relacionado con Recursos Humanos se desarrolla con base en la NTC ISO-27001 control A.7, NTC ISO/IEC 27002 numeral 7 relacionado con la seguridad del recurso humano, donde la oficina de Gestión Tecnológica de la Gobernación del departamento del Cauca implementa la política de seguridad y privacidad de la información y la dependencia relacionada realizará la aplicación del control, el procedimiento se despliega en 3 etapas principales en las cuales se determina el ciclo laboral de un funcionario y/o contratista, el objetivo: asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.

- Etapa 1: Procedimiento de Vinculación Laboral.
- Etapa 2: Procedimiento de Capacitación y Sensibilización.
- Etapa 3: Procedimiento de Desvinculación Laboral.

2.2.1 Etapa 1: Procedimiento de Vinculación laboral.

La fase de vinculación laboral, posee las actividades pertinentes al nombramiento del funcionario y/o contratista y los requerimientos necesarios para que sea viable. En la Tabla 10, se describen las actividades que la Gobernación del Departamento del Cauca debe implementar, relacionado a la actividad, tarea a desarrollar, el responsable y el registro que se genera en el procedimiento de seguridad de información – recurso humano [37].

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 1 VINCULACIÓN LABORAL.							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe realizar de acuerdo con las leyes, normas y códigos éticos que sean de aplicación en la Gobernación del Departamento del Cauca.	Convocatorias de empleo.	Realizar la convocatoria de empleos (La Gobernación del Dpto del Cauca se encargará de estudiar las necesidades de las oficinas que la componen, con el fin de abrir convocatorias para nombramiento de planta o como contratista, con los perfiles requeridos).	**Implementa** Oficina de Talento Humano-Prof. Universitario **Aplica control** Oficina de Talento Humano-Profesional Universitario	I, II, III, IV y V	Convocato-ria abierta	A.7.1.1 Selección	7.1 Antes del empleo. 7.1.1 Investigación de antecedentes
	Investigación de antecedentes	Solicitar referencias: la oficina de talento humano debe solicitar referencias pertinentes con el fin de realizar la investigación de los antecedentes del postulante. Referencias: a.Profesional y personal b.Comprobación de hoja de vida c.Verificación de calificaciones académicas y profesionales. d.Identificación adicional a la cedula de ciudadanía. e.Solicitud de Antecedentes emitidos por Procuraduría General de la Nación, Contraloría General de la Nación, Policía Nacional f.Otros requerimientos solicitados por el área de Talento Humano y a su vez por la Gobernación del Cauca. **Observación:** dado que no se cumpla con los requisitos válidos para realizar la posesión del cargo, debe continuar el procedimiento con la asignación a el próximo postulante.	**Implementa** Oficina de Talento Humano-Técnico Admin o Prof. Universitario. **Aplica control** Oficina de Talento Humano-Prof. Universitario	I, II, III, IV y V	Notificación al postulante	A.7.1.1 Selección	

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 1 VINCULACIÓN LABORAL.							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
	Aseguramiento de que el personal a contratar tiene la competencia necesaria para desarrollar su rol en seguridad.	Sensibilizar al postulante referente al cumplimiento de las leyes, normas y códigos éticos, donde los empleados de la Gobernación del Cauca deben garantizar sus capacidades para tomar posesión del cargo, responsabilidades y rol a desempeñar, considerando la legislación relativa a la privacidad y seguridad de la información, protección de datos personales y legislación laboral. Garantizar conocimiento en herramientas de ofimática. **Observación:** en caso de que no se sensibilice al postulante y/o este mismo no esté de acuerdo con lo establecido para garantizar la seguridad de la información, debe continuar el procedimiento con la notificación a la Oficina de Talento Humano para asignación al siguiente postulante.	**Implementa** Oficina de Talento Humano-Prof. Universitario. **Aplica control** Oficina de Gestión tecnológica- Prof. Universitario.	II, III, IV y V	Registro de sensibilización	A.7.2.2 Toma de conciencia	
Los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como	Términos y Condiciones. (Datos Personales)	La Gobernación del Dpto. del Cauca, actuará como responsable del tratamiento de sus datos personales y hará uso de los mismos únicamente para las finalidades para las que se encuentra facultado, especialmente las señaladas en el título "Modo en que se utiliza la información" de la presente política y sobre la base de la ley y la normatividad vigente. Dando cumplimiento a la Ley 1581 de 2012 y al Decreto 1377 de 2013. **Observación:** en caso de que el postulante no esté de acuerdo con lo establecido en el contrato, debe continuar el procedimiento asignando al siguiente postulante.	**Implementa** Oficina de Talento Humano- Prof. Universitario. **Aplica control** Oficina de Gestión tecnológica-Prof. Universitario.	II, III, IV y V	Contrato formal-Acto administrativo	A.7.1.2 Términos y condiciones del empleo	7.1 Antes del empleo. 7.1.2 Términos y condiciones

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 1 VINCULACIÓN LABORAL.							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
hacia la organización.	Firma del acuerdo de confidencialidad - Responsabilidades y los derechos legales de los empleados y contratistas	Se realiza la aclaración de funciones y firma del acuerdo de confidencialidad de la Gobernación del Departamento del Cauca, donde la dependencia de Gestión Tecnológica esclarecer las cláusulas de uso y manipulación de activos de la información; además de software y hardware relacionados con las diferentes dependencias y oficinas. dando cumplimiento a los derechos de propiedad intelectual que defina el uso legal de los productos software y de los de información; b) adquirir software únicamente a través de las fuentes conocidas y de confianza para garantizar que no se infringen los derechos de autor; c) mantener el conocimiento de las políticas de protección de los derechos de propiedad intelectual y notificar la intención de aplicar medidas disciplinarias a cualquier miembro del personal que quebrante dichas políticas; d) mantener registros adecuados de los activos e identificar todos los activos que requieran la protección de los derechos de propiedad intelectual; e) mantener pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.; f) implementar controles para garantizar que no se excede el número máximo de usuarios permitidos por la licencia; g) llevar a cabo comprobaciones de que sólo se instala software autorizado y productos licenciados; h) disponer de una política para mantener las condiciones de las licencias en forma adecuada; i) disponer de una política para eliminar el software o	**Implementa** Oficina de Talento Humano-Prof. Universitario. **Aplica control** Oficina de Gestión tecnológica-Prof. Universitario.	II, III, IV y V	Acuerdo de confidencialidad		

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 1 VINCULACIÓN LABORAL.							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
		para transferirlo a un tercero cuando cese su uso; j) cumplir las condiciones contractuales del software y de la información que se obtenga de redes públicas; l) No copiar parcial o totalmente libros, artículos, informes u otros documentos salvo lo que permita la ley de derechos de autor.					
	Organización de documentación sobre tratamiento de datos personales	Se organizan y se folian los documentos acorde a la normatividad en materia archivística	**Implementa** Archivo-Técnico Administrativo **Aplica control** Archivo-Prof. Universitario	I, II, III, IV y V	Folio de control de personal	Procedimiento de la entidad	Procedimiento de la entidad

Tabla 10. Procedimiento de Seguridad del Recurso Humano-Etapa 1: Vinculación Laboral.

Fuente propia

La vinculación laboral se inicia en la oficina de Talento Humano por medio de la convocatoria de empleo donde al ser asignados los postulantes a las bacantes, se investigan los antecedentes proporcionados por los mismos; y donde dado el caso en que no cumplan con los requerimientos, se procederá a investigar el siguiente postulante, de lo contrario se le notificará y sensibilizará. Continuando con el procedimiento una vez el postulante asista a la sensibilización se debe acordar entre la oficina de talento humano y el postulante los términos y condiciones del contrato para posteriormente firmar el acuerdo de confidencialidad. Documentación por la cual la división de archivo abrirá el folio de documentación del funcionario y/o contratista que ingresa (Figura 12). Cabe resaltar que el acuerdo de confidencialidad es una herramienta que soporta las obligaciones que deben cumplir los funcionarios y/o contratistas desde el momento en que inician operaciones laborales en la entidad; el documento fue elaborado, plasmando las principales necesidades de la entidad respecto al manejo de activos de información.

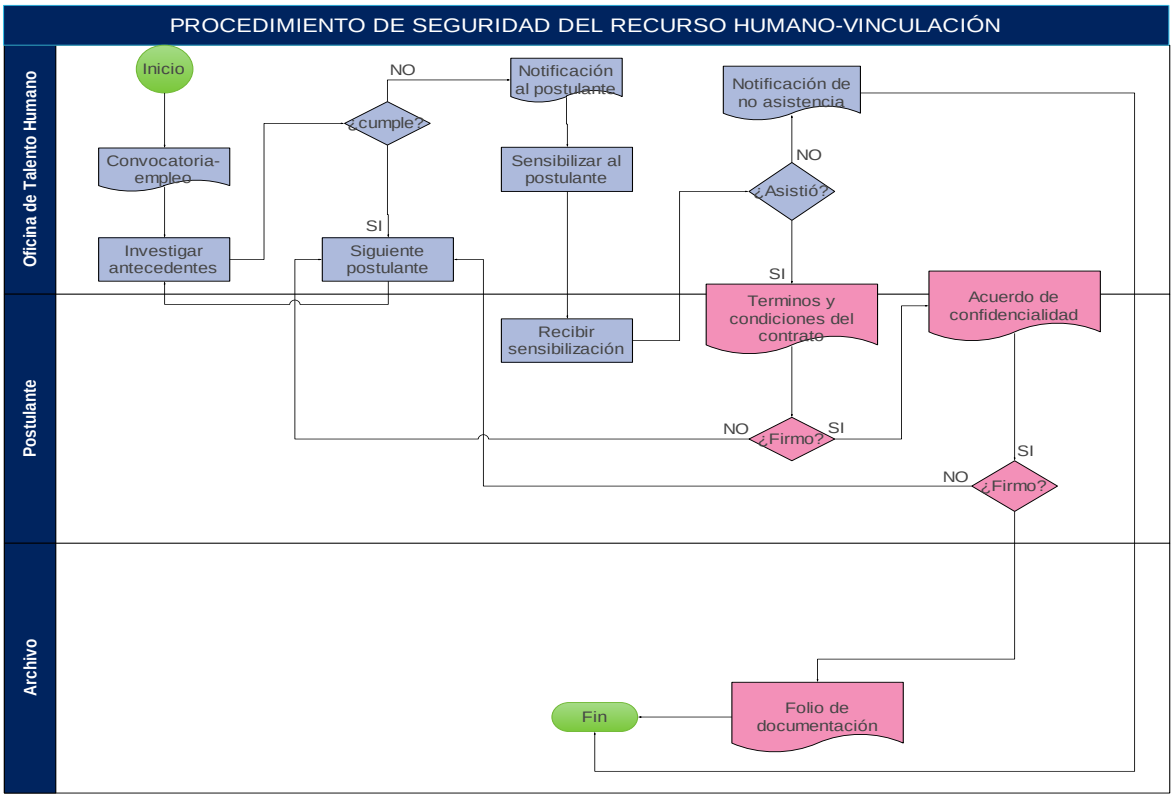


Figura 12. Diagrama de Procedimiento de Seguridad de Recurso Humano-Vinculación Laboral. Fuente propia.

2.2.2. Etapa 2: Procedimiento de Sensibilización y capacitación

El procedimiento de sensibilización y capacitación del personal contiene las actividades pertinentes a las herramientas de aprendizaje lúdico en las cuales se pone a disposición de la Gobernación del Cauca la información que concierne al buen manejo de los activos asociados con información e instalaciones de procesamiento de información de información en busca de la seguridad y privacidad de la información.

- **Sensibilización del personal**

La capacitación en seguridad de la información para la Gobernación del departamento del Cauca para los funcionarios y/o contratistas es de vital importancia, debido a que la información, es uno de los activos con mayor valor que tiene la entidad. Se indicará la metodología para concientización y capacitación del personal respecto al manejo de los activos de información, con el fin de mitigar el peligro latente de sufrir la pérdida de datos y afrontar sus consecuencias. La capacitación en seguridad y privacidad de la información refiere a dar a conocer y educar sobre la materia. La concientización implica algo un tanto más profundo y que deviene de una capacitación bien ejecutada, según los parámetros señales en el Modelo de Seguridad y Privacidad de la Información.

Cuando un empleado está consciente del efecto de sus acciones en la seguridad de su empresa indica que realmente ha arraigado toda la serie de conceptos que le fueron enseñados y que entiende a cabalidad lo que debe y no debe hacer [37].

Para realizar el procedimiento de sensibilización y capacitación del personal se toman en cuenta los riesgos más prominentes a los cuales está expuesta la entidad:

- Administración de contraseñas
- Uso y manejo de inventario
- Malware y sus diferentes tipos Software (Permitido/Prohibido) en la entidad
- Políticas organizacionales
- Relacionadas con seguridad de la información
- Uso de dispositivos de la entidad fuera de las instalaciones
- Uso de correo electrónico e identificación de correos sospechosos
- Seguridad en el puesto de trabajo
- Uso apropiado de internet

- Temas de control de acceso a los sistemas (privilegios, separación de roles)
- Política de escritorio limpio ingeniería social
- Sanciones por incumplimiento de las políticas
- Gestión de incidentes (como reportar, que puedo reportar)

Según lo anteriormente descrito, se indica la metodología a emplear (Tabla 5), que consiste en:

✓ Identificar ideas clave.
✓ Planificar charlas y capacitaciones.
✓ Realizar talleres de carácter evaluativo como indicador de eficacia.

.

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 2 CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	Identificar ideas clave para fortalecer sensibilización.	Realizar evaluación de la sensibilización y capacitación actual con el propósito de identificar falencias en su implementación e identificar nuevos temas de sensibilización y capacitación y plantear los objetivos de las sesiones, así como la duración de las mismas.	**Implementa** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica control** Oficina de Gestión Tecnológica-Prof. Universitario	III, IV y V	Plan de sensibilización y capacitación.	A.8.2.1 Clasificación de la información.	7. 2 Durante el empleo
	Planificar la elaboración de distintas capacitaciones y conferencias en temas de seguridad y privacidad de la información.	La sensibilización y capacitación del personal debe contener: a) la expresión del compromiso de la Dirección con la seguridad de la información en toda la organización; b) la necesidad de conocer y cumplir con las normas y obligaciones aplicables en seguridad de la información, según se define en las políticas, normas, leyes, reglamentos, contratos y acuerdos; c) la responsabilidad personal por las propias acciones y omisiones, y las responsabilidades generales relativas a asegurar o proteger la información que pertenece a la organización y a terceras partes; d) los procedimientos básicos de seguridad de la información (tales como la notificación de incidentes de seguridad de la información) y los controles básicos (tales como la seguridad de las contraseñas, los controles de software malicioso (malware) y mesas despejadas); e) los puntos de contacto y los recursos de información y consejos adicionales sobre cuestiones de seguridad de la información, que incluyan materiales adicionales para profundizar	**Implementa** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica control** Oficina de Gestión Tecnológica-Prof. Universitario	III, IV y V			7. 2 Durante el empleo 7.2.2 Concienciación, educación y capacitación en seguridad de la información

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 2 CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
		en la capacitación y formación en seguridad de la información.					
	Presentación del código de conducta para la seguridad y privacidad de la información	La Gobernación del Departamento del Cauca en consideración con el Código de Integridad de función pública toma como referencias de este, los 5 valores (Honestidad, respeto, compromiso, respeto, diligencia y justicia) que guían las acciones de los funcionarios con el fin de promover relaciones sólidas con un buen ambiente laboral de trabajo. En relación con la dependencia de Gestión Tecnológica se toman como base los lineamientos Ref. Código de Buen Gobierno MinTIC. Por lo anterior: Solicitar al funcionario o contratista estar enterado del Código de Integridad para funcionarios públicos en los numerales referentes a los procedimientos de seguridad y privacidad de la información.	**Implementa** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica control** Oficina de Gestión Tecnológica-Prof. Universitario	II, III, IV y V	Registro de entrega de código de conducta	A.8.2.2 Educación, formación y concientización sobre la seguridad de la información	7. 2 Durante el empleo
	Realización de taller como evaluación de resultados	La sensibilización y/o capacitación que se realice al interior de la entidad debe mostrar indicadores válidos de la actividad, con el fin de evaluar el cumplimiento de los objetivos propuestos. Los talleres permiten evaluar de manera dinámica y didáctica, las falencias y fortalezas en cada tema expuesto (Al final del taller deben recogerse todos los carteles, fichas y materiales implementados ya que reúnen información valiosa).	**Implementa** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica control** Oficina de Gestión Tecnológica-Prof. Universitario	II, III, IV y V	Evaluación de taller	A.8.2.2 Educación, formación y concientización sobre la seguridad de la información	7. 2 Durante el empleo

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION RELACIONADA AL RECURSO HUMANO-ETAPA 2 CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	Se debe contar con un proceso formal, el cual debe ser comunicado a todos los funcionarios y/o contratistas, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	El proceso disciplinario no debe iniciar sin una previa verificación de que se ha producido una violación de la seguridad El proceso disciplinario formal debería proporcionar una respuesta gradual que tenga en cuenta factores tales como la naturaleza y gravedad de la violación de la seguridad y su impacto en la entidad, si es la primera vez o se trata de una infracción repetida, si el causante fue adecuadamente formado, o no lo fue, en la legislación aplicable, los compromisos de la entidad u otros factores según sea necesario.	**Implementa** Oficina de Asesora de Jurídica. **Aplica control** Oficina de Asesora de Jurídica.	II, III, IV y V	Folio de investigación	A.8.2.3 Proceso disciplinario	7.2.3 Proceso disciplinario

Tabla 11. Procedimiento de Seguridad del Recurso Humano- Etapa 2: Capacitación y Sensibilización.

Fuente propia.

Dando continuidad al procedimiento de seguridad del recurso humano, en su segunda etapa de capacitación y sensibilización, ésta, parte de la identificación de las ideas por parte de la oficina de Talento Humano para lograr tener el cronograma que permita que los funcionarios y/o contratistas reciban la capacitación y sensibilización. En esa actividad se debe proporcionar al funcionario y/o contratista el manual de conducta digital que proporciona los lineamientos necesarios para el cuidado de los activos de información; y de esa manera realizar el taller evaluativo que brinda indicadores de falencias y fortalezas de la entidad (Figura 13).

Por otro lado, si la oficina asesora de jurídica tiene la leve sospecha de una infracción a las políticas de seguridad de la información, debe en primer lugar cerciorarse de la falta cometida y una vez se compruebe, llevar a cabo la apertura del proceso disciplinario y folio de la investigación oficial (Figura 13).

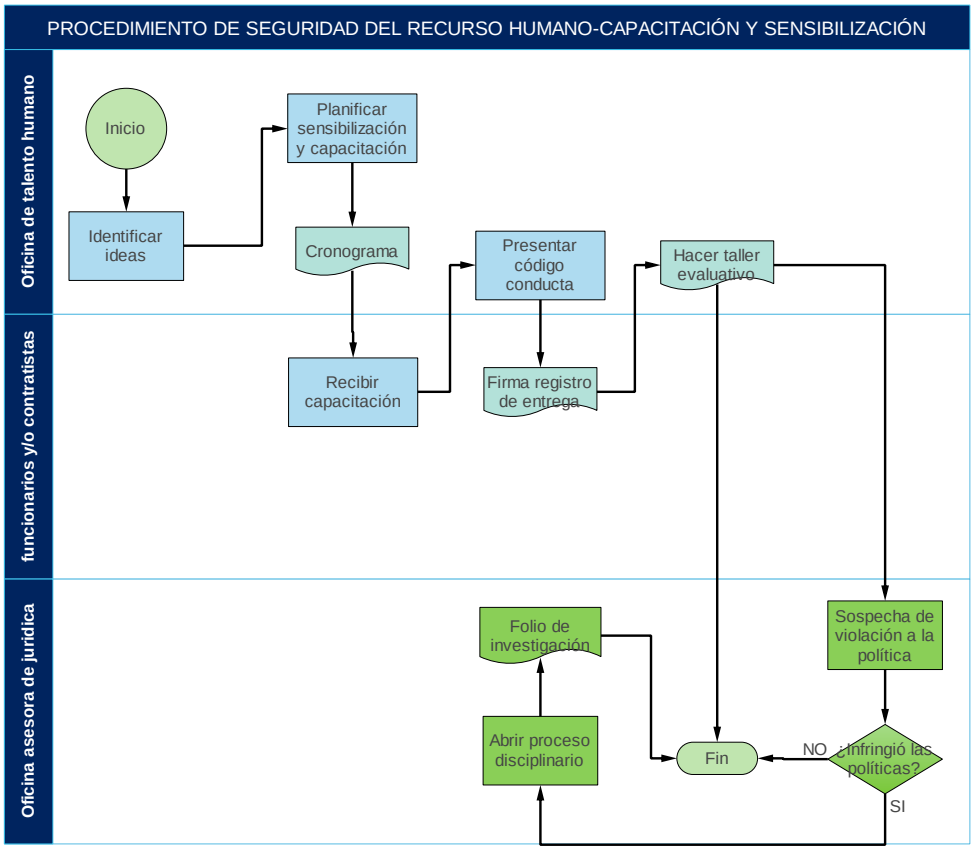


Figura 13. Diagrama-Seguridad del Recurso Humano-Capacitación y Sensibilización.
Fuente propia.

2.2.3 Etapa 3: Procedimiento de Desvinculación del personal

En la tercera fase se indican las actividades para desvincular o cambiar de cargo, al personal de la Gobernación del Cauca, teniendo en cuenta actividades que deben ser de obligatorio cumplimiento.

Las actividades de obligatorio cumplimiento se estipulan con el fin de mitigar los riesgos de pérdida de información por mal manejo de los activos de información [37].

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN-RECURSHO HUMANO ETAPA 3: DESVINCULACIÓN LABORAL							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
La Gobernación del Departamento del Cauca debe garantizar que las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se comuniquen al empleado o contratista y se cumplan.	Las responsabilidades y funciones que son válidas después de la finalización del empleo deben reposar en los contratos de los empleados o contratistas	La comunicación de la revisión de cumplimiento de las responsabilidades en el cese debería incluir los requisitos de seguridad y las responsabilidades legales en curso, y cuando sea apropiado, las responsabilidades que conlleven algún acuerdo de confidencialidad, así como los términos y condiciones del empleo que continúen vigentes durante un periodo definido después de la finalización del contrato del empleado o del contratista	**Implementa** Oficina involucrada. **Aplica control** Oficina de Talento Humano.	II, III, IV y V	Contrato vigente del funcionario	A.8.3.1 Responsabilidades en la terminación	7.3 Finalización del empleo o cambio en el puesto de trabajo.
	Entrega formal de los activos de información tangibles e intangibles a su cargo.	Cuando se realice el procedimiento de desvinculación, solicitar al funcionario y/o contratista la entrega formal de equipos, dispositivos, archivos de información, documentos, registros y demás a la respectiva dependencia, mediante un informe completo que exprese el estado de entrega de los activos y manejo de herramientas. **Observación:** si el empleado no realiza la entrega formal del informe con el resumen de la información manipulada, no se le otorgará la constancia laboral respectiva.	**Implementa** Oficina involucrada. **Aplica control** Oficina de Talento Humano- Control interno disciplinario.	II, III, IV y V	Paz y salvo	A.8.3.2 Devolución de activos	

Tabla 12. Procedimiento de Seguridad del Recurso Humano- Etapa 3: Desvinculación Laboral. Fuente propia

Como última etapa, la desvinculación laboral se genera a partir de la revisión del cumplimiento del contrato vigente, donde posteriormente el funcionario y/o contratista debe realizar un informe completo de la manipulación de los activos de información a su cargo (como se recibió y como se entrega) y proporcionarlo a su líder de oficina, quien dará el visto bueno y notificará si se le otorga o no el paz y salvo, donde en caso de que sea negativa la notificación la oficina de control interno deberá realizar la investigación de los datos faltantes (Figura 14).

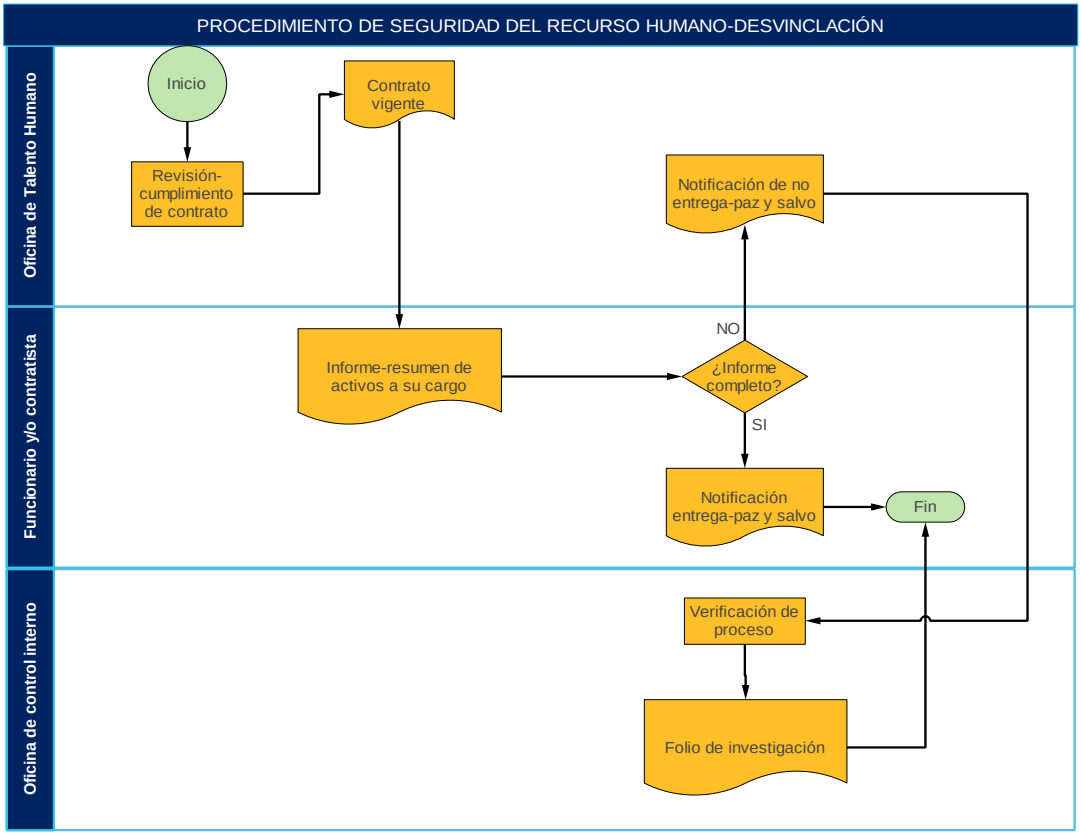


Figura 14. Diagrama-Seguridad del Recurso Humano-Desvinculación. Fuente propia.

2.3 Gestión de Activos-A.8 ISO 27001

La caracterización de activos de información, permite clasificar los mismos según el nivel de protección que requieran, pues identifica claramente Responsabilidad por activos, clasificación de la información, manejo de medios. Las acciones realizadas para el inventario de activos corresponden a definición, revisión, actualización y publicación. Regidos por normatividad establecida por el Ministerio de la Tecnologías de la Información y Comunicación, se ha definido el procedimiento de clasificación de activos de la información de la Gobernación del Departamento del Cauca, estipulando su grado de confidencialidad, integridad y disponibilidad basados en la NTC/IEC ISO 27002 – 27001, numerales A.8 y 8 Gestión de activos de información y las consecuencias que traería consigo la pérdida y manipulación inapropiada de los mismos.

Se establece procedimientos de gestión de activos de información para la Gobernación del Departamento del Cauca, dando cumplimiento a normas de calidad conexas a las tecnologías de la información y comunicación; además, con base a los niveles y criterios definidos en las políticas del MinTIC, con estas características se fija el formato de procedimientos para la gestión de activos información, donde se describen las definiciones, actividades y tareas; al igual que los registros y la información generada dentro del procedimiento, con el propósito de establecer actividades puntuales para dar cumplimiento al Modelo de Seguridad y Privacidad de la Información (MSPI). La distribución del formato se implementa a partir de la Guía N° 3 - Procedimientos de Seguridad de la Información del MSPI otorgados por el MinTIC; la siguiente descripción muestra las actividades a realizar y tener en cuenta para realizar el procedimiento de gestión de activos a nivel general al interior de la entidad.

El procedimiento de gestión de activos de información específica el paso a paso para obtener la identificación, clasificación e inventariado de los activos de información de la Gobernación del Departamento del Cauca. De esta manera se logra el tratamiento requerido y la protección adecuada en cumplimiento de la misión y los objetivos institucionales. Quien encabeza el levantamiento, mantenimiento, clasificación y

publicación de la información será liderado por las siguientes oficinas: Oficina de asesoría Jurídica, Archivo central, Oficina de Planeación Departamental y Oficina de Gestión de Tecnologías, Servicio al Ciudadano [38].

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN-GESTIÓN DE ACTIVOS							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar identificados y debería elaborarse y mantenerse un inventario.	Inventario del activo de información	**1.** Asignación de identificador: es el código consecutivo con el cual se puede llevar el conteo de los activos de información (Nomenclatura disponible en el numeral XXX). **2.** Nombrar la categoría de la información: conjunto de unidades de información de contenidos semejantes, creadas por una misma dependencia o sujeto como consecuencia del ejercicio de sus funciones específicas. **3.** Nombrar el activo de información: definir el título, palabra y/o frase con la que se da a conocer el activo de información. **4.** Descripción del activo de información: breve descripción de la función del activo de información. **5.** Medio de conservación y/o soporte: es el medio en que se encuentra la información, que puede ser entre las siguientes: • Físico / Electrónico: En caso de encontrarse almacenada en los dos medios. **6.** Determinación del formato: Determinar la forma, tamaño o modo en la que se presenta la información, tales como: •Medio Digital (E-mail, formularios digitales, Hojas de Cálculo) •Documento de texto (Word, pdf, txt, entre otros) •Medio magnético (usb, cd) •Presentaciones •Imágenes •Audio **7**. Disponibilidad del tipo de activo: Definir la forma en la que se encuentra la información que puede ser de carácter: •Información privada •Información publicada **8.** Categorización: Determinar la categoría del activo de información. **9.** Proporcionar la fecha de generación: identificar la fecha de la creación y recepción de la información.	**Implementa**-Almacén y Oficina de Gestión Tecnológica-Técnico Admin o Prof. Universitario. **Aplica Control**-Oficina de Gestión Tecnológica- Técnico Admin o Prof. Universitario.	III y IV	Base de datos-activos de información	A.8.1.1 Inventario de activos	8. Gestión de Activos 8.1.1 Inventario de Activos

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN-GESTIÓN DE ACTIVOS							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
		10. Definir el lugar de consulta: definir donde se encuentra almacenada, publicada o disponible el activo de información. **11.** Descripción del Proceso(s) que produce la información y su respectivo nombre: breve descripción del proceso creado y definir el nombre del proceso. **12.** Frecuencia de Actualización: dato que se solicita para determinar la periodicidad con que se actualiza la información.					
El activo de información debe ser clasificado en términos de la importancia de su revelación frente a requisitos legales, confidencialidad, disponibilidad, integridad y criticidad ante revelación o modificación no autorizadas.	Calificar el grado de confidencialidad (Tabla 15)	Calificar el activo de información en términos de confidencialidad entendiendo que éste, no se debe poner a disposición ni se debe revelar a individuos, entidades o procesos no autorizados.	**Implementa-** Almacén Y oficina de Gestión Tecnológica- Prof. Universitario. **Aplica Control**- Oficina de Gestión Tecnológica-Prof. Universitario.	III y IV	Base de datos- activos de información	A.8.2.1 Clasificación de la información	8.2.1 Clasificación de la información
	Calificación de Integridad (Tabla 16)	Calificar el activo de información en cuanto a la integridad, mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.					
	Calificar la disponibilidad (Tabla 17)	Calificar el activo de información, en términos de disponibilidad, de acuerdo a la importancia que tiene en cuanto a este componente.					
	Asignación de nivel de Criticidad (Tabla 18)	Esta casilla no debe ser diligenciada por el usuario, corresponde al resultado final de la calificación de los criterios de confidencialidad, integridad y disponibilidad de la información.					
Todos los activos que figuran en el inventario deben tener un propietario	Responsable de la producción de la Información o Propietario	Nombre de la dependencia y/o funcionario que creo la información o que recibe el equipo. En caso de que sea un dispositivo o equipo debe relacionarse el nombre de quien lo manipulará y la dependencia donde va a reposar.	**Implementa**- Almacén- Técnico Admin o Prof. Universitario. **Aplica Control-** Oficina de Gestión Tecnológica- Prof. Universitario.	III y IV	Base de datos- activos de información	A.8.1.2 Propiedad de los activos	8.1.2 Propiedad de los activos

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN-GESTIÓN DE ACTIVOS							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Capacitación de usuarios para manejo óptimo de sistemas de info, aplicaciones, equipos, entre otros.	Capacitar usuarios	Realizar capacitaciones a usuarios de los sistemas de información, bases de datos, sistemas operativos, aplicaciones y software. Éstas se realizarán de acuerdo a los requerimientos de los servidores públicos y plan de capacitación. **Observación:** si el funcionario no recibe la capacitación necesaria no puede hacer uso de ningún activo de información con el fin de mitigar daños en los mismos.	**Implementa**-Personal interno capacitado o personal externo del proveedor. **Aplica Control**-Oficina de Gestión Tecnológica-Prof. Universitario.	II, III, IV y V.	Registro de capacitación	Procedimiento vigente-Gestión y administración de sistemas de información	
La Gobernación del Dpto. del Cauca debe mantener un uso correcto de los activos de información manipulados.	Operatividad de los Sistemas de Información	Mantener en normal funcionamiento y en óptimas condiciones de seguridad los sistemas de información, aplicaciones, sistemas operativos, software y bases de datos por parte del rol Administrador de la Entidad.	**Implementa-**Oficina de Gestión Tecnológica-Técnico Admin o Prof. Universitario. **Aplica Control**-Oficina de Gestión Tecnológica- Técnico Admin o Prof. Universitario.	II, III, IV y V.	Control de mantenimiento	Procedimiento vigente-Gestión y administración de sistemas de información	
	Obsolescencia del sistema de información	El Administrador del activo de Información, realizará el reporte y la justificación al Líder de la Oficina de Gestión Tecnológica de los sistemas de información, aplicaciones, sistemas operativos, software y bases de datos que están en estado inactivo para realizar el proceso de baja con el Almacén General. **Observación:** la oficina de G.T. realizara la revisión del reporte de baja, si es correcto se registrará, de lo contrario, debe realizarse de nuevo la solicitud.	**Implementa-** Almacén y Oficina de Gestión-Tecnológica- Técnico Admin o Prof. Universitario. **Aplica Control**-Oficina de Gestión Tecnológica- Técnico Admin o Prof. Universitario.	II, III, IV y V.	Registro de bajas	Procedimiento vigente-Gestión y administración de sistemas de información	

Tabla 13. Procedimiento de Gestión de activos de información. Fuente propia.

Teniendo en cuenta, que debe brindarse seguridad de la información a los activos tangibles e intangibles, el procedimiento de gestión de activos de información parte del inventario de los activos que reposan en una base de datos administrada por el Almacén de la entidad; a su vez, son clasificados respecto a confidencialidad, disponibilidad, integridad y criticidad; continuando con la asignación del propietario responsable del activo. Una vez sea entregado el activo de información, la oficina de gestión tecnológica debe capacitar sobre el manejo del activo al funcionario y verificar que si comprende la actividad.

Por otro lado, en la revisión periódica el funcionario y/o contratista a cargo del activo debe reportar si está dando el adecuado manejo o si el equipo necesita ser dado de baja.

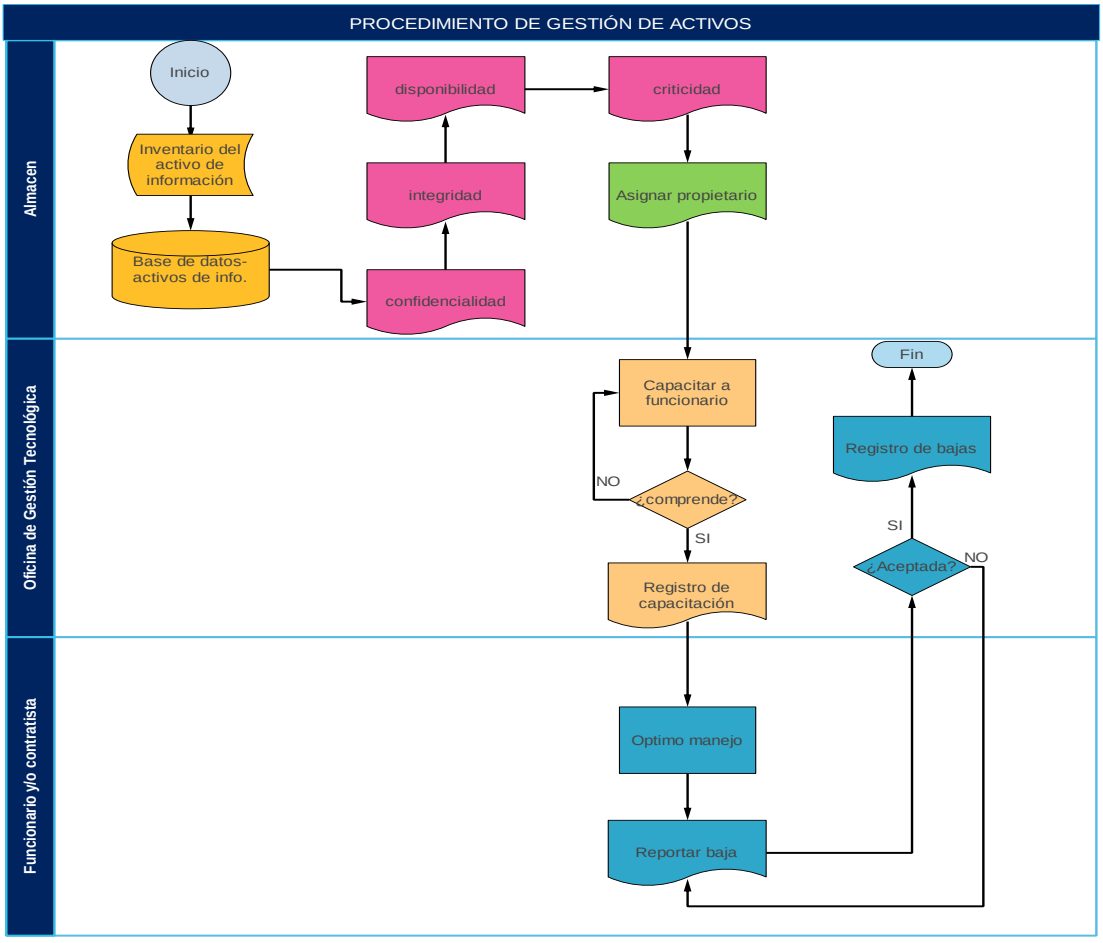


Figura 15. Diagrama procedimiento de Gestión de activos. Fuente propia.

2.3.1 Nomenclatura

La nomenclatura presentada se realiza con el fin de dar un identificador a los activos de información de manera que su lectura, asignación y reconocimiento sea trivial para quien los maneje, los servicios se clasificaron según la nomenclatura de Magerit que corresponde a un anexo de la metodología elaborada por el Consejo Superior de Administración Electrónica por la Agencia Europea de Seguridad de la Información.

Nomenclatura	Tipo de Activo	Descripción
S	Servicio	Función que satisface una necesidad de los usuarios
INT	Servicio Interno	Usuarios y medios de la propia organización
EXT	Servicio Externo	se presta a usuarios externos bajo relación contractual
PUB	Servicio Público	Prestado al público en general
WWW	Word Wide Web	Página Web
EMAIL	Correo Electrónico	Correo electrónico institucional
FILE	Almacenamiento de Ficheros	Archivos almacenados en una estructura jerárquica
DIR	Servicio de Directorio	Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado.
IDM	Gestión de Identidades	Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto la organización.

Tabla 14. Nomenclatura para clasificación de activos de información. Fuente: Gobernación del dpto. del Cauca. Fuente propia.

2.3.2 Categorización

Con el propósito de describir la naturaleza del activo de información para llevar a cabo una correcta gestión de activos de información:

- **Recursos de Información:** Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- **Recursos de Software:** Que pueden ser Físicos o digitales como: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- **Activos Físicos:** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos, switches, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, entre otros), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, entre otros [36].

- **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

- **Clasificación:** Es la calificación que le da la entidad, de acuerdo a la clasificación adoptada.

2.3.3 Atributos de los activos de información en cuanto a seguridad de la información:

Esta actividad se realiza con el fin de que los activos de información reciban el nivel de protección adecuada, de acuerdo con su clasificación, esta se realiza con base en los atributos de Confidencialidad, Integridad y Disponibilidad de la Información teniendo en cuenta la importancia del activo y su criticidad en los procesos o frente a la Gobernación del Departamento del Cauca, estos valores se calculan automáticamente, de acuerdo a las Tablas 15, 16 y 17 –Criterios de Confidencialidad, Integridad y Disponibilidad, respectivamente para dar una clasificación de criticidad respecto a lo anterior (Tabla 18).

En cumplimiento de las actividades anteriormente descritas se revelan los criterios necesarios para cumplirlas de manera satisfactoria, en relación con la clasificación de los activos teniendo en cuenta que se rige por las 3 características principales de privacidad y seguridad de la información, confidencialidad, integridad y disponibilidad [39].

Criterios de Confidencialidad		
Información	Individuo, entidad o proceso no autorizado accede al activo de información	
Hardware	Alguien conoce que existe el elemento o su configuración o accede al activo sin autorización.	
Software	Individuo, entidad o proceso no autorizado conoce la existencia o parametrización del activo	
Servicio	Alguien conoce su existencia o configuración o hace uso no autorizado del activo.	
Persona	Se hace uso inadecuado de la información privilegiada a la cual se tiene acceso por cargo o función que desempeña	
Descripción	**Criterio**	**Definición**
Alto	A	Conocimiento o divulgación no autorizada del activo impacta de manera negativa la imagen y el personal de la Gobernación del Cauca.
Medio	M	El conocimiento o divulgación no autorizada de la información que gestiona este activo puede tener consecuencias moderadas que a corto plazo pueden perjudicar e impactar de manera negativa la misión y objetivos institucionales de la Gobernación del Departamento del Cauca.
Bajo	B	El conocimiento o divulgación no autorizada de la información puede ocasionar un impacto pequeño o inexistente al este activo y puede impactar de manera negativa la misión y los objetivos institucionales.

Tabla 15. Criterios de confidencialidad. [39]

Criterios de Integridad		
Información	Se pierde la completitud, exactitud o precisión del activo de información	
Hardware	El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente	
Software	Se valora la completitud, exactitud o precisión de la parametrización del activo.	
Servicio	Se valora la completitud, exactitud o precisión del servicio	
Persona	La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempeñar el rol o función.	
Descripción	Criterio	Definición
Alto	A	La pérdida de exactitud y estado completo del activo impacta negativamente la prestación del servicio de la Gobernación del Cauca.
Medio	M	La pérdida de exactitud y estado completo del activo impacta negativamente no sólo a la misión, si no los objetivos institucionales de la Gobernación del Departamento del Cauca.
Bajo	B	La pérdida de exactitud y estado completo del activo puede tener un impacto pequeño o inexistente.

Tabla 16. Criterios de Integridad. [39]

Criterios de Disponibilidad		
Información	No se puede acceder al activo de información por el personal que está autorizado.	
Hardware	No se puede acceder al activo de información por el personal que está autorizado	
Software	No se puede acceder al activo de información por el personal que está autorizado.	
Servicio	No se puede acceder al activo de información por el personal que está autorizado.	
Persona	La persona no se encuentra disponible para el proceso.	
Descripción	Criterio	Definición
Alto	A	La falta o no disponibilidad del activo de información impacta negativamente la prestación del servicio e impacta negativamente a la Gobernación del Cauca.
Medio	M	La falta o no disponibilidad del activo de información impacta negativamente los procesos de la Gobernación del Departamento del Cauca.
Bajo	B	La falta o no disponibilidad del activo de información puede tener un impacto pequeño o inexistente.

Tabla 17. Criterios de Disponibilidad [39].

Criterios de Criticidad	
Alto: A	Activo de información de altísima importancia para la gobernación del Dpto. del Cauca.
Medio: M	Activo de información que impacta de manera negativa ante una eventualidad, pero puede suplirse.
Bajo: B	Activo de información con bajo impacto ante eventualidades.

Tabla 18. Criterios de Criticidad. Fuente propia

2.4 Control de Acceso a Sistemas de Información-A.9 ISO 27001

Este documento se elabora en seguimiento de las políticas de seguridad de la información establecidas por la Oficina de Gestión Tecnológica de la Gobernación del Departamento del Cauca y basados en la norma NTC ISO-IEC 27001, control A.9 – Control de Acceso y la norma NTC ISO-IEC 27002, 9. Control de acceso, donde se plantean los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de los activos de información, en este caso las normas de calidad rigen los controles enfocados al control de acceso a los Sistemas de Información al igual

que a la Gestión de usuarios y contraseñas, para implementar buenas prácticas organizacionales respecto a estos mismos.

El procedimiento establecido tiene una relación directa con el control de acceso a los distintos sistemas de información que maneja la entidad, proporcionando las actividades paso a paso que deben realizar los funcionarios de acuerdo a sus funciones para un manejo óptimo de los Sistemas de información, la solicitud de acceso proveniente de las diferentes dependencias y el acceso a los mismos. El control de acceso a los sistemas de información es de vital importancia dentro de una entidad como la Gobernación del Cauca, motivo por el cual se deben implementar procedimientos que mitiguen riesgo de tipo físico y digital; como primera medida se emplean métodos preventivos contra ataques de fuerza bruta y en segunda medida ataques digitales, como filtración de información, modificación e interrupción son formas de perder información invaluable para la Gobernación del Cauca [41].

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN- CONTROL DE ACCESO							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
La oficina de Gestión Tecnológica solo puede proporcionar acceso a redes y a los servicios de red a usuarios que han sido específicamente autorizados.	Solicitud de servicios de red.	La solicitud de servicios de red, debe cumplir con las descripciones de las funciones a desempeñar con el fin de permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. **Observación:** si no se realiza la solicitud formal de los servicios de red de manera correcta, se rechazará la solicitud y no otorgaran accesos.	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control-**Oficina de Gestión Tecnológica--Prof. Universitario	IV	Formulario de solicitud de servicios de red	A.9 Control de acceso. A.9.1.2 Acceso a redes y a servicios de red.	9.1.2 Acceso a las redes y a los servicios de red
Implantar un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso y cancelación de los mismos.	Registro y cancelación de usuarios	Realizar un procedimiento formal de registro y de cancelación de registro de usuario, para posibilitar la asignación de los derechos de acceso a servicios de red.	**Implementa**- Oficina de Gestión Tecnológica--Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica--Prof. Universitario	IV	Registro de nuevo usuario-registro de cancelación de usuario	A.9.2.1 Registro y cancelación del registro de usuario	9.2.1 Registro y baja de usuario
Implantar un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas de información y servicios.	Solicitud de acceso a sistemas de información.	La solicitud de acceso a sistemas de información, debe cumplir con la descripción de las funciones a desempeñar para realizar la asignación de los mismos con el fin de gestionar el acceso a los Sistemas de Información dependiendo de la necesidad.	**Implementa-** Oficina de Gestión Tecnológica--Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica--Prof. Universitario	IV	Base de datos de acceso a sistemas de información	A.9.2.2 Suministro de acceso de usuarios	9.2.2 Provisión de acceso de usuario
Gestión de derechos de acceso privilegiado	Restringir y controlar la asignación y uso de derechos de acceso privilegiado, en caso de ser solicitado.	Debe establecerse un procedimiento formal de asignación y el uso de privilegios con el propósito de controlar los derechos de acceso a la información: derechos de acceso privilegiados debería estar controlada a través de un proceso formal de autorización de acuerdo con la política de control de	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica-Prof. Universitario	IV	Formulario de solicitud de acceso privilegiado	A.9.2.3 Gestión de derechos de acceso privilegiado	9.2.3 Gestión de privilegios de acceso

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN- CONTROL DE ACCESO							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
		acceso de la Gobernación del Dpto. del Cauca. Los siguientes pasos deberían ser considerados: a) Deben identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso, por ejemplo, sistema operativo, el sistema de gestión de base de datos y cada aplicación, junto con los usuarios a los que hay que asignarlos; b) los derechos de acceso privilegiados deben asignarse a los usuarios en base a la 'necesidad de uso' y caso a caso de acuerdo con la política de control de acceso, es decir, basados en los requisitos mínimos para el desempeño de sus funciones; c) deben mantenerse un proceso de autorización y registro de todos los privilegios asignados. Los derechos de acceso privilegiados no deberían concederse hasta que se complete el proceso de autorización; d) deben definirse los requisitos para el vencimiento de los derechos de acceso privilegiados; **Observación:** en caso de que la solicitud este diligenciada de manera incorrecta, debe volver a realizarse.					
El acceso a los sistemas y a las aplicaciones debe ser controlado por medio de un procedimiento seguro de inicio de sesión.	Ingresar de manera segura a los sistemas	Cuando se requiera una autenticación y verificación robusta de la identidad deberían usarse métodos de autenticación alternativos a las contraseñas, como por ejemplo, medios criptográficos, tarjetas inteligentes, dispositivos hardware o medios biométricos.	**Implementa**- Oficina de Gestión Tecnológica-Técnico Admin o Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica	III, IV y V	Registro de ingreso al sistema	A.9.4.2 Procedimiento de ingreso seguro	9.4.2 Procedimientos seguros de inicio de sesión

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN- CONTROL DE ACCESO							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	Gestionar contraseña	Un sistema de gestión de contraseñas debe: a) aplicar el uso de identificadores (ID) de usuario y contraseñas individuales para mantener la responsabilidad; b) permitir a los usuarios escoger y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada; c) imponer la selección de contraseñas de calidad; d) forzar a los usuarios a cambiar sus contraseñas tras el primer inicio de sesión; e) forzar los cambios regulares de contraseñas y bajo petición; f) mantener un registro de las contraseñas usadas anteriormente y evitar su reutilización; g) no mostrar las contraseñas en la pantalla cuando se estén introduciendo; h) almacenar los ficheros de contraseñas de manera separada de los datos del sistema de aplicación; i) almacenar y transmitir las contraseñas en forma protegida.	**Implementa**- Oficina de Gestión Tecnológica- Técnico Admin o Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica- Prof. Universitario	II, III, IV y V	Registro de contraseñas	A.9.4.3 Sistema de gestión de contraseñas	9.4.3 Sistema de gestión de contraseñas

Tabla 19. Procedimiento de Control de acceso.

Fuente propia.

En este caso el procedimiento de control de acceso es iniciado por el funcionario y/o contratista al tener la necesidad de solicitar los servicios de red de la entidad, donde la oficina de gestión tecnológica se encarga de revisar que la solicitud este diligenciada correctamente y asi proceder a incluir en la base de datos de accesos al funcionario que lo solicita. De esa misma manera se realiza para la solicitud de acceso a los sistemas de información y los accesos privilegiados. En cualquiera de los casos anteriores, se genera un registro de ingreso de usuario y contraseña. Lo anterior brinda soporte a las auditorias que se realicen como medida preventiva sobre los usuarios que intervienen en la entidad (Figura 16).

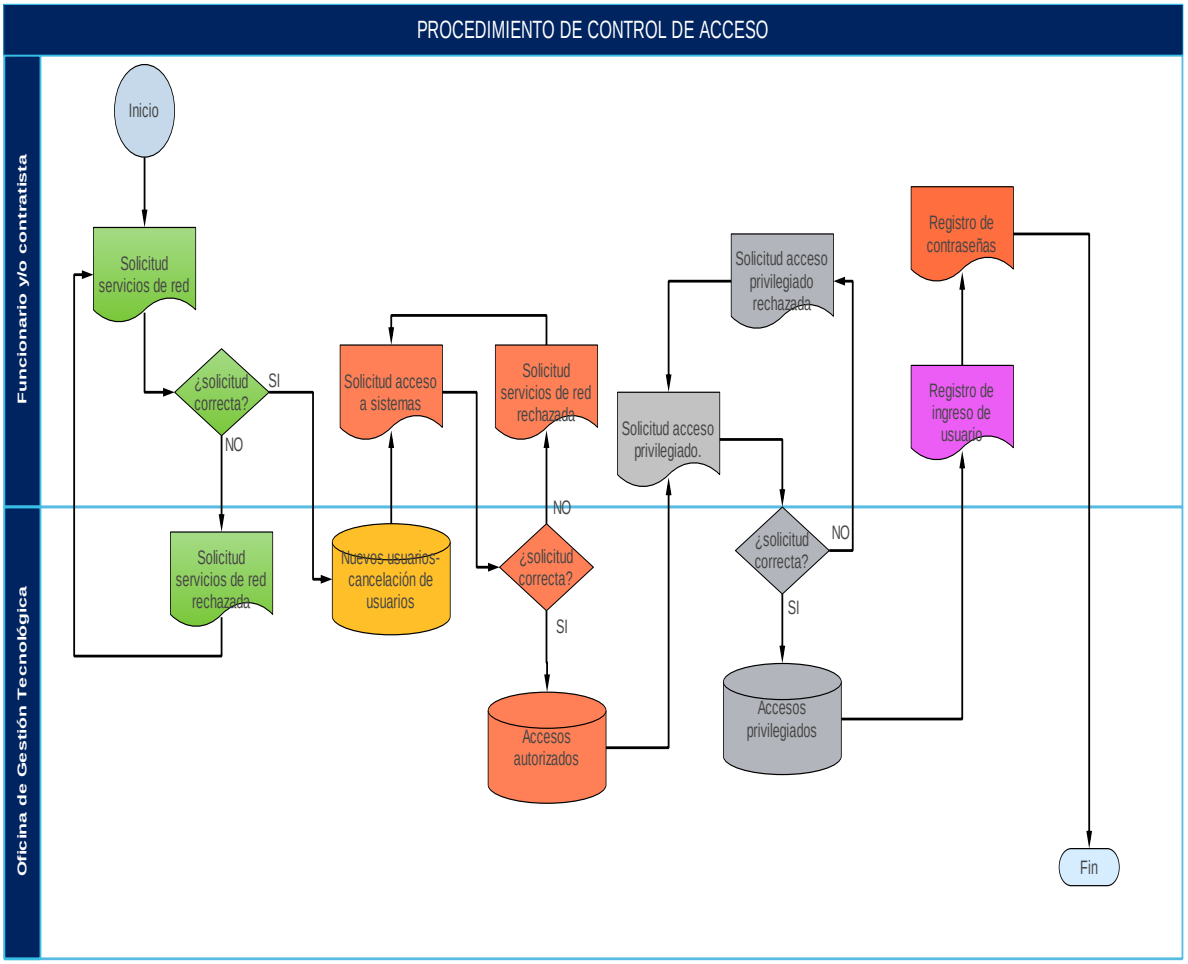


Figura 16. Diagrama Procedimiento de Control de Acceso. Fuente propia.

2.5 Criptografía-A.10 ISO 27001

El presente procedimiento en cumplimiento de los controles del numeral A.10. Criptografía de la norma NTC ISO/IEC 27001 y 10. Criptografía de la NTC ISO/IEC 27002 e ISO/IEC 11770 referentes a criptografía y a gestión de claves criptográficas respectivamente, presenta paso a paso la manera en que se implementan los controles criptográficos al interior de la Gobernación del Departamento del Cauca indistintamente de la dependencia y/o activo de información.

El objeto del procedimiento es estructurar la implementación de los controles y llaves criptográficas que implementen algún método de cifrado, con el fin de proteger la información y garantizar su privacidad, confidencialidad e integridad en el entorno que plantea el Modelo de Seguridad y Privacidad de la Información de la Guía N° 3 numeral 6.4 y con el cual se pretende encriptar los activos de información clasificados como confidenciales.

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACION-CRIPTOGRAFÍA							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	Desarrollo de la política criptográfica	Desarrollar en la política de seguridad respecto a criptografía el uso de la misma en toda la organización, incluyendo principios generales en base a los cuales debería protegerse la información de la Gobernación del Dpto. del Cauca. a) tomando como base la evaluación de los riesgos, debería identificarse el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido; b) el uso del cifrado para proteger la información sensible transportada a través de dispositivos móviles o extraíbles o a través de líneas de comunicación; c) el enfoque de la gestión de las claves, incluyendo los métodos para ocuparse de la protección de las claves criptográficas y la recuperación de la información cifrada en caso de pérdida, vulneración o daño de las claves; d) las funciones y responsabilidades; es decir, quién es responsable de: 1) la implantación de la política. 2) la gestión de las claves, incluyendo la generación de las mismas.	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control-** Oficina de Gestión Tecnológica y Oficina de Gestión Organizacional-Prof. Universitario	IV	Política de criptografía	A.10.1 Controles criptográficos. A.10.1.1 Política sobre uso de controles criptográficos	10.1.1 Política de uso de los controles criptográficos.
	Control de herramientas de encriptación	Las herramientas de encriptación deben mantener los requisitos de seguridad de la información. a) confidencialidad: uso del cifrado de la información para proteger información sensible o crítica, tanto si ésta se almacena como si se transmite; b) integridad/autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para verificar la autenticidad o la integridad de la información sensible o crítica que se almacene o se transmita por parte de la Gobernación del Dpto. del Cauca. c) no repudio: uso de técnicas criptográficas para obtener pruebas de la existencia o inexistencia de un evento o una acción. d) autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que soliciten acceso a, o transacciones con,			Registro de control	A.10.1.2 Gestión de llaves	10.1.2 Gestión de claves

		usuarios, entidades y recursos de los sistemas de información que emplea la Gobernación del Dpto. del Cauca.					
Desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	El sistema de gestión de claves debe basarse en un conjunto consensuado de normas, procedimientos y métodos seguros.	La política debe incluir los requisitos de gestión de las claves criptográficas en todo su ciclo de vida incluyendo la generación, almacenamiento, archivo, recuperación, distribución, retirada y destrucción de las mismas.	**Implementa**-Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica y Oficina de Gestión Organizacional-Prof. Universitario	IV	Registro de implementación de herramientas criptográficas	A.10.1.2 Gestión de llaves	10.1.2 Gestión de claves
	Generación de nueva clave para cifrado	La clave de cifrado proporcionada para uso de herramienta, debe ser solicitada y establecida por el usuario en caso de olvidar la clave, la información cifrada no es recuperable.			Base de datos-registro de nuevas claves		
	Generación de nuevo certificado para cifrado	La protección de los activos de información involucra generar y obtener certificados de clave pública.			Base de datos-registro de nuevas claves		
	Actualización y cambios de llaves	Las llaves existentes deben actualizarse o cambiarse, incluyendo las normas relativas a cuando y como deberían cambiarse las llaves.			Registro de actualización		
	Manejo de llaves	Realizar el manejo de llaves y retiro			Base de datos-Llaves obsoletas		
	Realizar copias	Deben realizarse copias de respaldo o archivar claves			Base de datos-copias de respaldo		
	Destrucción de llaves	Realizar la destrucción de llaves de cifrado			Base de datos-llaves destruidas		

Tabla 20. Procedimiento de criptografía. Fuente propia.

Se especifica (Tabla 20) cómo se utilizará la criptografía dentro de los sistemas de información de la organización para garantizar su integridad, disponibilidad y confidencialidad, de igual manera se describe la complejidad de los controles criptográficas a emplear, dependiendo de la criticidad del activo de información que circulará a través de la red o se encontrará alojada en un sistema determinado [41].

El procedimiento de seguridad en criptografía para la entidad parte de establecer una política de criptografía desde la oficina de gestión tecnológica, y posteriormente realizar el control sobre las herramientas criptográficas. En ese sentido, establecer la política de controles criptográficos, donde se indica que debe realizarse una solicitud de llave proveniente del funcionario, que será almacena en la base de datos con el fin de llevar un registro de las llaves utilizadas y sobre que activos son puestas. Esas actividades aplican de la misma manera para los certificados. Adicionalmente deben realizarse copias de respaldo de los datos anteriormente mencionados. Con el fin de mitigar el riesgo de filtración o robo de información, en caso de pérdidas de los repositorios principales (Figura 21).

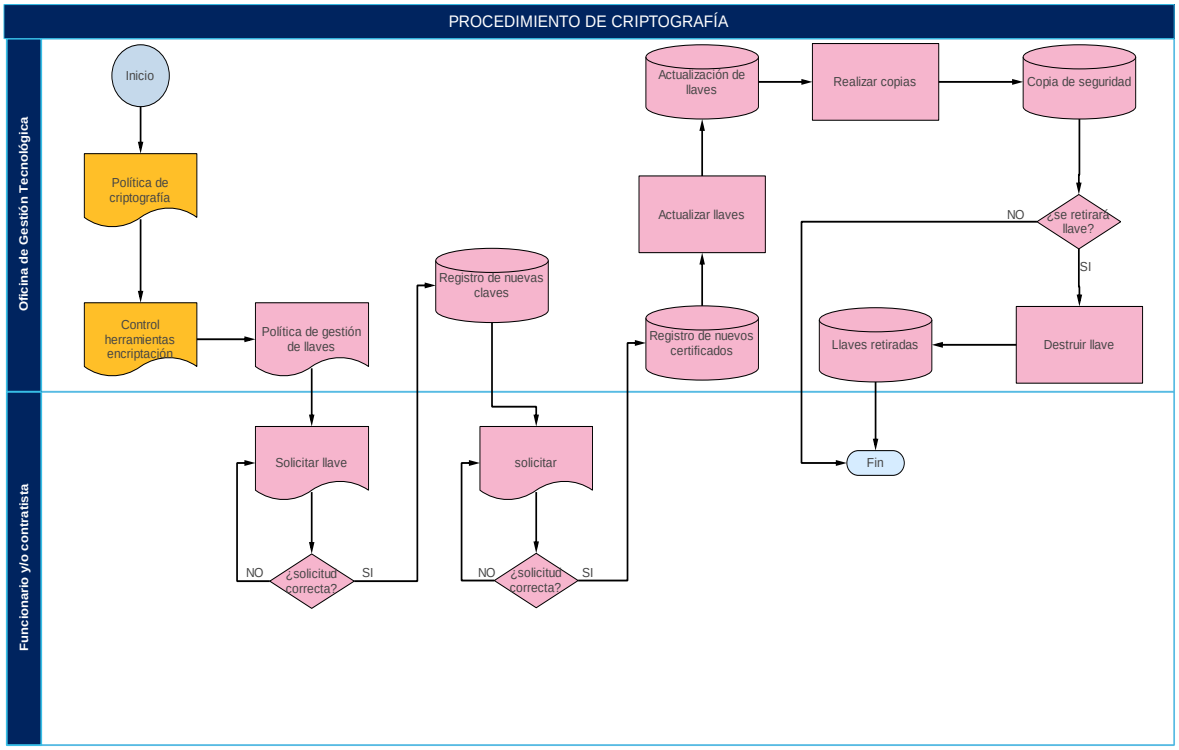


Tabla 21. Procedimiento Seguridad-Criptografía. Fuente propia.

2.6 Seguridad física y del entorno-A.11 ISO 27001

Consta de actividades precisas que cumplen con los requisitos de calidad, con el fin de garantizar la integridad de los equipos, mitigando daños ante desastres o manipulación incorrecta. En ese sentido el procedimiento brinda las actividades correspondientes a prevenir e acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización según los numerales A.11 Seguridad Física y del Entorno y 11. Seguridad física de las NTC 27001 Y 27002 respectivamente. De esa manera prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización, manteniendo las limitaciones de espacio en la estructura definida para los dispositivos de funcionamiento fundamental [42].

PROCEDIMIENTO DE SEGURIDAD FÍSICA Y DEL ENTORNO							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Las áreas seguras deben protegerse mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado	Perfil de usuario para control de acceso.	Debe crearse un perfil de usuarios, con el cual se determinan los acceso a los equipos de cada funcionario.	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica control-** Gestión Tecnológica- Prof. Universitario	III, IV y V	Base de datos perfiles de usuario	A.11.1.2 Controles de acceso físico.	11.1.2 Controles físicos de entrada
	Acceso al data center.	Generar un registro de acceso (entrada y salida) con fecha y hora, nombre y cargo que ocupa, con el fin de tener una base de registro de acceso. Mantener un libro físico de soporte, con accesos del personal que ha manipulado los equipos.			Libro de registro de accesos al data center		
	Asegurar el acceso al data center y a los equipos de servicio primordial de la Gobernación del Cauca.	Asegurar el acceso al data center y a los equipos de servicio por medio de sistema de seguridad con clave numérica. Cada funcionario debe llevar la identificación de manera visible para ingresar al data center. Observación: en el caso en que no se cuente con un sistema de seguridad para acceso al data center, debe notificarse por escrito que no se garantiza la seguridad de los equipos en las instalaciones.			Registro instalación de sistema de seguridad		
	Solicitud de acceso a áreas restringidas	Debe diligenciarse la solicitud de acceso a áreas restringidas con la cual se autoriza al personal “visitante” o proveedores, para ingreso a zonas críticas. De la misma manera para terceros que representan a proveedores prestadores de servicios en la Gobernación del Dpto. del Cauca			Registro de solicitud de visitantes		
	Actualizar los derechos de acceso	los derechos de acceso a las áreas seguras deberían ser revisados y actualizados regularmente, y revocados cuando sea necesario			Actualización de accesos autorizados		
Diseñar y aplicar una protección física contra desastres	Definir perímetro de seguridad	Definir el perímetro de seguridad de manera clara, dependiendo de los requisitos de seguridad y de los activos que reposen dentro del perímetro y de los resultados de la evaluación del riesgo.	**Implementa-** Oficina de Gestión Tecnológica y	III, IV y V	Plano de perímetro de seguridad	A.11.1.1 Perímetro de seguridad física.	11.1.1 Perímetro de seguridad física

naturales, ataques provocados por el hombre o accidentes	Supervisión del perímetro de seguridad	Supervisar que el perímetro de seguridad, edificio e instalaciones que contienen los recursos de tratamiento de la información sean físicamente sólidos.	Oficina de Gestión del Riesgo-Prof. Universitario **Aplica control**-Gestión Tecnológica-Prof. Universitario		Chequeo de instalaciones de perímetro de seguridad		
	Actividades no autorizadas dentro del perímetro de seguridad	En las instalaciones del centro de datos o de los centros de cableado, No está permitido: · Fumar dentro del Data Center. · Introducir alimentos o bebidas al Data Center · El porte de armas de fuego, corto punzantes o similares. · Mover, desconectar y/o conectar equipo de cómputo sin autorización. · Modificar la configuración del equipo o intentarlo sin autorización. · Alterar software instalado en los equipos sin autorización. · Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas. · Extraer información de los equipos en dispositivos externos. · Abuso y/o mal uso de los sistemas de información. · Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.			Señalización de acciones no permitidas		
	Montar sistema de alarmas contra desastres e intrusos	Instalación de alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control. Instalar sistemas de detección de intrusos adecuados conforme a las normas y ser probados periódicamente donde se dé cobertura.			Registro de instalación de métodos preventivos.		

	Ubicar los dispositivos principales en el data center (control aplicable a todas las dependencias)	Todo equipo primordial sea servidores, switches, tablero eléctrico, RACK contenedor de switches conexión a red, Patch Panel, equipo de borde de proveedor, firewall, bandejas de entrada de proveedores de fibra optica, router CISCO. DVR, puertos de servidores y patch panel. Deben estar ubicados en la el Data Center separados de los equipos gestionados por terceras partes. 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.			Plano con ubicación de los activos de información.		
	En caso de sufrir falla eléctrica utilizar el sistema alterno de respaldo de energía.	El Área de Tecnologías y Sistemas de la Información deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía. Unidades de potencia ininterrumpida 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.			Registro de activación de sistemas alternos		
Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	Identificarse para disponer de equipos	Identificarse como empleados y usuarios de terceras partes con permiso para sacar los activos fuera de las instalaciones, el permiso debe contener el tiempo de permanencia del equipo fuera de las instalaciones y retorno del mismo. Establecer limitación de tiempo que el activo puede estar fuera de las instalaciones y verificar que su retorno ha cumplido con dichas limitaciones.	**Implementa-** Oficina implicada **Aplica control-** Gestión Tecnológica-Prof. Universitario	II, III, IV y V	Permiso para disponer de equipos	A.11.2.5 Retiro de activos	11.2.5 Retirada de materiales propiedad de la empresa
	Registro de salida	El activo de información debe ser registrado en la salida con el fin de controlar y monitorear las salidas y retornos de los equipos de la Gobernación del Dpto. del Cauca			Registro de salida		
Aplicar medidas de seguridad a los equipos situados fuera las instalaciones de la	Manipular según instrucciones	Los equipos e información que sean sacados y manipulados fuera de la Gobernación del Dpto. del Cauca no deben ser descuidados en lugares públicos expuestos a daños y robo. Seguir las instrucciones de uso fuera de las instalaciones para los equipos respectivos	**Implementa-** Oficina implicada. **Aplica control-** Gestión	II, III, IV y V	Manual de uso e instrucciones	A.11.2.6 Seguridad de los equipos y activos fuera	11.2.6 Seguridad de los equipos fuera de las instalaciones

Gobernación del Dpto. del Cauca, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	Registro de custodios	cuando el equipo fuera de las instalaciones se transfiere entre diferentes individuos o entidades externas, se debería mantener un registro que defina la cadena de custodia de los equipos incluyendo, al menos, los nombres y las organizaciones de aquellos responsables de los equipos	Tecnológica-Almacén		Registro de cadena de custodios.	de las instalaciones	
Mantenimiento correcto de equipos que aseguren su disponibilidad y su integridad continuas.	Periodo de uso	Los equipos deberían mantenerse de acuerdo a las recomendaciones de intervalos de servicio y especificaciones del proveedor	**Implementa-** Oficina de Gestión Tecnológica-Técnico Admin. **Aplica control-** Gestión Tecnológica-Prof. Universitario	III, IV y V	Mantenimiento de equipos	A.11.2.4 Mantenimiento de equipos	11.2.4 Mantenimiento de los equipos
	Servicios y reparación	La reparación de los equipos y reparación y servicio de equipos, solo puede ser realizado por el personal de mantenimiento debidamente autorizado. Debe registrarse toda eventualidad de fallos, reales o sospechados, así como del mantenimiento preventivo y correctivo. Antes de poner el equipo en funcionamiento de después de su mantenimiento, debe ser inspeccionado para asegurar que el equipo no ha sido manipulado y que no funciona correctamente.					
	Cumplimiento de póliza de seguros	Se debe aplicar el cumplimiento con todos los requisitos de mantenimiento que exijan las pólizas de seguros..			Póliza de seguro		

Tabla 22. Procedimiento de seguridad física y del entorno. Fuente propia.

En el caso del procedimiento de seguridad física y del entorno deben cubrirse varios aspectos de tal manera, que los dispositivos principales corran el menor riesgo posible ante emergencias. Entonces, el procedimiento inicia con la creación del perfil de usuario a cargo de la oficina de gestión tecnológica que a su vez lleva un registro físico de los accesos del personal. Adicionalmente la oficina de gestión tecnológica debe gestionar la instalación de sistemas de acceso y actualizar los mismos; en ese sentido, el perímetro de seguridad debe ser delimitado en compañía y supervisión de la oficina de control del riesgo que notifica y realiza el chequeo de las instalaciones donde reposan los dispositivos de funcionamiento central (Figura 22).

El centro de datos debe estar señalizado con el fin de informar al personal las actividades no autorizadas en el lugar e informar a los visitantes las precauciones adecuadas en el sitio. Así mismo, debe realizarse el registro de salida de cualquier equipo de la central de la entidad y acatar su manual de uso tanto fuera de las instalaciones como para realizar el mantenimiento. Dado que el equipo presente alguna falla, el procedimiento finaliza con la aplicación de la póliza de seguro que lo proteja (Figura 22).

Dando lugar al perímetro de seguridad que busca proteger los principales dispositivos de tratamiento de información, se realiza la petición al Instituto Geográfico Agustín Codacci (IGAC) para realizar el levantamiento del área de la oficina de Gestión Tecnológica, que permite a los integrantes de la misma, delimitar los accesos físicos a los funcionarios que deben manipular los mismos. (Ver anexo C.)

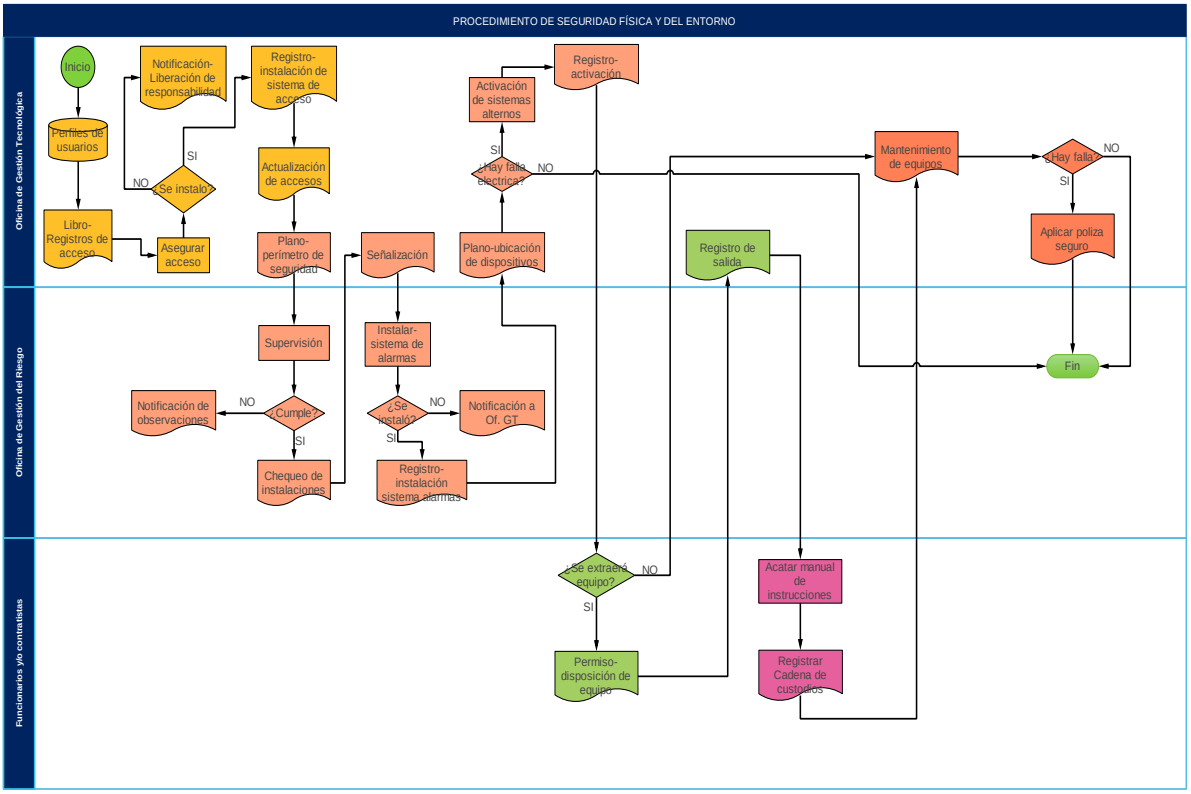


Figura 17 . Diagrama Seguridad física y del entorno. Fuente propia.

2.7 Seguridad de las operaciones-A.12 ISO 27001

El documento presenta el procedimiento de Seguridad de la información relacionado a la seguridad de las operaciones, donde se relacionan los procedimientos y responsabilidades, protección contra códigos maliciosos, copias de respaldo, el registro y seguimiento, control de software operacional, gestión de vulnerabilidad técnica y consideraciones sobre auditorias de sistemas de información. Lo anterior, tomado de los controles que se proporcionan en las normas NTC ISO/IEC 27001, A-12 y la norma NTC ISO/IEC 27001 -27002, numeral 12.

En ese sentido la seguridad de las operaciones debe documentarse y mantener procedimientos de operación y ponerse a disposición de todos los usuarios que los

necesiten, garantizando el correcto funcionamiento y seguridad de las instalaciones de tratamiento de información, de manera simultánea los procedimientos operacionales y los procedimientos documentados para las actividades del sistema deberían tratarse como documentos formales y los cambios deberían ser autorizados por la Dirección. Donde sea técnicamente posible, los sistemas de información, debieran gestionarse de una manera sistematiza, utilizando los mismos procedimientos, herramientas y recursos [43].

PROCEDIMIENTO DE SEGURIDAD DE LAS OPERACIONES							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deberían ser controlados.	Identificar y planificar cambios de gran impacto	Al planificar cambios deben realizarse las pruebas respectivas en los sistemas de procesamiento de información e instalaciones con funcionalidades a nivel central en la Gobernación del Dpto. del Cauca, así mismo, identificar y registrar los cambios que generan impacto en la Gobernación del Dpto. del Cauca a nivel de instalaciones de tratamiento de la información (unidades Hardware) y los sistemas que afectan a la seguridad (Software).	**Implementa**-Oficina de Gestión Tecnológica-Prof. Universitario y Técnicos Admin. **Aplica Control**-Oficina de Gestión Tecnológica-Prof. Universitario.	III, IV y V	Cronograma de cambios y pruebas	A.12.1.2 Gestión de cambios	12.1.2 Gestión de cambios
	Evaluar impactos	Todos los cambios que se realicen a nivel del Hardware y Software, en la Gobernación del Dpto del Cauca deben ser evaluados, respecto al impacto potencial en seguridad de la información. **Observación:** si la evaluación es favorable, se procede a aprobar el cambio, de lo contrario se rechaza.			Evaluación de impactos		
	Procedimiento de aprobación	Los cambios realizados en la Gobernación del Dpto. del Cauca deben ser aprobados a través de un procedimiento de aprobación formal, donde se verifique que cumplen con los requisitos mínimos en seguridad de la información: confidencialidad, disponibilidad e integridad.			Procedimiento de aprobación de cambios.		
	Comunicar cambios	Los cambios realizados en la entidad deben ser comunicados a todo el personal correspondiente, e involucrado en dichos cambios.			Registro de asistencia		

	Plan de retorno	Dado que alguno de los cambios o en su totalidad, no satisfagan lo esperado, la Gobernación del Dpto del Cauca debe contar con un plan de retorno al estado anterior de la entidad.			Plan retorno de cambios		
Supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema	Borrado de datos obsoletos	Los discos en uso deben ser limpiados constantemente con el fin del borrar datos que no sean necesarios y aumentar la capacidad de los mismos.	**Implementa-** Oficina de Gestión Tecnológica-Técnico Admin **Aplica Control-** Oficina de Gestión Tecnológica-Prof. Universitario	III, IV y V	Registro de limpieza de disco	A.12.1.3 Gestión de capacidad	12.1.3 Gestión de capacidades
	Desmantelar software y hardware.	La Gobernación del Dpto. del Cauca debe desmantelar toda aplicación, sistemas, bases de datos y dispositivos hardware que irrumpan en el funcionamiento óptimo de los recursos			Registro de desmantelamiento de software		
	Restringir uso de recursos	Debe restringirse o denegarse el ancho de banda utilizado para servicios que consumen gran cantidad de recursos, si no son críticos o fundamentales para la entidad.			Notificación de restricción de servicios.		
Definir metodología y separar los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	Definir metodología de desarrollo: diseño hasta implementación	A partir de: • Los requerimientos de la normativa dada por los organismos nacionales de control (Ministerios, superintendencias, entre otros). • Gestión de datos para diferentes sistemas de información. • Demás necesidades. Las entidades deben **definir y adoptar, una metodología de desarrollo en soluciones informáticas**, que permita realizar un proceso de: • Análisis de requerimientos. • Diseño de la solución informática. • Plan de pruebas. • Mantenimiento y actualización. El documento debe cumplir con una actualización constante, referente a las tecnologías que emplea la entidad y temas relacionados la misma.	**Implementa**- Personal vinculado a soluciones informáticas-Prof. Universitario y Técnicos Admin. **Aplica Control**- Oficina de Gestión Tecnológica-Prof. Universitario.	III y IV	Metodología de desarrollo Oficio-dispositivos para ambiente de pruebas	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.	12.1.4 Separación de los recursos de desarrollo, prueba y operación.

	Segregar los accesos	En ningún caso el ambiente de pruebas puede poseer acceso a los sistemas centrales de la entidad y viceversa	**Implementa**-Personal de desarrollo-Prof. Universitario y Técnicos Admin. **Aplica Control**-Oficina de Gestión Tecnológica-Prof. Universitario.	III y IV			
	Ejecución en distintos dispositivos	Todo software que este en proceso de desarrollo o actualización, debe ser ejecutado en diferentes sistemas, servidores y dispositivos alternos que sean asignados para pruebas, con el fin de mitigar el riesgo de obstruir los sistemas centrales de la Gobernación del Departamento del Cauca.	**Implementa** Personal de desarrollo-Prof. Universitario y Técnicos Admin. **Aplica Control**-Oficina de Gestión Tecnológica-Prof. Universitario.	III y IV	Registro de ejecución de pruebas.		
Implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación a funcionarios y/o contratistas.	Establecer una política formal prohibiendo el uso de software no autorizado	La política de prohibición de software no autorizado, debe contener la aclaración de las pautas de uso licenciado que otorga la Gobernación del Dpto del Cauca, que son brindadas para las aplicaciones adecuadas al cargo a desempeñar, si no se cuenta con un software debidamente autorizado, no podrá hacerse uso del mismo en las instalaciones de la entidad. La política también debe contener: política formal para proteger contra los riesgos asociados a la obtención de ficheros y software, ya sea a través de redes externas, o de cualquier otro medio, indicando las medidas de protección que deben implementarse;	**Implementa-** Oficina de Gestión Tecnológica-Técnico Admón y Prof. Universitario **Aplica Control-** Oficina de Gestión Tecnológica- Prof. Universitario	III, IV y V	Política de restricción de software no autorizado	A.12.2.1 Controles contra códigos maliciosos	12.2.1 Controles contra el código malicioso
Implementar los controles de detección, prevención y recuperación que sirvan como	Realizar chequeo de software no autorizado	Realizar establecimiento de: a) Lista de aplicaciones autorizadas por la cual se lleve a cabo un control sobre el uso de las mismas en la Gobernación del Dpto del Cauca. B) lista de sitios web no autorizados por la cual se controle el uso	**Implementa-** Oficina de Gestión Tecnológica-Técnico Admón y Prof. Universitario	III, IV	Lista de software no autorizado	A.12.2.1 Controles contra códigos maliciosos	12.2.1 Controles contra el código malicioso

protección contra el código malicioso, así como procedimientos adecuados de concienciación a funcionarios y/o contratistas.		inapropiado de los mismos en la Gobernación del Dpto del Cauca. c)Lista de de vulnerabilidades por la cual, se logra la reducción de las mismas que podrían ser explotadas por el código malicioso	**Aplica Control-** Oficina de Gestión Tecnológica- Prof. Universitario				
	Realizar chequeo de software no autorizado Detección de códigos maliciosos	Realizar establecimiento de: a) Lista de aplicaciones autorizadas por la cual se lleve a cabo un control sobre el uso de las mismas en la Gobernación del Dpto del Cauca. B) lista de sitios web no autorizados por la cual se controle el uso inapropiado de los mismos en la Gobernación del Dpto del Cauca. c)Lista de de vulnerabilidades por la cual, se logra la reducción de las mismas que podrían ser explotadas por el código malicioso a) Comprobación frente a código malicioso antes de usar los adjuntos al correo electrónico y las descargas; La Gobernación del Dpto del Cauca debe indagar en diferentes lugares, como: servidores de correo electrónico, los ordenadores de sobremesa y en la entrada de las redes de la organización que sea utilizada para manejo de información valiosa. b) Comprobación de páginas web para detectar código malicioso		III, IV	Lista de software no autorizado Registro de detección de códigos maliciosos		
	Definir responsabilidades	Definir responsabilidades de gestión para tratar la protección de los sistemas contra el código malicioso detectado, la formación en su uso, así como en el informe y recuperación de los ataques a los activos de información afectados;			Notificación de responsabilidades de gestión contra códigos maliciosos		

Tabla 23. Procedimiento de Seguridad de las operaciones. Fuente propia.

Con el fin de brindas seguridad en las operaciones que realiza la entidad en su interior, la oficina de gestión tecnológica realiza el cronograma de cambios y pruebas, para lo cual debe realizar la evaluación de impacto de los mismos; en esa actividad, se involucra la oficina de gestión organizacional, otorgando la aprobación y comunicación de los cambios en la entidad siempre y cuando sean favorables, de lo contrario serán rechazados.

El procedimiento involucra desmantelar discos, debido a la necesidad de realizar barridos de información obsoleta y restringir recursos que estén siendo desperdiciados. En ese orden, si la entidad se ve en la necesidad de desarrollar software, debe plantearse y comunicar la metodología de desarrollo y plan de pruebas en un ambiente adecuado para esa actividad. Dando lugar a lo anterior, el procedimiento plantea que la entidad posea la política de restricción de uso de software no autorizado, para lo cual realiza una lista de chequeo, que incluye detección de malware y eliminación del mismo.

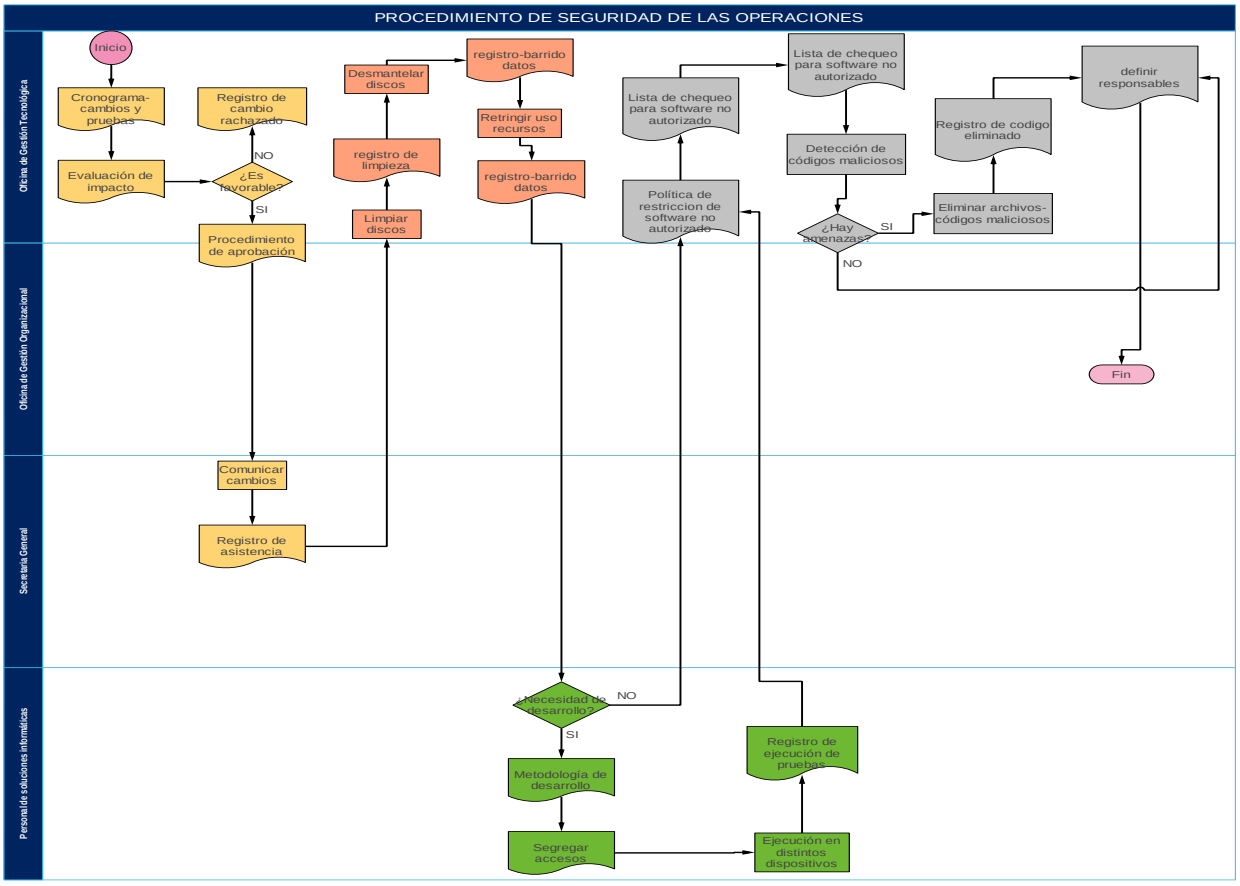


Figura 18. Diagrama Procedimiento de las operaciones.
Fuente propia.

2.8 Seguridad de las comunicaciones-A.13 ISO 27001

Seguridad de las comunicaciones involucra tres propósitos, brindar seguridad en redes e instalaciones y seguridad en la transferencia de información. Lo anterior, tomado de los controles que se proporcionan en los numerales A.13 y 13 de las normas NTC ISO/IEC 27001-27002 respectivamente.

La seguridad en las comunicaciones implica una aplicación transversal en la Gobernación del Departamento del Cauca, debido a que el fin de relacionar la seguridad de la información con la entidad, es mejorar la calidad de los servicios que se prestan

tanto interna como externamente, en ese sentido, la transferencia de activos de información debe contar con seguridad para los servicios de red, aclarando que no solo se involucran los servicios que presta la Gobernación del Departamento del Cauca, si no, también los servicios que otorgan algunos proveedores a la Entidad.

En este caso se recomienda según los estándares de calidad, mitigar los riesgos a los que se somete la información por medio de la segregación de las redes, con los criterios que considere la oficina de Gestión Tecnológica, definiendo parámetros, grupos de redes, unidades organizativas, entre otros ejemplos que pueden aplicarse con el fin de mejorar la seguridad de las comunicaciones en la Gobernación del Departamento del Cauca (Tabla 24).

PROCEDIMIENTO DE SEGURIDAD DE LAS COMUNICACIONES							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	Acordar gestión de servicios con el proveedor	Determinar y supervisar la capacidad del proveedor del servicio de red para gestionar los servicios acordados de una manera segura, y de igual manera, aclarar que la Gobernación del Dpto del Cauca tiene el derecho de realizar auditoria cuando lo considere pertinente. Los servicios de red incluyen la provisión de conexiones, servicios de red privada, redes de valor añadido y soluciones de seguridad de red gestionada, tales como, cortafuegos y sistemas de detección de intrusiones. El acuerdo debe contener una sanción al proveedor en caso de incumplimiento de contrato, exigir que el proveedor implemente tecnología como: autenticación y cifrado para acceder a los servicios de red y conexiones a la red, Parámetros técnicos requeridos para conexiones seguras con los servicios de red.	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica y Of. Gestión Organizacional-Prof. Universitario	III, IV y V	Acuerdo con proveedor	A.13.1.2 Seguridad de los servicios de red	13.1.2 Seguridad de los servicios de red
	Definir procedimiento de para restricción de servicios de red	Definir procedimiento de restricción de acceso a los servicios de red o aplicaciones donde su uso no sea necesario.			Procedimiento de restricción de servicios y acceso a red		

Establecer políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación	Diseñar procedimientos para proteger la información transferida de interceptación, copia, modificación, errores de enrutamiento y destrucción;	Procedimiento que debe considerar que: a) Para transferir la información, se debe contar la con previa autorización del Líder de la dependencia que se encuentre encargado. b) Todo equipo y red debe estar protegido con Firewalls y solución antivirus, aplicación que constantemente actualiza sus servicios y que la Gobernación del Dpto. del Cauca utiliza, para la protección contra el malware que se puede transmitir a través del uso de comunicaciones electrónicas. c) Hacer públicas y de carácter obligatorio la política de seguridad de la Información con el fin de evitar cometer errores humanos a causa de la falta de información, evitar correos con archivos que contengan origen desconocido o no autorizado por la Entidad.	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control**-Oficina de Gestión Tecnológica y Of. De Gestión Organizacional-Prof. Universitario.	III, IV y V	Documento de procedimiento para protección de información	A.13.2 Transferencia de Información	13.2 Intercambio de información.
	Definir política uso de recursos de comunicaciones	Establecer la política o directrices describiendo el uso aceptable de los recursos de comunicación para la Gobernación del Dpto del Cauca.			Política de uso de recursos de comunicación		
	Asignar Responsabilidades de personal	Asignar las responsabilidades del personal, partes externas y de cualquier otro usuario para no comprometer a la organización.			Notificación de responsabilidades		
	Cifrar documentos con acceso restringido dentro de la red de la Gobernación del Departamento del Cauca.	Cifrar con algoritmos de cifrado como RSA la información que se transfiere y se manipula en las redes internas de la Gobernación del Departamento del Cauca			Registro de documentos cifrados		

Tabla 24. Procedimiento de seguridad de las comunicaciones. Fuente propia.

En este caso el procedimiento tiene lugar a partir del acuerdo con los proveedores, donde la oficina de gestión tecnológica en mesa de trabajo con la oficina de gestión organizacional genera un procedimiento para restricción de los servicios de red, ya que al evaluar si un activo de información requiere transferirse, debe existir otro procedimiento que soporte esta última actividad. Dando continuidad a lo anterior, en cualquier caso debe establecerse la política de uso de recursos con el fin de dar lineamiento para manejo de los mismos y asignar responsables en las actividades anteriormente mencionadas (Figura 19).

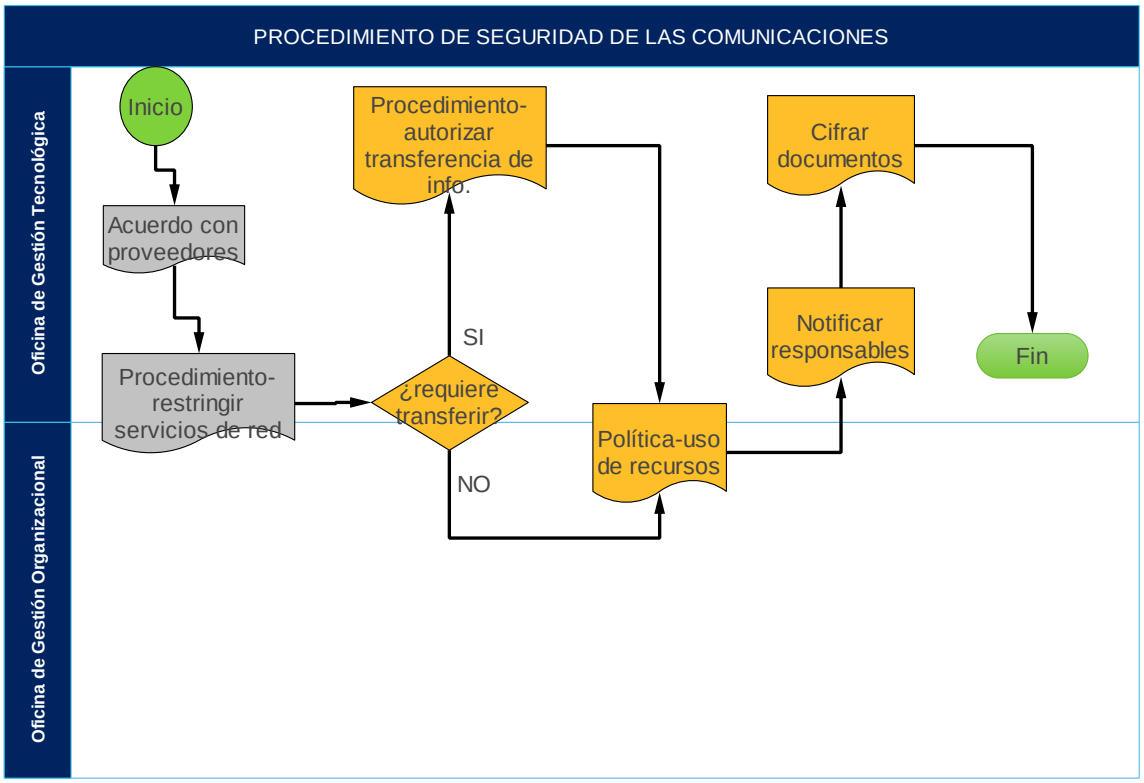


Figura 19. Diagrama de seguridad de las comunicaciones.
Fuente propia.

2.9 Relación con los proveedores- A.15 ISO 27001

Este procedimiento está relacionado con la protección de los activos de información involucrado con el manejo de la organización a los cuales los proveedores o terceros tienen acceso a los diferentes servicios de información; con base a los numerales A.15 y 15 de las normas NTC ISO/IEC 27001 y 27002 respectivamente. El procedimiento de relaciones con los proveedores brinda total claridad sobre el manejo de los acuerdos de confidencialidad que se construyen entre las partes interesadas (stakeholders), dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios [44].

Control	Actividades	Descripción	Responsable	Grupo Ocup.	Registro	Marco de Referencia	
						NTC ISO/IEC 27001	AENOR ISO/IEC 27002
Establecer los requisitos relacionados con la seguridad de la información con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes a la infraestructura tecnológica de la Gobernación del Dpto del Cauca.	Establecer acuerdo con el proveedor completo: legalidad, descripción de info y clasificación.	De acuerdo con el contrato ya sea de servicio y/o producto adquirido, se establecen los requisitos legales y de regulación para la protección de datos personales, derechos de propiedad intelectual, derechos de autor y definir cómo se va a garantizar el cumplimiento de los mismos. Implementar controles de acceso, control de evaluación de desempeño, supervisión e informes para soportar las respectivas auditorias. Incluir en el acuerdo las políticas de seguridad de la información importantes en el contrato. La Gobernación del Dpto del Cauca debe realizar en conjunto con el proveedor la descripción de la información que le será facilitada y a la cual tendrá acceso, con el fin de llevar un control de obligatorio cumplimiento sobre este acuerdo. Acordar la clasificación de la información de acuerdo a los esquemas de clasificación tanto del proveedor como de la Gobernación del Dpto del Cauca.	**Implementa-** Oficina de Gestión Tecnológica-Prof. Universitario **Aplica Control-** Oficina de Gestión Tecnológica-Prof. Universitario	III, IV y V	Acuerdo con proveedor (sea servicio o infraestructura)	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	15.1.2 Requisitos de seguridad en contratos con terceros
	Notificar y establecer accesos del personal	El proveedor debe acordar con la Gobernación del Dpto del Cauca la lista de personal que cuenta con acceso y recepción de la información de la entidad, procedimientos y condiciones; de igual forma informar las bajas respecto a los accesos por parte del personal del proveedor.			Notificación de accesos autorizados		
	Gestionar incidentes	El proveedor debe proporcionar los procedimientos de gestión de incidentes, notificarlos y colaborar en los mismos, informando el avance durante el mismo.			Procedimientos de gestión de incidentes		
	formación y concienciación del personal	La Gobernación del Dpto del Cauca en conjunto con el proveedor debe realizar la formación y concienciación del personal respecto a requisitos específicos de procedimientos de seguridad de la información.			Registro de asistencia		

Tabla 25. Procedimiento de seguridad en las relaciones con los proveedores.
Fuente propia.

El procedimiento referente a las relaciones con los proveedores parte de establecer el acuerdo ya sea por servicio o producto, por parte del proveedor y de la oficina de gestión tecnológica. En ese sentido, dado que el acuerdo sea satisfactorio, el proveedor debe proporcionar los accesos y el procedimiento de gestión de incidentes que implementa en un caso de emergencia; razón por la cual, el proveedor debe capacitar al personal en este tema y llevar un registro de asistencia como soporte (Figura 20).

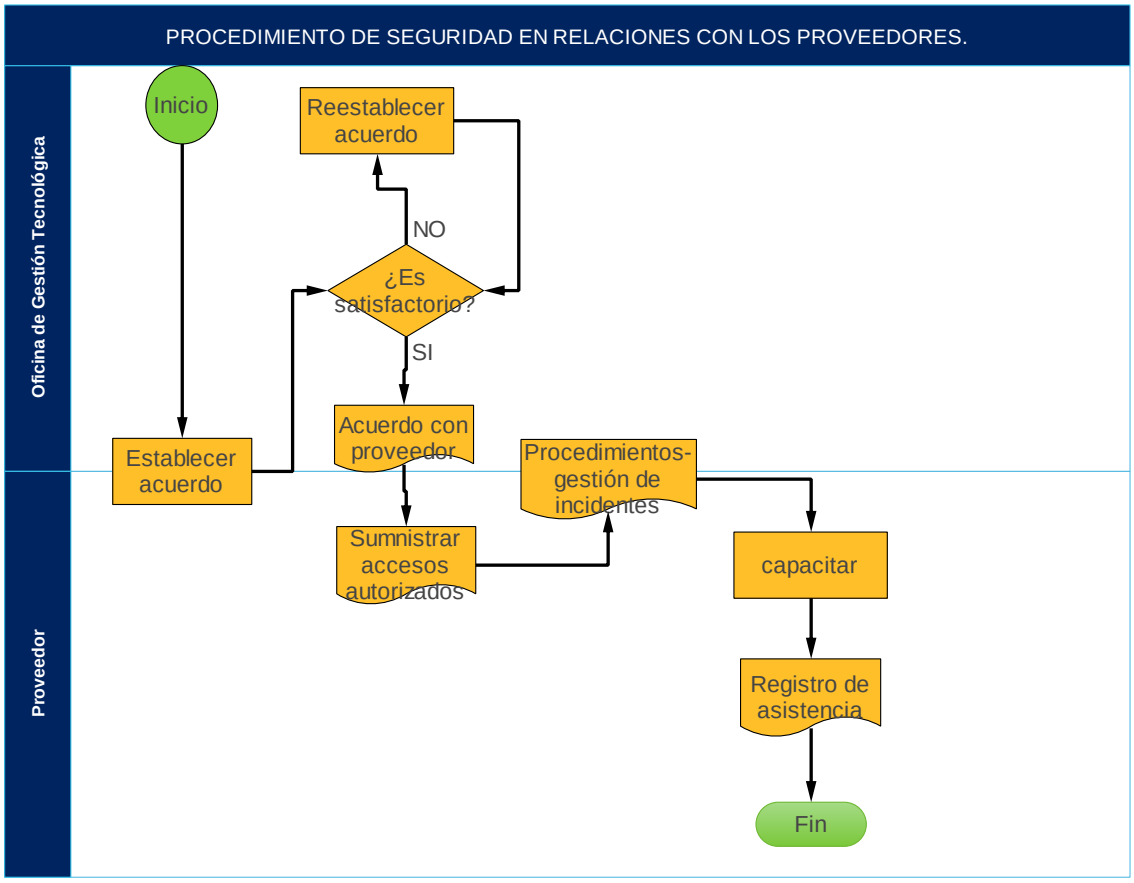


Figura 20. Diagrama de procedimiento de seguridad en relaciones con los proveedores. Fuente propia.

2.9 Adquisición, mantenimiento y desarrollo de sistemas de información-A.14 ISO 27001

El procedimiento establecido en la Tabla 25, identifica requisitos se seguridad de la información mediante diversos métodos, tales como los derivados del cumplimento de políticas y normativas, del modelo de amenazas, de la evaluación de incidentes o del uso de umbrales de vulnerabilidad [46]. Los resultados de la identificación de requisitos deberían ser documentados y revisados por todas las partes interesadas. Los requisitos y controles de seguridad de la información relacionada con la adquisición, desarrollo y mantenimiento de sistemas de información relacionadas en la norma NTC-ISO-IEC-27001, A.14 y la norma NTC-ISO-IEC-27002, 14, reflejan el valor empresarial de la información involucrada, y el impacto negativo en el negocio [45].

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN-ADQUISICIÓN, MANTENIMIENTO Y DESARROLLO.							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Preservar los requisitos relacionados con la seguridad de la información en los sistemas de información adquiridos, mejorados y actualizados.	Aprobar y autorizar acceso	La Gobernación del Dpto del Cauca en su facultad de usuario de los sistemas de información actuales, debe contar con un proceso de aprobación y autorización de acceso para los funcionarios y/o contratistas, de igual manera, para los usuarios con acceso privilegiado y usuarios técnicos.	**Implementa-**Oficina Gestión Tecnológica-Prof. Universitario. **Aplica control-**Oficina de Gestión Tecnológica-Prof. Universitario	IV y V	Proceso de aprobación y autorización, requisitos de seguridad de la información en sistemas de información.	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información	14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
	Autenticación de usuario	Orientar a los usuarios acerca de que deben contar con una identificación lo suficientemente específica para poder realizar la respectiva autenticación de usuario.		IV	Registro de autenticación valida		
	Informar deberes y responsabilidades	La Gobernación del Dpto del Cauca debe informar a los funcionarios y/o contratistas acerca de los deberes y responsabilidades que deben cumplir en el uso de los sistemas de información a los cuales están asociados.		IV y V	Documento de cumplimiento de deberes y responsabilidades del sistema de información en uso		
	Verificar necesidades de protección	La Gobernación del Dpto del Cauca, en el momento de adquirir o actualizar un sistema de información, debe realizar la verificación de cumplimiento particularmente de la confidencialidad, disponibilidad e integridad.		III, IV y V	Pruebas de protección de sistemas de información.		
	Verificación de otros controles	La Gobernación del Dpto del Cauca debe realizar la verificación de controles adicionales para mitigar riesgos como fuga de datos, modificación ilegal, interceptación de información, y daño de información.		IV y V	Pruebas de protección contra intrusos		

Establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas	Establecer política de desarrollo seguro	La política de desarrollo seguro debe ser aplicable para: para construir un servicio, una arquitectura, un software y un sistema seguros; debe tener los siguientes aspectos: a) La seguridad del entorno de desarrollo. b) Directrices sobre la seguridad en el ciclo de vida de desarrollo de software: 1) seguridad en la metodología de desarrollo de software, 2) guías de desarrollo seguro para cada lenguaje de programación utilizado, c) requisitos de seguridad en la fase de diseño; d) puntos de verificación de seguridad incorporados a los hitos del proyecto; e) repositorios seguros; f) seguridad en el control de versiones; g) conocimiento necesario sobre seguridad de aplicaciones; h) capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades	**Implementa-**Personal de desarrollo-Prof. Universitario. **Aplica control-**Oficina de Gestión Tecnológica-Prof. Universitario	III, y IV	Documento de política de desarrollo de software		14.2.1 Política de desarrollo seguro
La implantación de cambios a lo largo del ciclo de vida del desarrollo debería controlarse mediante el uso de procedimientos formales de control de cambios.	Mantener registro de cambios y comunicar cambios	a) el mantenimiento de un registro de los niveles de autorización aprobados; b) asegurar que los cambios son enviados a los usuarios autorizados;	**Implementa-**Personal de desarrollo-Prof. Universitario. **Aplica control-**Oficina de Gestión Tecnológica-Prof. Universitario	IV	Registro de autorización		14.2.2 Procedimiento de control de cambios en sistemas
	Proporcionar la documentación apropiada para cumplir con la metodología de desarrollo.	a) la identificación y comprobación de la seguridad del código crítico para minimizar la probabilidad de fallos de seguridad conocidos; b) la aprobación formal de propuestas detalladas antes de que comience el trabajo; c) la aceptación de los cambios por los usuarios autorizados antes de la implantación;	**Implementa-**Personal de desarrollo-Prof. Universitario. **Aplica control-**Oficina de Gestión Tecnológica-Prof. Universitario	IV	Documentación metodológica de desarrollo		14.2.2 Procedimiento de control de cambios en sistemas

		d) la actualización del conjunto de la documentación del sistema a la finalización de cada cambio y el archivo o eliminación de la documentación obsoleta; e) el mantenimiento de un control de versiones para todas las actualizaciones de software; f) el mantenimiento de registros de auditoría de todas las solicitudes de cambio; g) la adaptación de la documentación operativa y de los procedimientos de usuario, según sea necesario, para que sigan siendo apropiadas; h) la implantación de los cambios en el momento adecuado de forma que no perturbe los procesos de negocio involucrados.					
Establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	Evaluar los riesgos asociados con los proyectos de desarrollo de sistemas individuales y establecer entornos de desarrollo seguro	a) la sensibilidad de los datos a ser procesados, almacenados y transmitidos por el sistema; b) los requisitos externos e internos aplicables, por ejemplo, de reglamentos o políticas; c) los controles de seguridad ya implementados por la organización que apoyen el desarrollo del sistema; d) la honradez del personal que trabaja en el entorno e) el grado de contratación externa asociada con el desarrollo del sistema; f) la necesidad de la segregación entre los diferentes entornos de desarrollo; g) el control de accesos al entorno de desarrollo; h) la monitorización de los cambios en el entorno y el código almacenado en el mismo; i) el almacenamiento seguro de las copias de respaldo fuera de las instalaciones; j) el control del movimiento de datos desde y hacia el entorno.	**Implementa-**Personal de desarrollo-Prof. Universitario. **Aplica control-**Oficina de Gestión Tecnológica-Prof. Universitario	**IV**	Evaluación de riesgos y entorno de desarrollo.		14.2.6 Entorno de desarrollo seguro

Tabla 26. Procedimiento de adquisición, mantenimiento y desarrollo.

Fuente propia.

Se establece para el presente procedimiento, los controles necesarios en la adquisición, mantenimiento y desarrollo de los activos de información, iniciando con la aprobación y autenticación de usuarios por parte de la oficina de gestión tecnológica, que a su vez registrará la validación del usuario y notificará responsables a partir de las mismas. En ese orden, se deben realizar pruebas que cumplan con los requisitos mínimos en seguridad de la información, por lo cual se hace necesario establecer la política de desarrollo. Para lo anterior, el personal de desarrollo debe mantener un registro de cambios acorde con la metodología que se adopta y así mismo evaluar los riesgos que generan estas actividades de desarrollo (Figura 21).

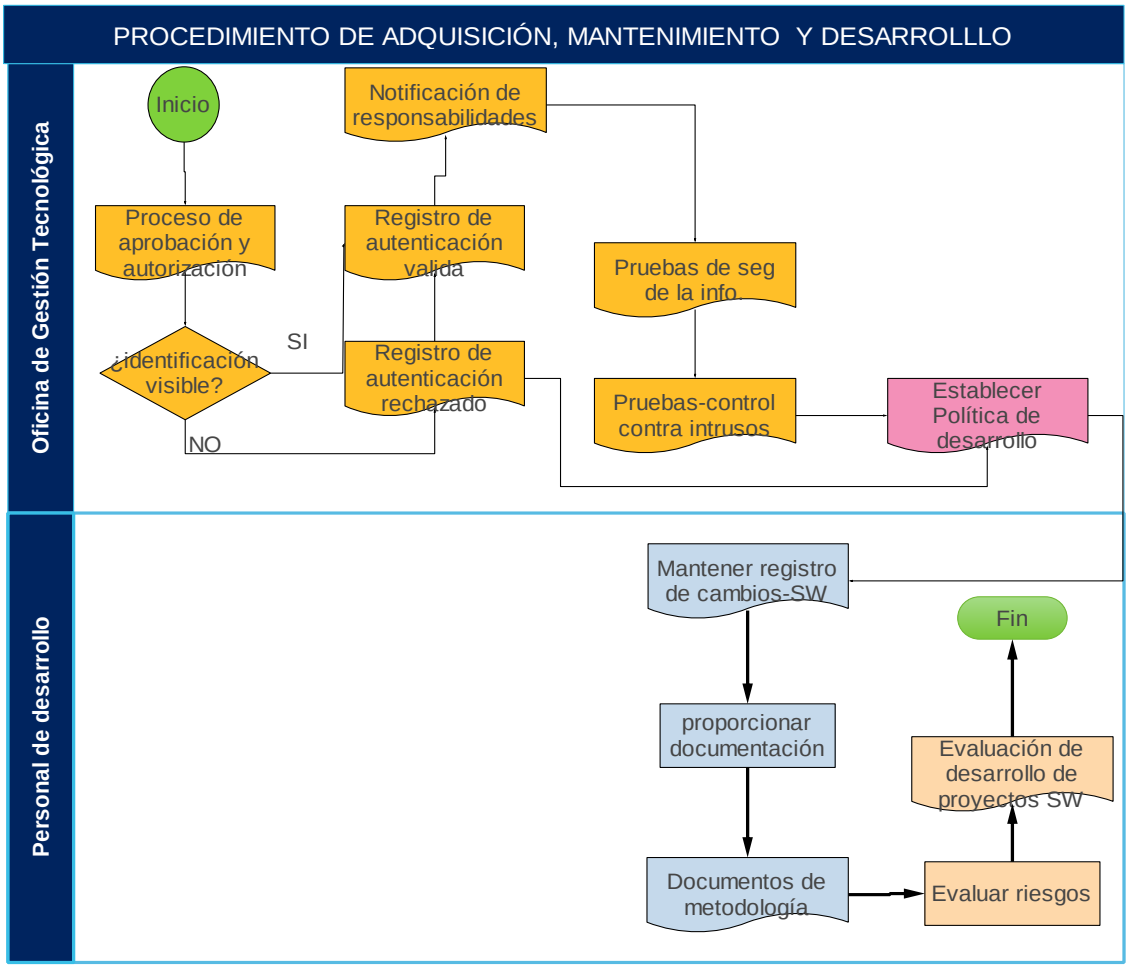


Figura 21. Diagrama de Procedimiento de Adquisición y Mantenimiento. Fuente propia.

2.10 Gestión de incidentes de seguridad de la información-A.16 ISO 27001.

El procedimiento de gestión de incidentes de seguridad de la información establece a partir de los numerales A.16 y 16 de las normas NTC ISO/IEC 27001 y 27002 respectivamente; los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes de Continuidad) dependiendo de la criticidad de la información y actividades de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información. En ese sentido este procedimiento indica cómo responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad [46].

PROCEDIMEINTO DE SEGURIDAD DE LA INFORMACIÓN-GESTIÓN DE INCIDENTES							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	Definir responsabilidades	Se deben definir responsabilidades a nivel de gestión con el fin de cubrir procedimientos de comunicación y desarrollo en un incidente, como: a) Planificar y preparar respuesta a incidentes. b) Seguimiento de monitoreo, detección, análisis y comunicación de incidentes de seguridad de la información. c) Registro de incidentes. d) Manejo de evidencias del incidente en cuestión. e) Evaluación y toma de decisiones sobre eventos de seguridad. f) Respuesta a personal interno y externo según sea el caso.	**Implementa-**Oficina Gestión Tecnológica-Prof. Universitario **Aplica control-**Oficina de Gestión Tecnológica- Prof. Universitario	III, IV y V	Documento-asignación de responsabilidades	A.16.1.1 Responsabilidades y procedimientos	16.1.1 Responsabilidades y procedimientos
	Definir requisitos para una correcta gestión de incidentes	Establecer procedimientos que aseguren: a) Personal competente para manejo de incidentes en la Gobernación del Dpto del Cauca. b) Determinación del punto de contacto para comunicar y detectar incidentes en seguridad de la información. c) Contacto externo: mantener contacto con entes externos y autoridades competentes en asuntos relacionados con seguridad de la información. Procedimientos para informar a funcionarios y/o contratistas: a) Como realizar la comunicación del incidente con el fin dar soporte al personal sobre las acciones a realizar en caso de sufrir un incidente. b) comportamiento que debe tener en caso de un incidente en seguridad de la información. c) Consecuencias: proceso disciplinario formal para investigar a funcionarios y/o contratistas. d) Retroalimentar: una vez se informe el incidente, los encargados deben establecer un canal de			Requisitos de aseguramiento y comunicación de incidentes		

		comunicación con el funcionario que lo reporto con el fin de dar seguimiento al mismo.					
Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	Identificar un incidente	Los funcionarios de la Gobernación del Dpto del Cauca deben saber que los incidentes a informar a través del punto de contacto, son: a) control ineficaz de seguridad de la información. B) Perturbación a la confidencialidad, integridad y disponibilidad de la información de la entidad. c) Incumplimiento de políticas o directrices. d) Obstrucción de la seguridad física. e) Cambios no autorizados en los sistemas de información. f) Violación de accesos.	**Implementa-**Gobernación del Dpto del Cauca **Aplica control-**Oficina de Gestión Tecnológica-Prof. Universitario	II, III, IV y V	Manual de identificación de incidentes en seguridad de la información	A.16.1.2 Reporte de eventos de seguridad de la información	16.1.2 Notificación de los eventos de seguridad de la información
	Reportar incidente	Una vez identificado un incidente, debe reportarse a la oficina responsable de seguridad de la información, a través de los canales de comunicación, donde se iniciará la respectiva inspección.			Reportes de incidente		

Tabla 27. Procedimiento de seguridad de la información-Gestión de incidentes.

Fuente propia.

Teniendo en cuenta que los riesgos en cualquier entidad siempre existen, debe contarse con una adecuada gestión de incidentes, que permita disminuir las pérdidas y daños de los activos de información al mínimo porcentaje. Por lo anterior, la oficina de gestión tecnológica debe asignar responsables con el fin de evaluar los requisitos mínimos a suplir en un incidente. Dado que se presente una situación riesgosa, debe inmediatamente notificarse la vulnerabilidad que ha sido detectada. De lo contrario, seguir el manual de incidentes y reportarlo por parte del funcionario y/o contratista logrará que se realice la debida inspección del incidente (Figura 22).

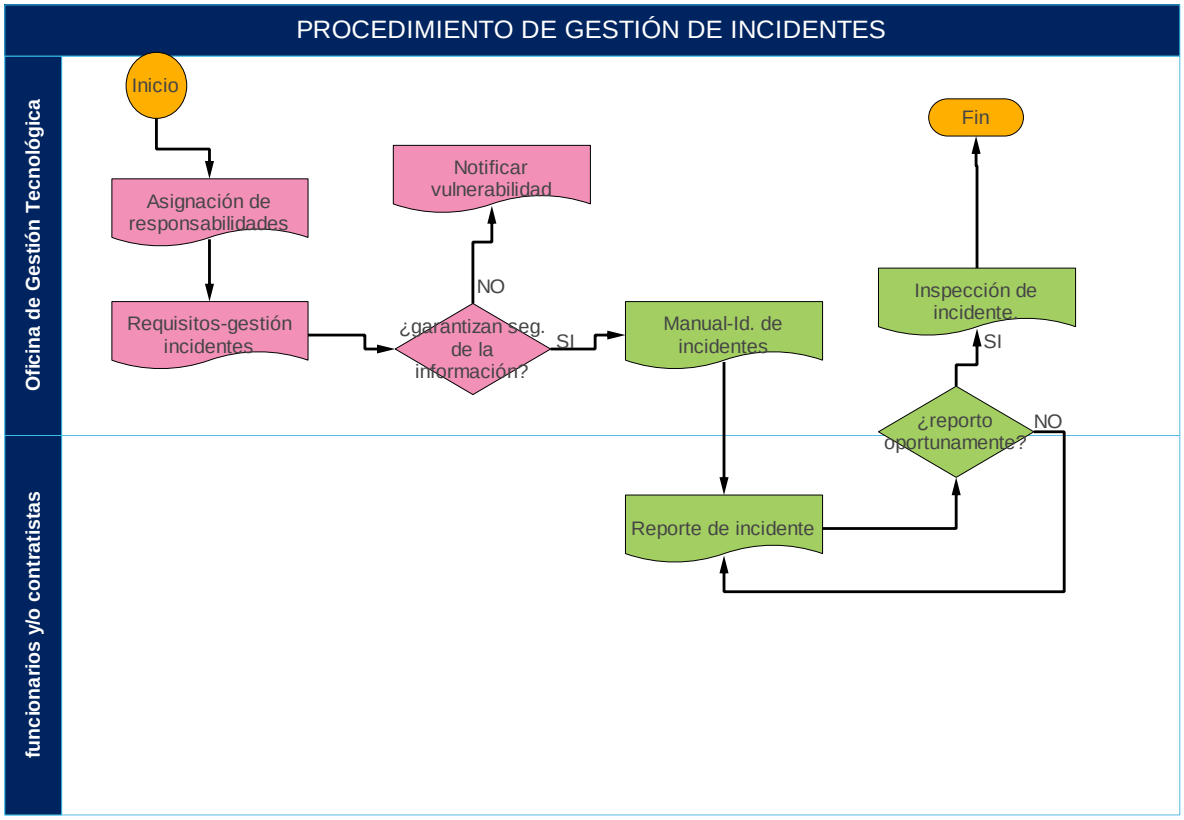


Figura 22. Diagrama de procedimiento de gestión de incidentes. Fuente propia.

2.11 Aspectos de seguridad de la información para la gestión de la continuidad del negocio-A.17 ISO 27001.

Indica la manera en que la entidad puede garantizar la continuidad para todos sus procesos y procedimientos (de ser posible o mínimamente los de carácter misional), permitiendo identificar los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico. En ese sentido el procedimiento define los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal; el procedimiento se define siguiendo los controles estipulados en los numerales A.17 y 17 de la norma NTC ISO/IEC 27001 y 27002 respectivamente.

PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN-GESTIÓN PARA LA CONTINUIDAD DEL NEGOCIO							
Control	**Actividades**	**Descripción**	**Responsable**	**Grupo Ocup.**	**Registro**	**Marco de Referencia**	
						NTC ISO/IEC 27001	**AENOR ISO/IEC 27002**
Determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre	Establecer plan de continuidad ante inconvenientes	La Gobernación del Dpto del Cauca debe establecer los requisitos de seguridad de la información en la planificación de la continuidad de los procesos de la entidad	**Implementa-** Oficina Gestión Tecnológica-Prof. Universitario **Aplica control-** Oficina de Gestión Tecnológica-Prof. Universitario.	III, IV y V	Plan de continuidad	A.17.1.1 Planificación de la continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información
	Análisis de impacto	En caso de que la Gobernación del Dpto del Cauca no cuente con un plan de continuidad formal, entonces, realizar un análisis de impacto en la entidad con una escala de valoración y así determinar los requisitos de seguridad en situaciones adversas.			Análisis de impacto, escala de valoración		
La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	Estructura adecuada ante eventos disruptivos	La Gobernación del Dpto del Cauca debe contar con una estructura adecuada para prevenir eventos disruptivos; de la misma manera que al personal capacitado para el manejo de estas situaciones.	**Implementa-** Oficina Gestión Tecnológica-Técnico Admin y Prof. Universitario. **Aplica control-** Oficina de Gestión Tecnológica-Prof. Universitario.	III, IV y V	Soporte de gestión ante eventos disruptivos	A.17.1.2 Implementación de la continuidad de la seguridad de la información.	17.1.2 Implementar la continuidad de la seguridad de la información
	Documentos de procedimientos.	Se deben desarrollar y aprobar documentos referentes a procedimientos de respuesta y recuperación, que detallen como la entidad realiza la gestión de estos eventos y mantendrá la seguridad de la información.		IV y V	Procedimientos de gestión y respuesta.		
	Gestión adecuada de conocimiento en incidentes.	El personal vinculado a la entidad que sea responsable o asignado en solución de incidentes, debe estar capacitado en temas de seguridad de la información, nuevas tecnologías y actualización de las tecnologías que se estén implementando en la entidad.			Soporte con listado de personal autorizado en gestión de incidentes.		
	Establecer controles de seguridad	Establecer controles de seguridad de la información en las herramientas y procesos que se implementen en el soporte y continuidad de negocio.			Controles principales en situación adversa		
	Establecer controles alternos	Establecer los controles alternos que suplan los principales con el fin de mantenerlos frente a una situación adversa.			Control alterno		

Tabla 28. Procedimiento de seguridad de la información-Gestión para la continuidad del negocio.

Fuente propia.

Con el fin de dar continuidad a los procesos de la gobernación del departamento del Cauca, el procedimiento consta de la implementación de un plan de continuidad previamente aprobado y verificado. Si no se cuenta con el plan de continuidad, debe realizarse por parte de la oficina de gestión tecnológica el análisis del impacto ocasionado.

Por otro lado, el control que permite disminuir los riesgos a nivel físico de la entidad, plantea diseñar una estructura sólida que permita ubicar de manera estratégica los equipos de funcionamiento central, también los procedimientos adecuados en eventos disruptivos y los controles que se implementarán en estos casos (Figura 23).

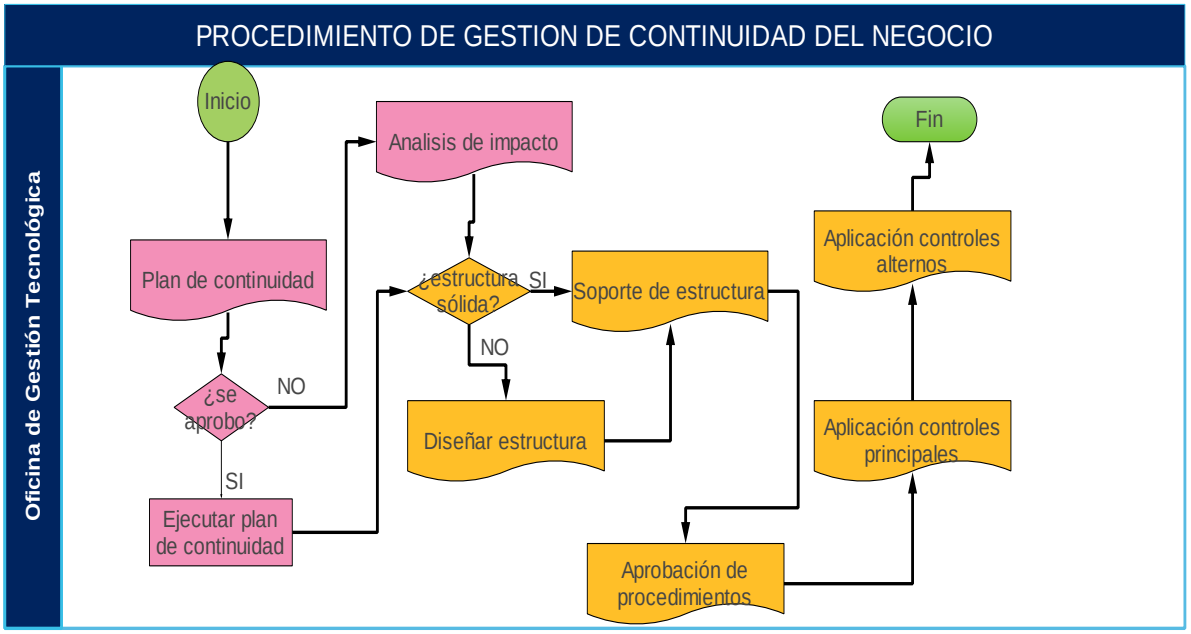


Figura 23. Diagrama de procedimiento de gestión para la continuidad del negocio.
Fuente propia.

Capítulo 3.
Cierre de Proyecto

3.1 Socialización de los procedimientos de seguridad de la información-herramienta de evaluación.

Inicialmente se realiza la sensibilización acerca de seguridad de la información a las siguientes oficinas:

- Oficina de Gestión Organizacional
- Oficina de Gestión Tecnológica.
- Oficina Asesora de Planeación.
- Oficina Asesora de Jurídica.
- Oficina de Talento Humano.
- Oficina de desarrollo integral e institucional.
- Oficina de Control Interno.

En la reunión se proporcionan, evidencias de las principales falencias que ocurren al interior de la entidad, y se explica de manera formal, la identificación del problema y las posibles soluciones que se establecerán desde la oficina de gestión tecnológica contando con la documentación necesarias de parte de las demás oficinas en pro de generar procedimientos con un alcance accesible.

Una vez definidos los procedimientos de seguridad de la información, teniendo en cuenta el formato y el respectivo marco de referencia de las Normas Técnicas relacionadas a las Tecnologías de la información, se procede a realizar la socialización de los mismos.

Por lo cual se realiza la intervención con las secretarías implicadas: Secretaría General, Secretaría de Educación y Secretaría de Salud. De manera conjunta se realiza la sensibilización al personal asistente, atendiendo en forma paralela las dudas y sugerencias de los involucrados.

Conforme a lo anterior, se realizaron las correcciones pertinentes a los procedimientos de seguridad; y a continuación se aprueban de manera uniforme en consenso del asesor y el jefe de la oficina de Gestión Tecnológica. Para posteriormente ser radicados y entregados a la oficina de Gestión Organizacional.

3.2 Resultados de Encuestas

Con el fin de obtener indicadores certeros sobre el avance del MSPI en la Gobernación del dpto. del Cauca se realizan dos encuestas, que permiten conocer el estado antes del establecimiento de los procedimientos de seguridad de la información y después del establecimiento de los mismos. Las encuestas son realizadas a 40 personas de la entidad con distintos cargos.

Encuesta-Estado actual de la entidad respecto a procedimientos de seguridad de la información.

a) ¿Tenía conocimientos en ofimática el ingresar a la entidad?

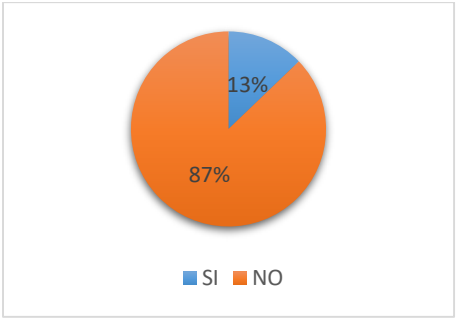


Figura 24. Porcentaje personal con conocimientos en ofimática.

b) ¿Genera registros de los procedimientos que realiza en la entidad?

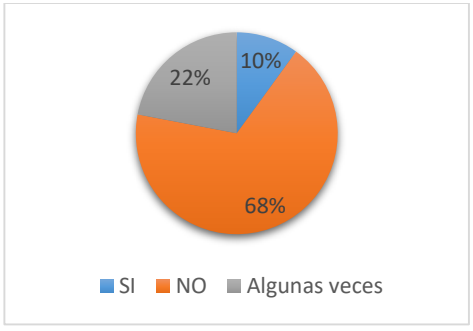


Figura 25. Porcentajes de generación de registros.

c) ¿El líder de su oficina realiza controles sobre los activos de información a su cargo?

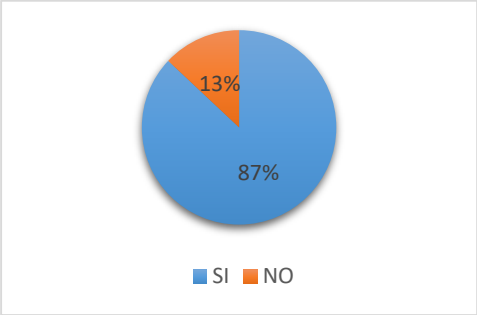


Figura 26. Controles sobre activos de información.

d) ¿Conoce los procedimientos de seguridad de la información que son vigentes en la entidad?

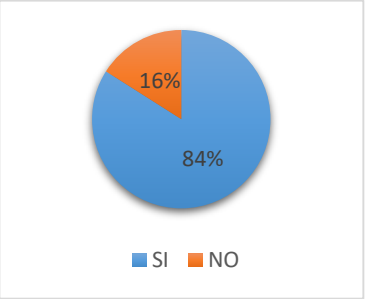


Figura 27. Porcentaje de personal enterado de los procedimientos vigentes.

Encuesta-Avance de procedimientos de seguridad de la información

a) ¿Qué importancia da al recurso humano respecto al manejo de la información de la entidad?

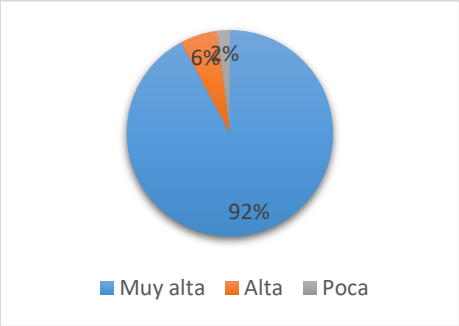


Figura 28. Importancia del recurso humano en seguridad de la información.

b) ¿Cómo califica la importancia de los procedimientos establecidos para la entidad?

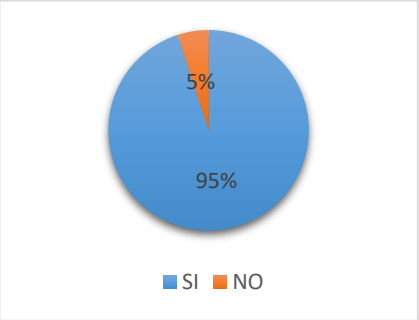


Figura 29. Importancia de los procedimientos según el personal

c) ¿En su concepto, los procedimientos suplen las necesidades principales de la entidad?

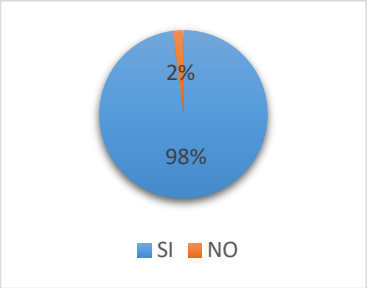


Figura 24. Satisfacción.

3.3 Conclusiones

Dando cierre al cumplimiento del cronograma y las actividades establecidas para realizar en la Oficina de Gestión Tecnológica, se concluye de la práctica profesional, lo siguiente:

- Debe definirse una estructura organizacional en la entidad con el fin de implementar los procedimientos de seguridad de la información.
- Se logra un nivel de madurez superior al encontrado previa la realización del proyecto, razón por la cual la entidad logra ascender del nivel inicial, al nivel de madurez repetible, donde se encuentran las entidades en las cuales existen procesos de gestión es una escala básica, con controles que mitigan el riesgo de seguridad de la información que se encuentran en implementación.
- El establecimiento de los procedimientos de seguridad de la información es de vital importancia debido a la necesidad de soportes sobre el manejo de los activos de información que permita mitigar riesgos como: filtración, modificación, daño o robo de información con un alto nivel de criticidad para la entidad.
- Implementar estándares de TI como ISO 27001 e ISO 27002 se hace fundamental en procesos donde garantizar la confidencialidad, integridad y disponibilidad de la información, son los requisitos básicos de operación ya

que en las entidades cuyo personal maneja tanto volumen de información el riesgo por manipulación incorrecta es mucho más alto.

- Todo documento que se genere relacionado con seguridad de la información, debe poseer un marco de referencia acorde al mismo, con el fin de evitar sanciones o irregularidades cuando se efectué una auditoria. En ese sentido, el documento que se establezca debe contar de manera paralela con la normatividad vigente en cuestión legal (decretos, leyes, entre otros) proporcionados por las entidades del estado.
- Asignar mesas de trabajo como gestoras para la seguridad de la información de manera que existan aportes y realimentación de los temas tratados de manera continua. La mesa de trabajo actúa como líder en cuestiones de avance de procesos, procedimientos y evaluación de indicadores a la hora de presentar resultados frente a las entidades de control.

  En esa ruta, la mesa de trabajo debe estar fuertemente construida, ya que tienen la responsabilidad de asignar los roles y responsabilidades a ejecutar en cada procedimiento y de manera general en un proyecto que trae beneficio a la entidad.
- Sensibilizar y capacitar al personal de la entidad, se convierte en el factor crucial en seguridad de la información, ya que son los principales actores que interactúan con los datos circulantes en la entidad y quienes deben responsabilizarse por ello ante cualquier incidente.

  La sensibilización y capacitación de los funcionarios y/o contratistas de la entidad influye de manera directa en el margen de error que se genere en la ejecución de procesos y procedimientos. Por lo anterior previo a contratarse, el personal debe estar informado sobre sus roles y responsabilidades, y así mismo debe poseer conocimientos en ofimática.
- La información es la fuente de sostenibilidad de una entidad, empresa u organización; lo que se convierte en el principal objetivo a mantener seguro el cien por ciento del tiempo, independiente del cargo que se esté ocupando. Como tal toda organización debe ser consciente de los activos de información que contengan gran valor y los que no, con el fin de tomar las precauciones necesarias para proteger cada uno de estos.

- Al llevar a cabo un trámite o solicitud, debe existir una comunicación fuerte y continua entre las oficinas involucradas; evitando crear islas de poder, pérdida de tiempo y perdida de información.
  En consonancia con lo anterior se deben generar registros que soporten de manera formal cada actividad realizada por los funcionarios encargados.

3.4 TRABAJOS FUTUROS

Cabe resaltar que Colombia posee grandes falencias a nivel público y es por ello que como trabajo futuro se propone continuar con el desarrollo del Modelo de Seguridad y Privacidad de la Información. De tal manera que se desarrollen los siguientes trabajos:

- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidente

Bibliografía

[1] ICONTEC, “Norma Técnica Colombiana NTC 9000:2015 “Sistemas de gestión de la calidad fundamentos y vocabulario”, núm. 571, pp. 1–47, 2015. [Internet]. Disponible en: https://www.ramajudicial.gov.co/documents/5454330/14491339/d2.+NTC+ISO+9000-2015.pdf/ccb4b35c-ee63-44b5-ba1e-7459f8714031

[2] MinTIC, “Modelo de Seguridad y Privacidad de la Información”, pp. 1–32, 2015. [Internet]. Disponible en: www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

[3] Techtarget, “Acuerdo de nivel de servicio o SLA”, [Internet]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Acuerdo-de-nivel-de-servicio-o-SLA

[4] IBM, “Identificación y autenticación”, [Internet]. Disponible en: https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm

[5] Delegación federal del trabajo en el estado de Guanajuato, “Implementación del proceso capacitador”, [Internet]. Disponible en: http://segob.guanajuato.gob.mx/sil/docs/capacitacion/La_funcion_de_la_capacitacion.pdf

[6] Kasperky Lab. “Definiciones: ¿Qué es el cifrado de datos?”. [Internet]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

[7] MinTIC, “Guía para la gestión y clasificación de activos de información”. 2016. [Internet]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[8] ICONTEC, “Norma Técnica Colombiana NTC ISO/IEC 27000:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de

la información (SGSI). Visión general y vocabulario". 2017. [Internet]. Disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27000.pdf

[9] UTP, "Términos y definiciones". [Internet]. Disponible en: https://www.utp.edu.co/gestioncalidad/sin-categoria/277/terminos-y-definiciones/pdf

[10] SISCA CCTV. Sistemas integrales de seguridad. "¿Qué es un control de acceso". 2015. [Internet]. Disponible en: http://sisca.co/que-es-un-control-de-acceso/

[11] Y. M. Travieso, "La Criptografía como elemento de la seguridad informática", 2003. [Internet]. Disponible en: http://eprints.rclis.org/5034/1/criptografia.pdf

[12] Econectia. "¿En que consiste la encriptación de datos?" [Internet]. Disponible en: https://www.econectia.com/blog/que-es-encriptacion-de-datos

[13] D. Rodriguez, "Clasificación y valoración de puestos". [Internet]. Disponible en: https://prezi.com/g-qlzbpdbehj/clasificacion-y-valoracion-de-puestos/

[14] C. A. Muñoz, Secretaría de Transparencia. "Ley de transparencia y acceso a la información pública". 2015. [Internet]. Disponible en: https://www.ramajudicial.gov.co/documents/5067224/14535305/ABC+LEY+DE+TRANSPARENCIA.pdf/68516da7-3ea2-4d64-9ca6-32bfb3737190

[15] Valdisito. "Seguridad de la información-Cifrado de la información". Enero, 2017. [Internet]. Disponible en: https://tanktroubleweb.wordpress.com/2017/01/26/cifrado-de-la-informacion/

[16] M. Rivero, "¿Qué son los malware?", 2016. [Internet]. Disponible en: https://www.infospyware.com/articulos/que-son-los-malwares/

[17] Escuela Tecnológico. Instituto Técnico Central. "Manual de políticas de seguridad y privacidad de la información". Versión 3. Pag 9/90, 2018. [Internet]. Disponible en: http://www.itc.edu.co/archives/calidad/GSI-MA-01.pdf

[18] MinTIC, “Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información”. pp 9, 2016. [Internet]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

[19] Insituto Nacional de Ciberseguridad de España, “Correo Electrónico”, 2018. [Internet]. Disponible en: https://www.osi.es/es/correo-electronico

[20] Presidencia de la República de Colombia, “Manual Operativo Sistema de Gestión”, 2018. [Internet]. Disponible en: http://www.funcionpublica.gov.co/documents/28587410/34112007/Manual+Operativo+MIPG.pdf/ce5461b4-97b7-be3b-b243-781bbd1575f3

[21] MinTIC, “Marco General-Modelo Integrado de Planeación y Gestión”, 2018. [Internet]. Disponible en: http://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/archivos/1511438319_9f397a80c4c6a995cea50fe93fcc59a9.pdf

[22] AENOR, “Norma Española UNE ISO/IEC 27002:2015 Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información”, 2016.

[23] MinTIC, “Manual de Gobierno Digital”, pp.21-27, 2001. [Internet]. Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf

[24] MinTIC, “Política de Gobierno Digital”, 2018. [Internet]. Disponible en: https://www.mintic.gov.co/portal/604/articles-74903_documento.pdf

[25] Gobernación del departamento del Cauca, “Manual de Política, Uso y Administración de Recursos Tecnológicos de la Gobernación del Departamento del Cauca.” , 2018. Oficina de Gestión Tecnológica.

[26] MinTIC, “G.GEN.01 Generalidades del Marco de Referencia de AE para la gestión de TI”, 2017. [Internet]. Disponible en:

https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8158_descargable_3.pdf

[27] MinTIC, “Marco General-Modelo Integrado de Planeación y Gestión”, 2018. [Internet]. Disponible en: http://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/archivos/1511438319_9f397a80c4c6a995cea50fe93fcc59a9.pdf

[28] ICONTEC, “Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos”, *Icontec*, núm. 571, p. 37, 2013. [Internet]. Disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

[29] MinTIC, “Procedimientos De Seguridad De La Información”, núm. 3, 2016. [Internet]. Disponible en: www.mintic.gov.co/gestionti/615/articles5482_G3_Procedimiento_de_Seguridad.pdf

[30] R. F. Oltra, UPV, “ ITIL, ¿Que és y breve historia”, [Internet]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/68323/Oltra%20-%20ITIL%C2%AE%20%28Information%20Technology%20Infrastructure%20Library%29%20Qu%C3%A9%20es%20y%20Breve%20Historia.pdf?sequence=1

[31] J. F. Pacheco y A. Prieto, “Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas”. 2005. [Internet]. Disponible en: www.mef.gob.pe/contenidos/pol_econ/documentos/ILPES_CEPAL_Marco_Logico_Metodologia.pdf

[32] DAFP,” Autodiagnóstico MIPG”, 2017. [Internet]. Disponible en: http://www.funcionpublica.gov.co/eva/mipg/herramientas-furag.html

[33] MinTIC, “Fortalecimiento de la Gestión TI en el Estado-Seguridad TI”, 2018.

[Internet]. Disponible en: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[34] MinTIC, “Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información”, 2016. [Internet]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf

[35] DIGEIG, Presidencia de República dominicana, “Descripcion de clase de cargo”, 2012. [Internet]. Disponible en: http://www.oas.org/juridico/PDFs/mesicic4_repdom_man.pdf

[36] R. F. Oltra, UPV, “Procesos, Funciones y Roles en ITIL®”, [Internet]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/68356/Oltra%20-%20Procesos,%20Funciones%20y%20Roles%20en%20ITIL%C2%AE.pdf?sequence=1

[37] Personeria de Itagüi, “Procedimiento para la vinculación y desvinculación de personal”, 2015. [Internet]. Disponible en: https://www.personeriaitagui.gov.co/uploads/entidad/calidad/cb77e-pth-01.pdf

[38] Superintendencia de sociedades, “Procedimiento de clasificación y etiquetado de activos de información”, 2014. [Internet]. Disponible en: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Calidad/DOCUMENTOS/GC-PR-004%20Procedimiento%20Clasificacion%20y%20Etiquetado%20de%20Activos%20de%20Informacion.pdf

[39] MinTIC, “Gestión para la clasificación de activos de información”, 2016. [Internet]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[40] SIGEPRE, “Lineamientos para el control de acceso”, 2017. [Internet]. Disponible en: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-TI-20-Control-Acceso.pdf

[41] UOC, “Política de seguridad criptográfica de la Universitat Oberta de Catalunya”, 2015. [Internet]. Disponible en: https://seu-electronica.uoc.edu/portal/_resources/ES/documents/seu-electronica/Politica_Seguretat_Criptogrxfica_UOC-cat_ES.pdf

[42] Supersalud, “Guía seguridad física y del entorno”, 2016. [Internet]. Disponible en: https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/SGGU01.docx

[43] Supersalud, “Guía seguridad de las operaciones”, 2016. [Internet]. Disponible en: https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSGU11.docx

[44] itaú, “Código de Relaciones con Proveedores”. [Internet]. Disponible en: https://www.itau.com.ar/Documents/Proveedores/Codigo_de_relacionamiento_con_proveedores.pdf

[45] Superintendencia de sociedades, “Procedimiento: adquisición, desarrollo, implementación y mantenimiento de sistemas de información”, 2017. [Internet]. Disponible en: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Infraestructura%20Tecnologica/Documentos/GINT-PR-003%20Implementacion%20Sistemas%20de%20Informaci%C3%B3n.pdf

[46] Superintendencia de sociedades, “Guia: gestion de incidentes”, 2017. [Internet]. Disponible en: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Infraestructura%20Tecnologica/Documentos/GINT-G-006%20Gu%C3%ADa%20Gestion%20de%20Incidentes.pdf

Anexos

Anexo A: Tabla de Autodiagnóstico Modelo Integrado de Planeación y Gestión MIPG

Seguridad y privacidad de la información	31,0	Indicadores de Proceso Logro: Definición del marco de seguridad y privacidad de la información y de los sistemas de información	35,8	¿Durante el periodo evaluado, cuál de las siguientes acciones realizó la Entidad? a. Generó un documento de diagnóstico, donde se identifica de manera clara el estado actual de la entidad en la implementación de Seguridad y Privacidad de la Información. b. Determinó el estado actual de la infraestructura tecnológica para desarrollar el plan de transición del protocolo IPv4 a IPv6.	30	La fase de diagnóstico de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quién está FORMA DE ASIGNAR EL PUNTAJE **Entidades del orden nacional y territorial:** Si la entidad generó un documento de diagnóstico, donde se identifica de manera clara el estado actual de la entidad en la implementación de Seguridad y Privacidad de la Información O determinó el estado actual de la infraestructura tecnológica para desarrollar el plan de transición del protocolo IPv4 a IPv6, obtiene una puntuación de 50. Si generó un documento de diagnóstico, donde se identifica de manera clara el estado actual de la entidad en la implementación de Seguridad y Privacidad de la Información Y determinó el estado actual de la infraestructura tecnológica para desarrollar el plan de transición del protocolo IPv4 a IPv6, obtiene una puntuación de 100. Si no ha hecho ninguna de las 2 acciones, obtiene 0.
				En lo que respecta a la política de seguridad y privacidad de la información: a. Está establecida b. Se encuentra alineada con los objetivos estratégicos de la entidad. c. Define los objetivos y da alcance a todos los procesos de la entidad d. No se cuenta con una política de seguridad.	45	La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada al interior de la entidad. Entiéndase por política la declaración de la alta Dirección de la entidad de su compromiso en la implementación de la seguridad y privacidad de la información. Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información. Entiéndase que el Manual de Políticas contiene el conjunto de lineamientos que serán implementados en la entidad y que definen la forma de implementar la seguridad y privacidad de la información en la entidad para dar cumplimiento a la declaración del compromiso de la alta Dirección de la entidad FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Calcule por separado: 1. Si la política de seguridad y privacidad de la información se encuentra alineada con los objetivos estratégicos de la entidad (opción b) Y define los objetivos y da alcance a todos los procesos (opción c), obtiene un puntaje de 100. Si la política de seguridad y privacidad de la información se encuentra alineada con los objetivos estratégicos de la entidad (opción b) O define los objetivos y da alcance a todos los procesos (opción c), obtiene un puntaje de 50. 2. Si el documento o manual con las políticas de seguridad y privacidad de la información se encontraba en construcción (opción a), la entidad obtiene un puntaje de 25. Si estaba en revisión (opción b), obtiene 50. Si estaba en aprobación (opción c), obtiene 75. Si estaba revisado, aprobado y divulgado por el comité institucional de desarrollo administrativo o el que haga sus veces (opción d), obtiene 100. Luego sume los dos resultados obtenidos de los cálculos anteriores y divida en 2.
				Durante el periodo evaluado, el documento o manual con las políticas de seguridad y privacidad de la información se encontraba a En construcción b En revisión c En aprobación d Revisado, Aprobado y divulgado por el comité institucional de desarrollo administrativo o el que haga sus veces e. No lo tiene		

				En el periodo evaluado, la entidad cuenta con un acto administrativo a través del cual se crean o se modifican las funciones del comité institucional de desarrollo administrativo o el que haga sus veces, donde se incluyen los temas de seguridad y privacidad de la información	30	Teniendo en cuenta que los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión, se hace necesario que la entidad formalice este procedimiento. Para mayor información, consulte la Guía No. 4, llamada Roles y Responsabilidad de Seguridad de la Información establece las funciones que debe tener el Comité de Desarrollo Administrativo o quien haga sus veces en materia de seguridad de la información. FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Sí la Entidad cuenta con un acto administrativo a través del cual se crean o se modifican las funciones del comité institucional de desarrollo administrativo o el que haga sus veces, donde se incluyen los temas de seguridad y privacidad de la información, obtiene un puntaje de 100. En caso contrario, obtiene 0.
				En el periodo evaluado, la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: Cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos. a La metodología de gestión de activos de información está en construcción b La metodología de gestión de activos de información está en revisión c La metodología de gestión de activos de información está en aprobación d La metodología de gestión de activos de información está revisada, aprobada y divulgado por comité institucional de desarrollo administrativo o el que haga sus veces. e No la tiene En el periodo evaluado, la entidad contó con un inventario de activos de información acorde a la metodología planteada a. Sí b. En Desarrollo/En proceso c. No.	30	La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios. Para mayor información consulte la Guía No 5 - Gestión De Activos, disponibles en el siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf 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. FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Calcule por separado: 1. Si la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, en construcción, obtiene un puntaje de 25. Si cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, en revisión, obtiene 50. Si la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, en aprobación, obtiene 75. Si la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, revisada, aprobada y divulgado por comité institucional de desarrollo administrativo o el que haga sus veces, obtiene 100. En caso contrario, obtiene 0. 2. Si la entidad cuenta con un inventario de activos de información acorde a la metodología planteada, obtiene un puntaje de 100. Sí está en desarrollo o en proceso de elaboración de un inventario de activos de información acorde a la metodología planteada, obtiene un puntaje de 50. De lo contrario, obtiene 0. Luego, sume los resultados obtenidos en las 2 operaciones anteriores y divida en 2

				En el periodo evaluado, la Entidad contó con: a. Un avance del documento de la metodología para la gestión de los riesgos de seguridad y privacidad de la información. b. Una metodología formalizada para la gestión de los riesgos de seguridad y privacidad de la información. c. Un avance del plan de tratamiento del riesgo. d. El plan de tratamiento del riesgo establecido. e. La declaración de aplicabilidad en desarrollo. f. La declaración de aplicabilidad definida. g. Ninguna de las anteriores	40	La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad. Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, puede emplearse la Guía No 8 - Controles de Seguridad, disponible en el siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Calcule por separado: 1. Si la entidad contó con la metodología formalizada para la gestión de los riesgos de seguridad y privacidad de la información(opción b), Y con el plan de tratamiento del riesgo establecido (opción d) Y con la declaración de aplicabilidad definida (opción f), obtiene un puntaje de 100. Si la entidad contó con la metodología formalizada para la gestión de los riesgos de seguridad y privacidad de la información (opción b), Y con un avance del plan de tratamiento del riesgo (opción c), Y con la declaración de aplicabilidad en desarrollo (opción e), obtiene 75. Si la entidad contó con 3 de las opciones de respuesta, pero con una combinación diferente a las señaladas anteriormente, obtiene 50. Si la entidad contó con 2 de las opciones de respuesta, cualquier combinación, obtiene 25. Si la entidad contó con 1 opción de respuesta, obtiene 12.5. Si no contó con ninguna opción de respuesta obtiene 0. 2. Si la entidad realizó la identificación, análisis y evaluación de los riesgos de seguridad y privacidad de la información conforme a la metodología planteada, obtiene un puntaje de 100. Si está en desarrollo o en proceso, obtiene 50. De lo contrario, obtiene 0. 3. Si el documento del plan de diagnóstico y estrategia de transición de IPv4 a IPv6, se encuentra en construcción, obtiene un puntaje de 25. Si está en revisión, obtiene 50. Si está en aprobación, obtiene 75. Si ya está revisado, aprobado y divulgado por el comité institucional de desarrollo o el que haga sus veces, obtiene 100. Luego, sume los resultados obtenidos en las 3 operaciones anteriores y divida en 3.
				En el periodo evaluado, la entidad realizó la identificación, análisis y evaluación de los riesgos de seguridad y privacidad de la información conforme a la metodología planteada a. Sí b. En Desarrollo/En Proceso b. No		
				Para el periodo evaluado, el documento del plan de diagnóstico y estrategia de transición de IPv4 a IPv6, se encontraba: a En construcción b En revisión c En aprobación d Revisado, aprobado y divulgado por el comité institucional de desarrollo o el que haga sus veces. e No lo tiene		

				La entidad formuló un plan de capacitación, sensibilización y comunicación de las políticas y buenas prácticas que mitiguen los riesgos de seguridad de la información a los que están expuestos los funcionarios	40	La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. Para estructurar dicho plan puede utilizar la Guía No 14 – plan de comunicación, sensibilización y capacitación, disponible en el siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Calcule por separado: 1. Si la entidad contaba con un plan de capacitación, sensibilización y comunicación de las políticas y buenas prácticas que mitiguen los riesgos de seguridad de la información a los que están expuestos los funcionarios, obtiene un puntaje de 100. En caso contrario, obtiene 0. 2. Para obtener el puntaje, divida el número de actividades realizadas por la entidad en materia de apropiación de la Estrategia de Gobierno en línea, sobre el total de aspectos evaluados (4) enunciadas en los literales a hasta d, y luego multiplique el resultado por 100. Luego, sume los resultados obtenidos en las 2 operaciones anteriores y divida en 2
				Seleccione las actividades realizadas por la entidad en materia de apropiación de la Estrategia de Gobierno en línea: a. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de sitio Web o Intranet b. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de eventos especiales relacionados con seguridad. c. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de medios físicos (Volantes, carteleras etc…) d. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de medios Digitales (e-learning, correo, pantallas, etc...)		

		Indicadores de Proceso Logro: Plan de seguridad y privacidad de la información y de los sistemas de información	30,0	Seleccione las fortalezas que la entidad ha mostrado frente a la implementación del Sistema de Gestión de Seguridad de la Información a. Asignación presupuesto para la implementación del SGSI. b. Asignación recurso humano altamente capacitado. c. Identificación de los controles adecuados. d. Definición de la implementación de las actividades o fases del SGSI. e. Compromiso por parte de la Dirección y Coordinadores en el apoyo activo al MSPI, mostrando su importancia para la entidad.	30	La entidad debe identificar sus fortalezas de acuerdo a las actividades realizadas para implementar los temas de seguridad y privacidad de la información incluyendo IPv6. FORMA DE ASIGNAR EL PUNTAJE: Si la entidad realizó alguna de las acciones que están entre los numerales (a) hasta (e), obtiene un puntaje de 20. Si realizó 2 de estas acciones, obtiene 40. Si realizó 3 de estas acciones obtiene 60. Si realizó 4 de estas acciones, obtiene 80. Si realizó las 5 acciones, obtiene 100. Si no realizó ninguna de las acciones, obtiene 0.
				Respecto al plan de tratamiento de riesgos de seguridad y privacidad de la información, indique las acciones realizadas por la entidad: a. Está construyendo el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos. b. Generó y aprobó el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos c. Está construyendo los informes relacionados con la implementación de los controles de seguridad y privacidad de la información d. Generó y aprobó los informes relacionados con la implementación de los controles de seguridad y privacidad de la información e. Está definiendo los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI es eficiente, eficaz y efectiva f. Definió y aprobó los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI es eficiente, eficaz y efectiva	30	La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos. FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Si la entidad generó y aprobó el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos (opción b), generó y aprobó los informes relacionados con la implementación de los controles de seguridad y privacidad de la información (opción d) y definió y aprobó los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI es eficiente, eficaz y efectiva (opción f), obtiene 100. Si la entidad generó y aprobó el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos (opción b), está construyendo los informes relacionados con la implementación de los controles de seguridad y privacidad de la información (opción c), y está definiendo los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI es eficiente, eficaz y efectiva (opción e), obtiene 75. Si la entidad realizó 3 acciones en combinaciones distintas a las anteriores, obtiene 50. Si la entidad realizó 2 acciones en combinaciones, obtiene 25. Si la entidad realizó 1 acción, obtiene 12,5. Si no hizo ninguna acción, obtiene 0

				Seleccione las actividades realizadas por la entidad en materia de apropiación de la Estrategia de Gobierno en línea: a. Formulación del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información b. Ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, sin tener en cuenta la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros). c. Ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, con base en la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros).	**30**	La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. Para estructurar dicho plan puede utilizar la Guía No 14 – plan de comunicación, sensibilización y capacitación, disponible en el siguiente enlace:: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la Entidad realizó la Formulación del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información (opción a), obtiene 25. Si la entidad realizó la Formulación y la ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, sin tener en cuenta la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros) (opciones a y b), obtiene 50. Si la entidad realizó la Formulación y la ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información con base en la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros) (opciones a y c), obtiene 100. Si la entidad no tiene el plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, obtiene 0.
		Indicadores de Proceso Logro: Monitoreo y mejoramiento continuo	**30,0**	Seleccione las actividades realizadas por la entidad en materia de monitoreo de la Estrategia de Gobierno en línea: a. Revisión periódica de los compromisos establecidos para ejecutar el plan de tratamiento de riesgos a la seguridad de la información b. Seguimiento a la efectividad de los controles a los riesgos a la seguridad de la información c. Determinación de la eficacia en la gestión de incidentes de seguridad de la información en la entidad. d. Formulación del plan de seguimiento, evaluación y análisis de resultados del MSPI, teniendo en cuenta los indicadores de gestión y cumplimiento. e. Formulación de los planes de auditoria para la revisión y verificación de la gestión de la seguridad y privacidad de la información al interior de la entidad. f. Seguimiento y control a la implementación del MSPI, por parte del comité institucional de desarrollo administrativo o el que haga sus veces	**30**	El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. Guía No 16 – Evaluación del desempeño: http://www.mintic.gov.co/gestionti/615/articles-5482_G16_evaluaciondesempeno.pdf Guía No 15 – Guía de Auditoría: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Calcule de forma separada: 1. Si se revisaron periódicamente los compromisos establecidos para ejecutar el plan de tratamiento de riesgos (opción a) obtiene un puntaje de 100 2. Si la entidad realizó seguimiento a la medición de efectividad de los controles (opción b), O determinó la eficacia en la gestión de incidentes de seguridad de la información en la entidad (opción c) obtiene un puntaje de 100 3. Si la entidad formuló el plan de seguimiento, evaluación y análisis de resultados del MSPI, teniendo en cuenta los indicadores de gestión y cumplimiento (opción d) O si la entidad formuló los planes de auditoria para la revisión y verificación e la gestión de la seguridad y privacidad de la información al interior de la entidad. (opción e) obtiene un puntaje de 100 4. Si la entidad realizó seguimiento y control a la implementación del MSPI, por parte del comité institucional de desarrollo administrativo o el que haga sus veces (opción f) obtiene un puntaje de 100 Luego, sume los resultados obtenidos en las 4 operaciones anteriores y divida en 4. Si la entidad no realiza ninguna de estas actividades, obtiene 0.

				Respecto a la implementación de acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la Información, la entidad: a. Determina las posibles acciones correctivas derivadas de los hallazgos o debilidades identificadas en la evaluación del desempeño de la seguridad y privacidad de la información al interior de la entidad b. Implementa las acciones correctivas y los planes de mejora de la seguridad y privacidad de la información al interior de la entidad. c. Determina si las acciones correctivas aplicadas son las adecuadas para gestionar los hallazgos y debilidades identificadas en seguridad y privacidad de la información al interior de la entidad.	30	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. Los instrumentos que deben consultar las entidades para esta etapa son: Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Para mayor información, consulte la Guía No 17 – Mejora Continua, disponible en el siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Calcule de forma separada: 1. Si la entidad determinó las posibles acciones correctivas derivadas de los hallazgos o debilidades identificadas en la evaluación del desempeño de la seguridad y privacidad de la información al interior de la entidad, obtiene 100. En caso contrario, obtiene 0. 2. Si la entidad implementó las acciones correctivas y los planes de mejora de la seguridad y privacidad de la información al interior de la entidad, obtiene un puntaje de 100. En caso contrario, obtiene 0. 3. Si la entidad determinó si las acciones correctivas aplicadas son las adecuadas para gestionar los hallazgos y debilidades identificadas en seguridad y privacidad de la información al interior de la entidad, obtiene un puntaje de 100. De lo contrario, obtiene 0. Luego, sume los resultados de las 3 operaciones realizadas anteriormente y divida en 3,
		Indicadores de resultado Seguridad y Privacidad de la Información	30,0	La entidad contó con un proceso de identificación de infraestructura crítica, lo aplicó y comunicó los resultados a las partes interesadas	30	Esta pregunta se puede responder con base a la valoración de activos que está haciendo en la entidad puesto que hasta este año se oficializa el catálogo de infraestructuras críticas y se inicia con su identificación oficial. Es una pregunta informativa sobre identificación y clasificación de activos. FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial** Si la entidad a entidad contó con un proceso de identificación de infraestructura crítica, lo aplicó y comunicó los resultados a las partes interesadas, obtiene un puntaje de 100. De lo contrario obtiene 0.
				Indique si el tiempo en promedio que demoró la entidad en corregir sus vulnerabilidades luego de ser reportadas por el COLCERT tardó: a. Minutos b. Horas c. Días d. Semanas e. La entidad no ha recibido reporte de COLCERT	30	Se hace necesario que las entidades y el Colcert tengan un mayor relacionamiento, así que debemos empezar a medir la efectividad de la comunicación y así poder tener acciones de mejora al respecto. FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Si demoró minutos, obtiene un puntaje de 100. Si demoró horas, obtiene 75. Si demoró días, obtiene 50. Si demoró semanas, obtiene 25. (Si la Entidad no ha recibido reporte de COLCERT esta actividad no aplica. En consecuencia, no deberá tenerse en cuenta para el cálculo de los indicadores de resultado de Seguridad y Privacidad de la Información)

				La entidad intercambió información de incidentes de seguridad con la entidad cabeza de sector o de ser necesario con el Colcert.	30	Es necesario que las entidades midan y gestionen sus incidentes de seguridad y privacidad de la información, de la misma forma es necesario hacer una medición continua de los mismos para tener una base consolidada. FORMA DE ASIGNAR EL PUNTAJE: **Entidades del orden nacional y territorial:** Si la entidad intercambió información de incidentes de seguridad con la entidad cabeza de sector o de ser necesario con el Colcert, obtiene 100. De lo contrario, obtiene 0. (Si la Entidad no ha identificado incidentes, esta actividad no aplica. En consecuencia, no deberá tenerse en cuenta para el cálculo de los indicadores de resultado de Seguridad y Privacidad de la Información)

Anexo B: Tabla de gestión Administrativa de la Herramienta de evaluación del MSPI

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
AD.3	Responsable de SI/Gestión Humana/Líderes de los procesos	SEGURIDAD DE LOS RECURSOS HUMANOS		A.7	ITIL	
AD.3.1	Responsable de SI	Antes de asumir el empleo	Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.	A.7.1	Modelo de Madurez Definido	
AD.3.1.1	Gestión Humana	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.	A.7.1.1		Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de: a) Referencias satisfactorias b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; c) Confirmación de las calificaciones académicas y profesionales declaradas; d) Una verificación más detallada, como la de la información crediticia o de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización. f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo estudio de seguridad, polígrafo, visita domiciliaria) g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud.

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
						h) La información sobre todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales.
AD.3.1.2	Gestión Humana	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.	A.7.1.2		
AD.3.2	Responsable de SI/Líderes de los procesos	Durante la ejecución del empleo	Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.	A.7.1.2	Modelo de Madurez Definido	
AD.3.2.1	Responsable de SI	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.	A.7.2.1		De acuerdo a la NIST los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información. Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas: a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas. d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular. e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).
AD.3.2.2	Responsable de SI/Líderes de los procesos	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	A.7.2.2	Componente planeación Modelo de Madurez Inicial	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
			actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.			información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con que criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. Para la calificación tenga en cuenta que: Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información. Diseñar programas para los conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, deben estar aprobados y documentados, por la alta Dirección, están en 40. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, están en 60.

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
AD.3.2.3	Responsable de SI	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.	A.7.2.3	Proceso definido en la Gobernación del Cauca	Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor?
AD.3.3	Responsable de SI	Terminación y cambio de empleo	Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.	A.7.3	Modelo de Madurez Definido	
AD.5.1.3	Responsable de SI	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.	A.7.3.1		Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.
GESTIÓN DE ACTIVOS						
AD.4	Responsable de SI	GESTIÓN DE ACTIVOS		A.8		
AD.4.1	Responsable de SI	Responsabilidad de los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	A.8.1	Modelo de Madurez Gestionado	

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
AD.4.1.1	Responsable de SI	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.	A.8.1.1	Componente Planificación Modelo de madurez inicial	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. Tenga en cuenta para la calificación: 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.
AD.4.1.2	Responsable de SI	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	A.8.1.2		Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades: a) asegurarse de que los activos están inventariados; b) asegurarse de que los activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.
AD.4.1.3	Responsable de SI	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.	A.8.1.3		Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
AD.4.1.4	Responsable de SI	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.	A.8.1.4		Revisar las políticas, normas, procedimientos y directrices relativas a los controles de seguridad de la información durante la terminación de la relación laboral por ejemplo, la devolución de los activos de información (equipos, llaves, documentos, datos, sistemas) , las llaves físicas y de cifrado, la eliminación de los derechos de acceso, etc. En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad. Durante el período de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.
AD.4.2	Responsable de SI	Clasificación de información	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.	A.8.2		
AD.4.2.1	Responsable de SI	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.	A.8.2.1	Modelo de Madurez Inicial	Solicite el procedimiento mediante el cual se clasifican los activos de información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
AD.4.2.3	Responsable de SI	Manejo de activos		A.8.2.3		Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los activos; c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; e) Marcado claro de todas las copias de medios para la atención del receptor autorizado. f) De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida.
AD.4.3	Responsable de TICs	Manejo de medios	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.	A.8.3		
AD.4.3.1	Responsable de TICs	Gestión de medios removibles		A.8.3.1		Solicite las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren: a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo; i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo DLP)

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
AD.4.3.2	Responsable de TICs	Disposición de los medios		A.8.3.2		Solicite los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. Verifique si se ha realizado esta actividad y si existen registros de la misma.
AD.4.3.3	Responsable de TICs	Transferencia de medios físicos		A.8.3.3		Solicite las directrices definidas para la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c) Indague y evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos; d) Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.
AD.5	Responsable de la Continuidad	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		A.17		
AD.5.1	Responsable de la Continuidad	Continuidad de la seguridad de la información	La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.	A.17.1		
AD.5.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Modelo de Madurez Gestionado	Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez)

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS						
						Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. Tenga en cuenta para la calificación: 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentan tan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección, están en 40. 2) Si se reconoce la importancia de ampliar los planes de continuidad de del negocio a otros procesos, pero aun no se pueden incluir ni trabajar con ellos, están en 60.
AD.5.1.2	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2	Modelo de Madurez Definido	Verifique si la entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección. Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA	
SEGURIDAD DE LOS RECURSOS HUMANOS							
AD.5.1.3	Responsable de la Continuidad	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		A.17.1.3	Modelo de Madurez Optimizado	PR.IP-4 PR.IP-10	Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información; Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.
AD.5.2	Responsable de la Continuidad	Redundancias	Asegurar la disponibilidad de las instalaciones de procesamiento de la información.	A.17.2			
AD.5.2.1	Responsable de la Continuidad	Disponibilidad de instalaciones de procesamiento de información		A.17.2.1		ID.BE-5	Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.
CUMPLIMIENTO							
AD.6	Responsable de SI/Responsable de TICs/Control Interno	CUMPLIMIENTO		A.18			

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA	
SEGURIDAD DE LOS RECURSOS HUMANOS							
AD.6.1	Responsable de SI	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		ID.GV-3	De acuerdo a la NIST: Los requerimientos legales y regulatorios respecto de la ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.
AD.6.1.1	Responsable de SI	Identificación de la legislación aplicable y de los requisitos contractuales.		A.18.1.1	Modelo de Madurez Gestionado Cuantitativamente		Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.
AD.6.1.2	Responsable de TICs	Derechos de propiedad intelectual.		A.18.1.2			1) Solicite los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 2) Verifique si la Entidad cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. Esta política debe estar orientada no solo al software, si no también a documentos gráficos, libros, etc. 3) Indague como se controla que no se instale software ilegal. 4) Indague si se tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en cuenta los controles que deben existir para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA	
SEGURIDAD DE LOS RECURSOS HUMANOS							
AD.6.1.3	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	A.18.1.3		PR.IP-4	Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.
AD.6.1.4	Responsable de SI	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	A.18.1.4		DE.DP-2	Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013. 1) Revise si existe una política para cumplir con la ley 2) Si están definidos los responsables 3) Si se tienen identificados los repositorios de datos personales 4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho. 5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5			n/a
AD.6.2	Control interno	Revisiones de seguridad de la información		A.18.2	Modelo de Madurez Gestionado Cuantitativamente		

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	PRUEBA	
SEGURIDAD DE LOS RECURSOS HUMANOS							
AD.6.2.1	Control interno	Revisión independiente de la seguridad de la información		A.18.2.1			Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de gestionar la seguridad de la información. Para esto solicite: 1) El plan de auditorías del año 2015 2) El resultado de las auditorías del año 2015 3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.
AD.6.2.2	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	A.18.2.2		PR.IP-12	1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información
AD.6.2.3	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3		ID.RA-1	Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.
RELACIONES CON LOS PROVEEDORES							
AD.7	Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES		A.15			

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI		PRUEBA
SEGURIDAD DE LOS RECURSOS HUMANOS							
AD.7.1	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	A.15.1	Modelo de Madurez Definido		1) Solicite la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nomina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor. 3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.
AD.7.2	Responsable de compras y adquisiciones	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	Modelo de Madurez Definido		1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Indague y evidencie como se gestionan 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, los incidentes de seguridad de la información y la revaloración de los riesgos. 2)

Anexo C: Levantamiento de área de la oficina de Gestión Tecnológica (Tendido de red, cableado y ubicación de dispositivos)