GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005:2011 ADAPTANDO LA *METODOLOGÍA MEHARI* PARA EL CASO DE ESTUDIO: PROCEDIMIENTO DE DESARROLLO Y MANTENIMIENTO DE APLICACIONES DE LA DIVISIÓN TIC DE LA UNIVERSIDAD DEL CAUCA

Anexos

Diego Fernando Calero Velasco
Jesús Eduardo Flores Quinayás

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistema
Grupo de Tecnologías de la Información (GTI)
Línea de Investigación: Seguridad Informática
Popayán, Junio de 2016

Tabla de Contenido

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

A. DEFINICIONES

A.1. ISO/IEC 27001:2013

La norma ISO/IEC 27001 es la norma que da las pautas para el establecimiento, operación, seguimiento, mantenimiento, y mejorara de un sistema de gestión de seguridad de la información SGSI [1]

Esta norma hace parte de las serie ISO 27000. La ISO/IEC 27001 provee los requerimientos que debe tener un SGSI. El modelo que sigue la ISO/IEC 27001 es el ciclo Deming, muy utilizado en las organizaciones ya que permite la mejora continua SGSI. Sus fases son: plan, do, check, act, la imagen muestra el ciclo Deming con cada una de sus fases.

Ilustración A-1. *Ciclo Deming de un SGSI*

Se debe tener claro, que para la certificación de cualquier organización en la norma ISO/IEC 27001 se debe tener lo siguiente:

- ✓ De los 10 incisos que tiene la norma, deben cumplirse completamente del inciso 4 al 10. Entiéndase por completo, incluso notaciones, párrafos, etc.

- ✓ Todos los controles de la norma ISO/IEC 27002:2013 que se hayan seleccionado para la declaración de aplicabilidad (SOA) en la etapa de planeación del SGSI.

Esto se evidencia con preguntas de auditoria.

A.2. ISO/IEC 27002:2013

La ISO/IEC 27002 es la norma que define los controles de seguridad de la información, esta norma está constituida por 14 dominios de seguridad, 35 objetivos de control y 114 controles. Esos controles de seguridad son los que se seleccionarán y se expondrán en el documento denominado declaración de Aplicabilidad (SOA) y su objetivo es disminuir las vulnerabilidades existentes en los sistemas de información en un nivel lo más mínimo posible. Siempre abran riesgos que quedan después de aplicar controles de seguridad este riesgo es denominado riesgo residual. El riesgo residual se conoce como el riesgo que queda después de aplicar un control de seguridad.

A.3. ISO/IEC 27003:2010

Esta norma provee una guía de implementación de un SGSI, en cada una de sus fases para cumplir con los requerimiento de la ISO 27001, en esta norma se detalla cada fase del ciclo Deming para la mejora continua y sus respectivos entregables.

A.4. ESTRATEGIA GOBIERNO EN LÍNEA

Gobierno en línea es el nombre que recibe la estrategia de gobierno electrónico en Colombia y busca prestar mejores servicios al ciudadano haciendo uso de las tecnologías de la información y las Comunicaciones TIC [1].

La estrategia actualmente trabaja 4 ejes temáticos los cuales son TIC para gobierno abierto, TIC para servicios, TIC para la gestión y por ultimo Seguridad y privacidad de la información.

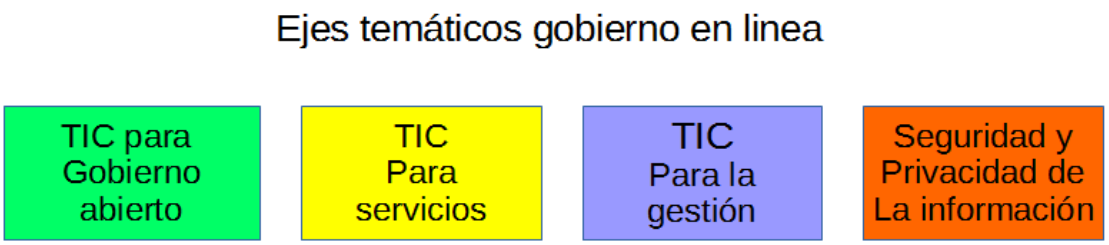


Ilustración A-2. *Ejes gobierno en linea*

A.4.1 TIC parar Gobierno Abierto

Lo que busca gobierno abierto es construir un estado más transparente y colaborativo, en donde los ciudadanos pueden participar activamente en la toma de decisiones haciendo uso de las tecnologías de la información y las comunicaciones.

Gobierno abierto promueve la participación de los ciudadanos poniendo a disposición diferentes medios de comunicación con el fin de llegar al ciudadano, busca involucrar al ciudadano por medio de las consultas ciudadanas y además busca que el ciudadano sea partícipe en la toma de decisiones.

Igualmente en gobierno abierto se busca la colaboración con el fin de que los ciudadanos, usuarios y diferentes grupos de interés puedan dar soluciones a las problemáticas o retos públicos que se presenten.

La transparencia busca que el ciudadano tenga acceso a toda la documentación pública de interés a través de los diferentes medios electrónicos, se pretende que el ciudadano sea un conocedor de los movimientos y las decisiones que se tomen al interior de las organizaciones públicas, es deber de las organizaciones difundir esta información pública por los diferentes medios de comunicación, de igual manera se ponen a disposición del ciudadano la rendición de cuentas qué busca

fomentar el diálogo y la retroalimentación entre las entidades el estado, usuarios, ciudadanos y grupos de interés se pone a disposición esta información por los diferentes medios electrónicos posibles. Las organizaciones deben publicar la información más relevante para el Ciudadano priorizando los de mayor impacto para ellos.

A.4.2 TIC para servicios

Buscar proveerle al ciudadano los mejores trámites y servicios en línea para responder a las diferentes necesidades.

Se busca que los ciudadanos tengan a su disposición formularios descargables, diligenciables y transaccionales, con el fin de que se pueda tramitar diferentes servicios haciendo uso de los formularios que las organizaciones ponen a su disposición por medios electrónicos, de la misma manera a cómo se realiza o se llenan formularios o registro de forma presencial, se da la información necesaria para la verificación y corrección de errores con el fin de lograr que las diligencias se hagan correctamente.

TIC Para servicios también busca que los usuarios internos o externos puedan gestionar certificaciones y constancias totalmente en línea, dando los registros de todos los datos necesarios para su respectivo trámite como su fecha de radicación, Información de los tiempos de respuesta, entre otros. De igual manera se le da respuesta a su indigencia y se le informa por medio de correo electrónico, además se busca que los usuarios gestionen de manera integrada los trámites y servicios agrupados por temáticas, intereses o poblaciones que están en cabeza de una o varias entidades de esta manera se provee una solución completa al usuario presentando una cara unificada del estado.

TIC para servicios provee un sistema integrado de peticiones, quejas reclamos y denuncias (PQRD) A través de un sistema web de contacto que permite hacer seguimiento y responder a las diferentes solicitudes teniendo en cuenta asimismo la ley vigente para sus respectivos trámites y respuestas, también se pone a disposición del ciudadano un canal de comunicación de peticiones quejas reclamos

y denuncias para ser tramitados a través de dispositivos móviles los cuales son muy usados por los ciudadanos igualmente se cumplen con los requerimientos y la ley vigente.

Se busca integrar y centralizar Las peticiones quejas reclamos y denuncias recibidas a través de los diferentes canales habilitados y desarrollar actividades de mejoramiento continuo a través de la evaluación de la satisfacción del usuario

TIC Para servicios busca servicios centrados en el usuario, identificando las necesidades del ciudadano caracterizándolos, de tal manera que las actividades de diseño, rediseño comunicación y mejoramiento de trámites y servicios respondan a las necesidades. Se busca la accesibilidad para que todos los ciudadanos tengan acceso a los recursos que se ponen a disposición, que todos puedan acceder a ellos incluso población con alguna discapacidad, se busca también la usabilidad con el fin de que todos los trámites y servicios puestos a disposición sean de fácil uso por los ciudadanos. Se busca la promoción con el fin de incentivar al personal a tramitar servicios en línea, se busca la evaluación de la satisfacción de los usuarios y finalmente se busca el mejoramiento continuo de acuerdo a la evaluación de la satisfacción de los usuarios del trámite y diligenciamiento de servicios.

A.4.3 TIC para la gestión

Busca dar un uso estratégico a la tecnología con el fin de hacer más eficaz la gestión administrativa, en ese sentido se busca la estrategia y la apropiación del uso de las tecnologías de la información y generar un cambio para la implementación de proyectos o iniciativas en tecnologías de la información, se busca establecer Implementar el monitoreo y evaluación del impacto de la estrategia del uso y la apropiación de los proyectos de tecnologías de la información.

TIC para la gestión Busca la apropiación de las tecnologías de la información y las comunicaciones para los objetivos de la organización, busca implementar servicios haciendo uso de las tecnologías de la información, también el uso eficiente del papel y la gestión de documentos electrónicos, la automatización de procesos y procedimientos

A.4.4 Seguridad y privacidad de la información

La seguridad y privacidad de la información busca garantizar que toda la información éste resguardada en cuanto a integridad confidencialidad y disponibilidad principios básicos de la seguridad de la Información.

Debido a que todos los servicios que se pretenden dar con la estrategia gobierno en línea se requiere que toda la información que será dispuesta al ciudadano y tramitada por los diferentes medios se haga de forma segura, tiene que haber un proceso de monitoreo y mejora continua en los procesos de gestión de la seguridad de la información y se requiere que se lleve a cabo un plan de gestión de seguridad de la información y que se defina el marco de seguridad y privacidad de la información

A.5. PROYECTOS GOBIERNO EN LÍNEA

Gobierno en línea actualmente viene trabajando en una serie de proyectos los cuales fortalecen la interacción del ciudadano y el gobierno, los proyectos que actualmente viene trabajando gobierno en línea se muestran en la imagen

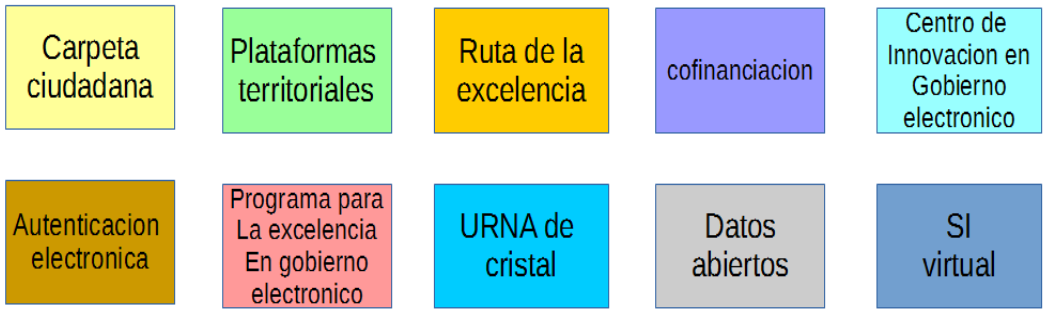


Ilustración A-3. *Proyectos de gobierno en linea*

A.5.1 Carpeta ciudadana

Con la carpeta ciudadana, Los colombianos podrán tener un espacio gratuito de almacenamiento en la nube para almacenar los documentos o registros que se generen en su relación con el estado a lo largo de su vida [1].

Todo ciudadano tendrá derecho a contar con un repositorio virtual dónde poder almacenar, recibir y compartir documentos e Información enviada por entidades públicas, y aquellos de interés personal, más importantes para interactuar con el estado. Todo anterior con los debidos estándares de seguridad de la información garantizando siempre que la propiedad de la información sea solamente del ciudadano.

Las metas que tiene el gobierno en línea con respecto a carpeta ciudadana es tener 50.000 usuarios para el 2016, 250.000 Para el 2017 y 500.000 Para el 2018 como se muestra en la gráfica

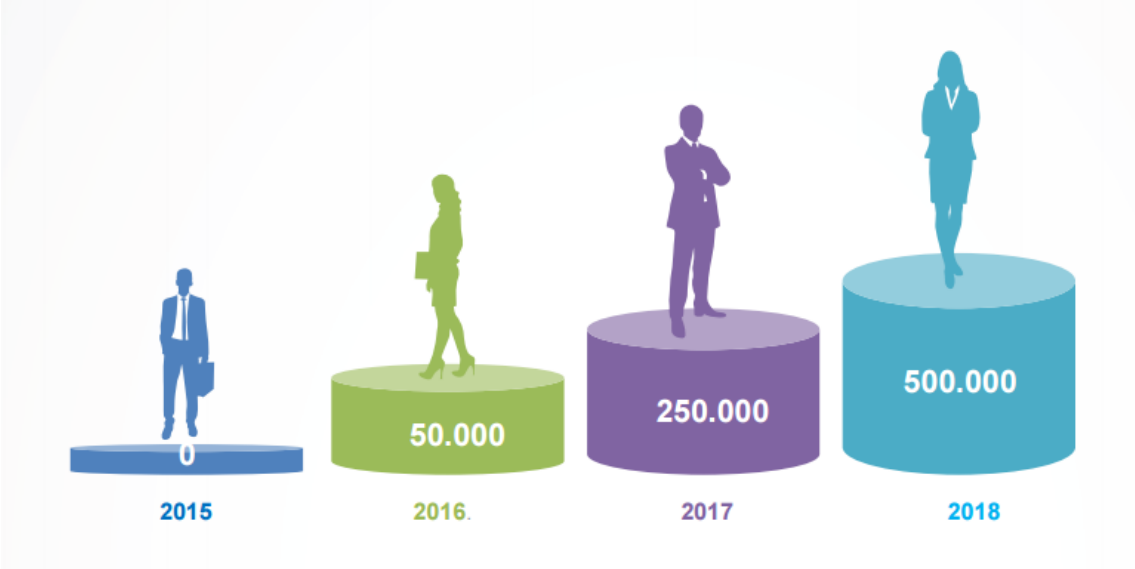


Ilustración A-4. *Proyecciones de gobierno en linea*

A.5.2 Ruta de la excelencia

Este proyecto prioriza Los trámites y servicios que más necesitan los colombianos en línea. 16 trámites y servicios, 3 proyectos de mejoramiento para la gestión y 6 proyectos para la apertura de datos, relacionados con los eventos más importantes en la vida de las personas y el desarrollo de las empresas integran este mapa.

El mapa de ruta lo que pretende es que el ciudadano pueda ingresar a las ofertas que el gobierno pone a disposición y que son las que más utilizan o necesitan los ciudadanos. Con esta iniciativa se busca que el ciudadano no tenga necesidad de desplazarse hacia un lugar en para tramitar documentos sino que lo pueda hacer cómodamente accediendo a internet y haciendo la respectiva diligencias desde su casa o de un sitio con acceso a internet

A.5.3 Cofinanciación

La cofinanciación de proyecto busca fortalecer La eficiencia de la administración pública con el apoyo de la Industria TI para la implementación de soluciones tecnológicas que mediante el desarrollo de actividades de ciencia tecnología e innovación mejore la prestación de los servicios a los ciudadanos y las empresas con acceso a datos abiertos para obtener información y lograr interacción con el fin de crear espacios de participación, generar visibilidad y transparencia. A través de incentivos se pretende fortalecer los proyectos en tecnología de la información. El gobierno saca convocatorias para aplicar a este tipo de financiación para proyectos TI

A.5.4 Centro de innovación el Gobierno electrónico

El centro Fortalece y dinamiza el ecosistema de innovación pública digital, de forma tal que se disponga tanto de herramientas, como de una comunidad de actores comprometidos con la sostenibilidad en la producción de innovaciones para resolver problemáticas públicas.

A.5.5 Autenticación electrónica

La autenticación electrónica será un servicio y permitirá reconocer a una persona y evitar suplantaciones, Cuando se adelanten trámites con el estado.

A.5.6 Programa para la excelencia de Gobierno electrónico

El programa para la excelencia de gobierno electrónico es una iniciativa en apoyo con el programa de Naciones Unidas (PNUD) qué busca fortalecer la capacidad del estado colombiano en materia de gobierno en línea y también promover Una cultura de Innovación en la gestión pública.

Este programa abre convocatorias para el fortalecimiento del conocimiento de gobierno en línea así como también otorga certificados a funcionarios públicos.

A.5.7 Urna de cristal

Urna de cristal es una iniciativa del gobierno nacional que lidera la estrategia de participación ciudadana electrónica y transparencia gubernamental. Urna de cristal actualmente funciona desde su lanzamiento en el año 2010, donde los colombianos pueden consultar avances, resultados e iniciativas del gobierno, y se pueden hacer llegar solicitudes inquietudes o aportes y de esta manera acercando al ciudadano con el estado haciéndolo partícipe en la toma de decisiones.

A.5.8 Datos abiertos

Con el proyecto de datos abiertos, el gobierno colombiano promueve la transparencia, El acceso a la información pública, la competitividad, el desarrollo

económico y la generación del impacto social a través de la apertura, reutilización de datos públicos, el uso y la apropiación de las TIC.

A.5.9 Seguridad de la información virtual

El *SI virtua*l es una plataforma web que busca resolver la problemática que enfrentan los ciudadanos cuando deben cumplir sus obligaciones con el estado para acceder a servicios provistos por el mismo.

En el sitio web que el gobierno nacional ha dispuesto a la ciudadanía se encuentran directorios que a veces es muy difícil encontrar, formularios para tramitar entre otros servicios que se ofrecen en el portal.

A.6. FASES DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

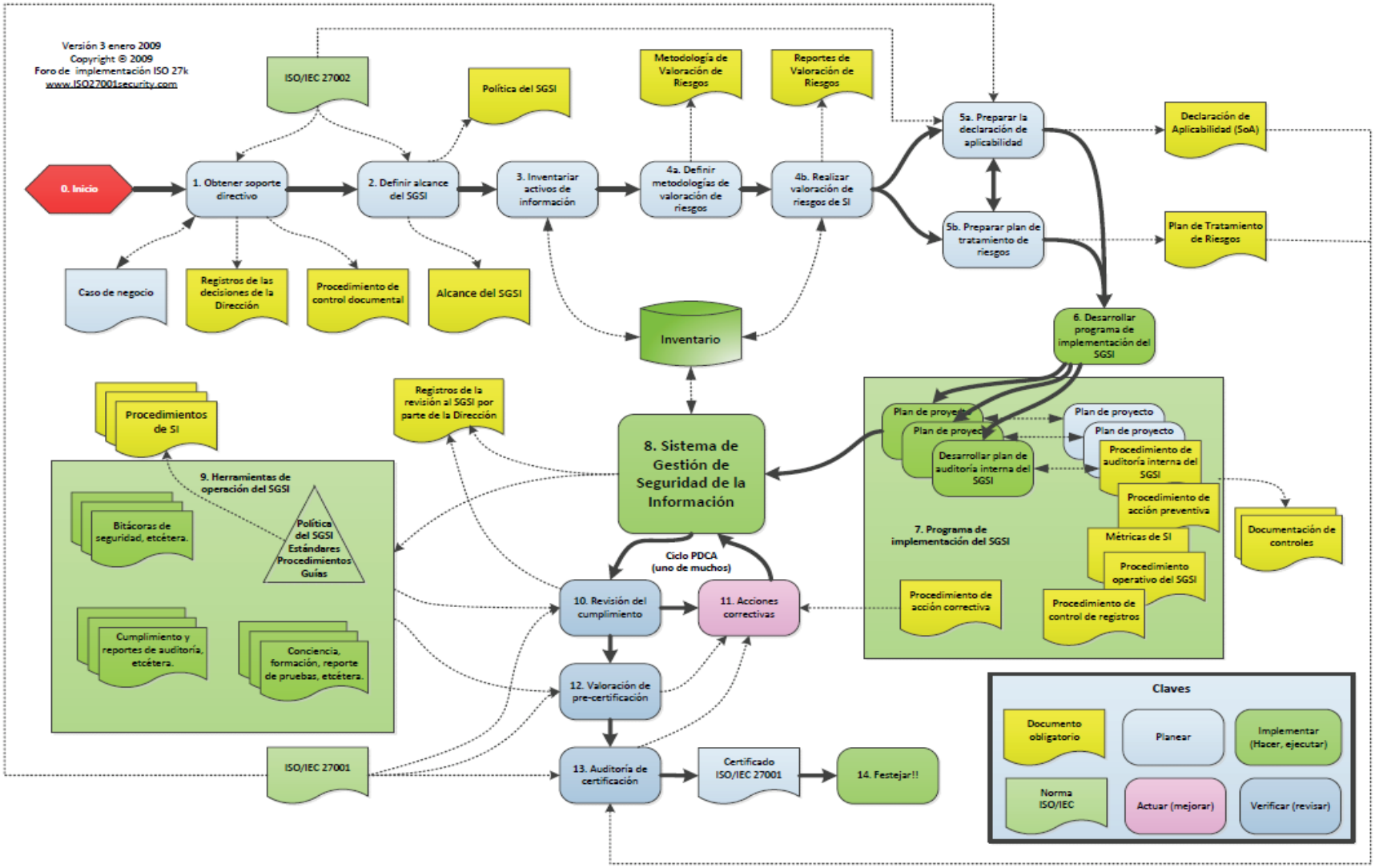


Ilustración A-5. *Proceso de implementación de SGSI ISO/EC27001*

A.6.1 Fase de planeación

La fase *PLAN* es la fase inicial de un SGSI esta se termina con el plan de tratamiento de riesgo y la declaración de aplicabilidad.

En la fase inicial la alta dirección debe estar consciente de la importancia de llevar a cabo un SGSI y de su iniciación, así como la disposición de la asignación de recursos que es muy importante. En esta fase se estudian los requerimientos de la organización, se realiza un plan de proyecto y un caso de negocio para que la dirección apruebe la realización del SGSI es importante que la alta dirección esté involucrada en todo el proceso, así como el resto del personal de la organización.

En la fase de planeación se definen el alcance y los límites de la organización que es donde se define que activos de información se tendrán en cuenta para la aplicación del SGSI, este establecimiento del alcance y los límites es muy importante y cualquier exclusión del alcance debe estar debidamente justificada.

En esta fase se define las políticas de gestión de seguridad de la información que serán las directrices que guiaran el SGSI, la políticas de seguridad es un documento que expone y que guía la implementación de un SGSI, es importante que tanto la dirección como el personal encargado de la administración de los activos aprueben estas políticas.

En la fase PLAN Se evalúan la organización en términos de la seguridad es decir cómo se encuentra la organización actualmente, también se identifican los requerimiento para la implementación de un SGSI.

Se clasifican los activos de información que en otras palabras es la materia prima del SGSI, para ser clasificados en cuanto a integridad, confidencialidad y disponibilidad, es importante hacer una análisis detallado para la clasificación de los activos, esta información se recoge realizando reuniones con el personal involucrado en las actividades de la organización.

La fase de gestión de riesgos se realiza definiendo una metodología que valore y haga la gestión del riesgo, existen varias metodologías para llevar a cabo esta fase.

Finalmente culminada la fase de planeación los entregables requeridos son el plan de tratamiento del riesgo y la declaración de aplicabilidad, el plan de tratamiento de riesgos define como se ejecutara la fase plan y como se realizara la asignación de recursos.

La declaración de aplicabilidad es un documento que lista los controles de seguridad que se implementarán con el fin de reducir los riesgos hasta un límite que sea aceptado por la organización, esta selección de controles de seguridad que lo provee la ISO/IEC son seleccionados de acuerdo a el análisis de riesgos.

A.7. TABLAS DE REPRESENTACIÓN DE VALORES MEHARI

Eficiencia de medidas disuasivas	
Nivel 4 el efecto de medidas disuasivas es muy alto	El posible atacante pude lógicamente considerar que los empleados deberían abandonar cualquier idea de la ejecución de una acción. Ellos deberían comprender que la realización será identificada y que el resultado de la sanciones más bien serán mayores que cualquier beneficio posible.
Nivel 3 el efecto de medidas disuasivas es alto	El posible atacante pude lógicamente considerar los empleados corren un alto riesgo. Ellos deberían darse cuenta de que sin duda lo que harán será identificado y que las sanciones serán duras.
Nivel 2 el efecto de medidas disuasivas es medio	El posible atacante pude lógicamente considerar que él o ella corren un pequeño riesgo. En cualquier caso cualquier posible prejuicio personal será soportable
Nivel 1 el efecto de medidas disuasivas es bajo o nulo	El posible atacante puede lógicamente considerar que él o ella no corren riesgos. Ellos pueden considerar que no serán identificados o que podrán usar argumentos fuertes para refutar cualquier acusación que tenga que ver con la acción realizada, o que cualquier castigo será muy leve.

Tabla A-1. *Medidas de disuasión en fase de tratamiento*

Eficiencia de medidas preventivas	
Nivel 4 el efecto de medidas preventivas es muy alto	Solo uno pocos y determinados expertos, con excepcionales recursos podría tener éxito. Solamente la ocurrencia de muy raros o circunstancia extremamente excepcionales permitirían que el escenario sucediera.
Nivel 3 el efecto de medidas preventivas es alto	Solamente un especialista o profesional con herramientas especiales o recursos o un grupo de profesionales en conspiración y utilizando sus conjuntos recursos y herramientas permitiría que sucediera.

Nivel 2 el efecto de medidas preventivas es medio	Un profesional puede accionar el escenario sin la necesidad de herramientas o recursos especiales fuera de los disponibles en la profesión. Raras circunstancias naturales pueden producir el mismo resultado
Nivel 1 el efecto de medidas preventivas es bajo o nulo	Cualquier persona en la organización, o cercano o incluso alguien que conozca algo de acerca de esto, es capaz de activar el escenario en mención, con los medios a su disposición (o fáciles de obtener) perfectamente circunstancias ordinarias pueden ser causa de este escenario (uso indebido, error, condiciones ordinarias desfavorables)

Tabla A-2. *Medidas de prevención en fase de tratamiento*

Eficiencia de medidas de protección o confinamiento	
Nivel 4 las medidas tienen un efecto muy fuerte	Las consecuencias directas podrán limitarse, el impacto residual será bajo e incluso no significativo
Nivel 3 las medidas de confinamiento tiene un importante efecto para el límite de las consecuencias directas	Los límites impuestos al escenario reducirán las consecuencias y los eventos serán rápidamente detectados, con inmediata reacción. Las medidas de protección que son usadas tendrán una real influencia sobre el impacto directo el cual queda limitado por el alcance y es manejable.
Nivel 2 el efecto del confinamiento y los límites de las consecuencias inmediatas es medio	El daño puede ser débilmente limitado en sus consecuencias directas si este es detectado, pero el tiempo de detección y reacción será largo. Las medidas de protección usadas tiene una real influencia en el resultado, pero las consecuencias directas son aún muy grandes.
Nivel 1 el efecto de medidas de confinamiento y los límites de las consecuencias inmediatas es muy bajo o nulo	Ambos el daño y las consecuencias directas no pueden ser limitados debido al retardo de detección o no podrá ser detectado por algún tiempo. Las medidas solamente tendrán unas influencias muy restrictivas sobre los niveles de las consecuencias directas.

Tabla A-3. *Medidas para confinamiento en fase de tratamiento*

EFICIENCIA DE MEDIDAS PALIATIVAS	
Nivel 4 el efecto de la limitación de las consecuencias directas son muy altas en realidad	La normal operación continúa sin ninguna notable interrupción.
Nivel 2 el efecto de la limitación de las consecuencias directas es alto	Las medidas paliativas no solamente han sido exactamente planeadas y organizadas sino además probadas y validadas. El tiempo del restablecimiento de la normal operación puede ser precisamente estimado o conocida, de tal manera que cuantificara la reducción de la gravedad de las consecuencias directas del escenario.
Nivel 3 el efecto de la limitación de las consecuencias directas es medio	La ayuda o solución paliativa ha sido ampliamente planeada pero el detalle se ha perdido. Esto puede ser considerado que, debido a la carencia de detalle habrá una correspondiente carencia de eficiencia o medidas

	paliativas. El tiempo de restablecimiento de la normal operación no puede ser precisamente predicha no será fundamentalmente cambiada la naturaleza del daño causado.
Nivel 1 el efecto de la limitación de las consecuencias directas es bajo o nulo	Ambas medidas totalmente improvisadas son usadas, o se considera que su efecto será bajo

Tabla A-4. *Medidas de paliación en fase de tratamiento*

A.8. DIAGRAMA DE FLUJO CASO DE ESTUDIO

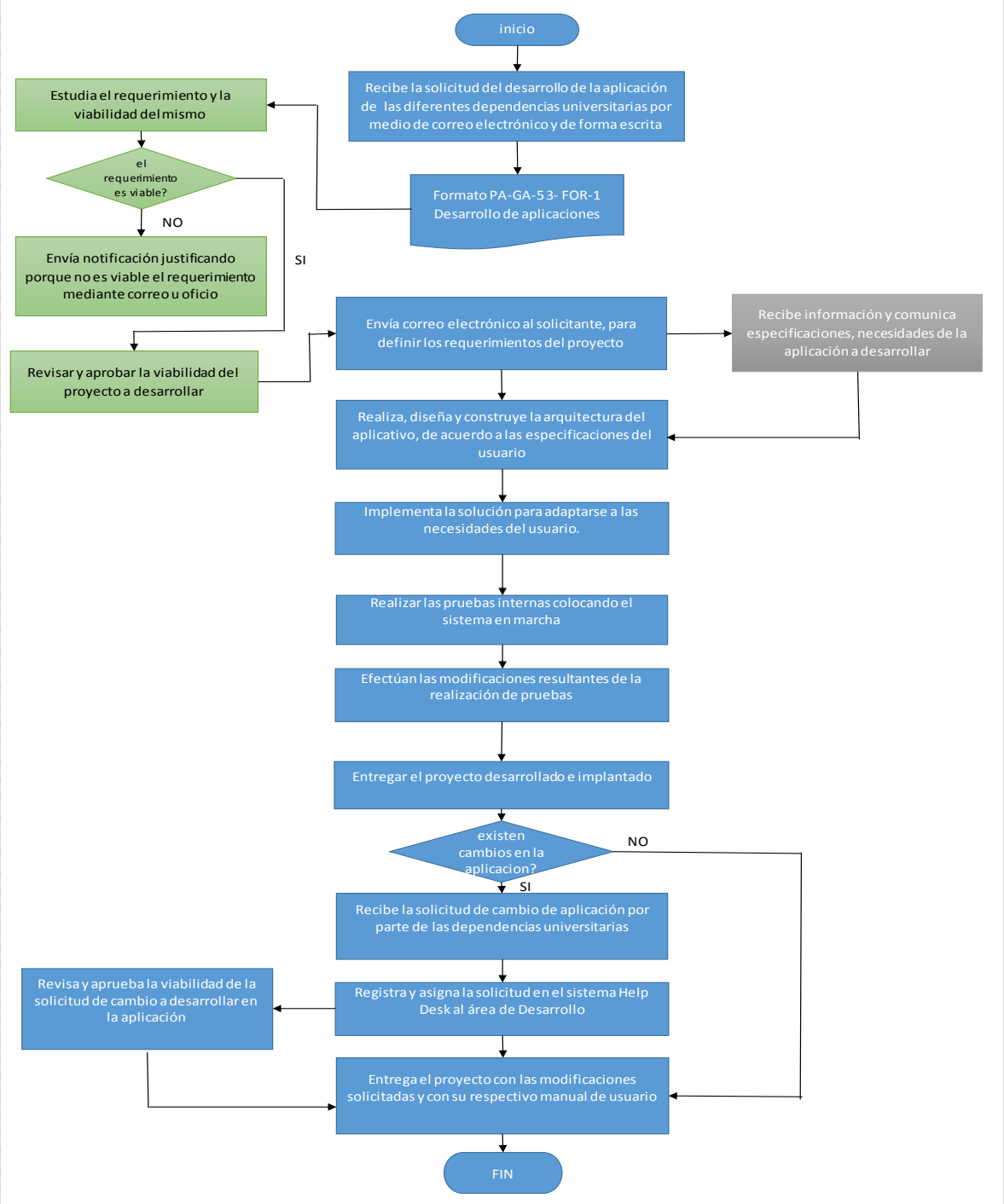


Ilustración A-6. *Diagrama de flujo del caso de estudio*

B. DOCUMENTACIÓN RELEVANTE RESPECTO AL SGSI DEL CASO DE ESTUDIO

B.1. CARACTERÍSTICAS DEL NEGOCIO

El procedimiento de desarrollo y mantenimiento de aplicaciones de la División TIC de la Universidad del Cauca se centra en la capacidad de solicitudes que pueden recibir y llevar a su completa terminación pasándolas por los procesos críticos de receptación, análisis, diseño, implementación y pruebas. Este procedimiento es el encargado de realizar las aplicaciones para uso universitario, es la única que se encarga de realizar mantenimiento a las aplicaciones, como también ajustes o modificaciones de las aplicaciones existentes.

El papel que juega este procedimiento dentro de la Universidad del Cauca es vital. Al momento de recibir nuevas solicitudes de parte de las dependencias universitarias, el equipo de desarrollo que recepciona es el encargado de pasar este requerimiento por las etapas críticas, como resultado se obtiene un código fuente que es de intelecto y autoría de la Universidad del Cauca. Este desarrollo llega a su finalidad cuanto la aplicación es implementada, probada y aceptada por el equipo de desarrollo. En este punto la aplicación pasa a la etapa de producción y publicación en otras áreas de la División de TIC de la Universidad del Cauca.

- ✓ **La organización**

El procedimiento de desarrollo y mantenimiento de aplicaciones hace parte de la Universidad del Cauca. Según el esquema organizacional de la Universidad del Cauca, este procedimiento pertenece a la División TIC y esta pertenece a la Vicerrectoría Administrativa, la Vicerrectoría Administrativa pertenece a la Rectoría y la Rectoría al Consejo Superior. Según el mapa de procesos universitarios, el área de desarrollo y mantenimiento se identifica con el procedimiento que tiene el mismo nombre del área, este procedimiento pertenece al subproceso, gestión de recursos tecnológicos, el cual pertenece al proceso gestión administrativa.

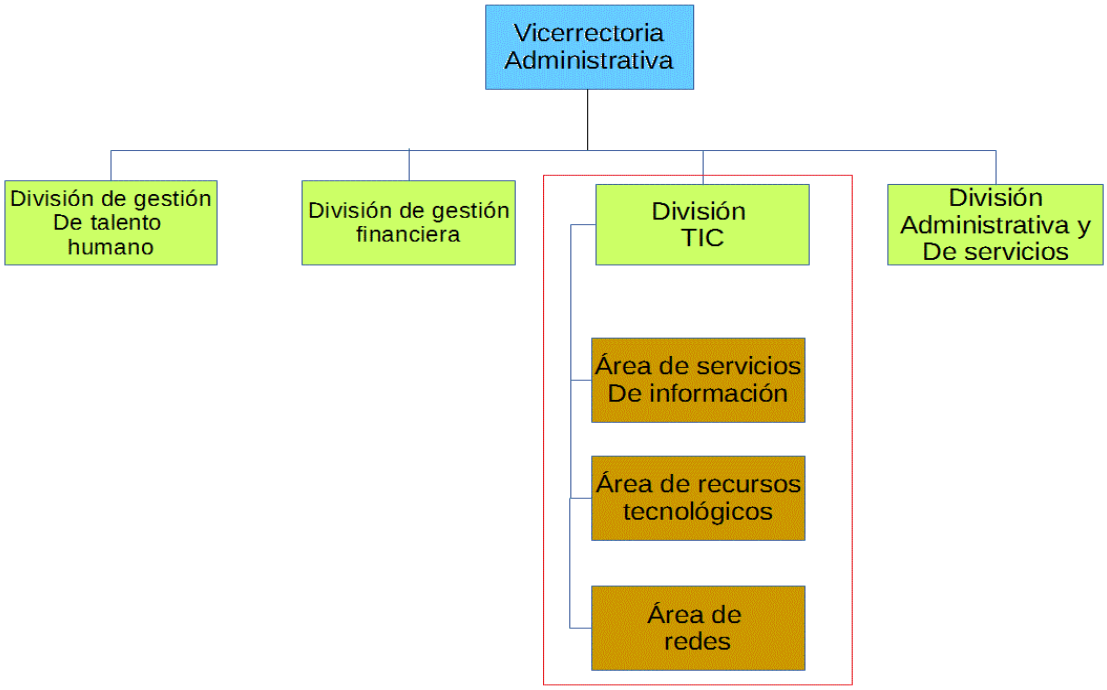


Ilustración B-1. *Esquema Organizacional de la división TIC*

✓ **Ubicación**

El área de desarrollo y mantenimiento de la División TIC de la Universidad del Cauca se encuentra en la Carrera 2N No. 3N – 111 en el edificio de la Facultad de Ciencias Naturales, Exactas y de la Educación en la ciudad de Popayán, Cauca, Colombia.

✓ **Tecnología**

La tecnología que utiliza, es tecnología asociada con la gestión del código, metodología Scrum y algunas relacionas con las buenas prácticas. Herramientas para guardar copia de repositorios remotos y para trabajo colaborativos.

B.2. ALCANCE PRELIMINAR DEL SGSI

Actualmente no existen obligaciones impuestas por la dirección con respecto a la seguridad de la información, es decir, en el procedimiento de desarrollo y

mantenimiento de aplicaciones no existe requisitos para gestionar la seguridad de la información.

Por otra parte existen obligaciones con entidades externas para la seguridad de la información nombradas en numeral 2.3. Las diferentes leyes de protección de datos impuestas por el gobierno que protege la información privada de los usuarios por lo que es un mandato superior relacionado con seguridad.

Dentro de los *procesos* críticos del negocio se encuentra el procedimiento de desarrollo y mantenimiento de aplicaciones procedimiento donde se podrían presentar fallos de seguridad graves que podrían involucrar a toda la organización y causar graves daños a la institución ya que este procedimiento *interactúa* con otros igualmente críticos tales como servidores que es donde finalmente se ejecutan las aplicaciones desarrolladas. En el procedimiento en cuestión se identifica el recurso humano: los desarrolladores como procedimiento crítico de la organización y del negocio, la rotación de personal que no es de planta, el código fuente y la documentación de dicho desarrollo son activos importantes para la organización, que se deben gestionar adecuadamente.

- ✓ **Roles y responsabilidades**

Según la norma ISO/IEC 27001:2013 se deben tener roles y responsabilidades dentro de un SGSI. Teniendo en cuenta lo dicho por esta norma y las recomendaciones que se da en ISO/IEC 27002 e ISO/IEC 27005. Se tiene:

ROL	DESCRIPCION DE LA RESPONSABILIDAD
Alta dirección(ENCARGADO)	Responsable de la visión, decisiones estratégicas y coordinación de las actividades para dirigir y controlar la organización.
Jefe de seguridad de la información (ENCARGADO)	Tiene responsabilidad y gobierno de la seguridad de la información, que asegura el manejo correcto de los activos de información.
Comité de seguridad de la información(ENCARGADOS)	Maneja los activos de la información y tiene el Rol de líder en el SGSI de la organización (Debe tener suficiente comprensión de la seguridad de la información, para dirigir, hacer seguimiento y llevar a cabo las tareas necesarias).

Administrador de sistemas (ENCARGADO)	El administrador de sistemas es responsable de un sistema TI
Propietarios de los activos	La persona debe estar consciente de la seguridad de la información y seguir lo lineamientos de las políticas internas establecidas
Auditorias de seguridad(ENCAEGADO)	Es la persona encargada de verificar que los controles implantados cumplen con los requerimientos según la norma.

Tabla B-1. *Roles y Responsabilidades*

Estos son los roles y responsabilidades mínimas que debe contar el SGSI.

B.3. CASO DE NEGOCIO Y PROPUESTA DE PROYECTO

El procedimiento de desarrollo y mantenimiento de aplicaciones es la encargada de diseñar y desarrollar aplicaciones que permitan dar solución a las diferentes dependencias universitarias que lo soliciten con el fin de optimizar los procesos en las diferentes dependencias universitarias. El procedimiento de desarrollo y mantenimiento de aplicaciones es un procedimiento crítica en cuanto a la seguridad de la información ya que este procedimiento es importante para el cumplimiento de los objetivos de la universidad del cauca a quien le da soporte y mantenimiento para la automatización de los diferentes procesos haciendo uso de las TIC, además dicho procedimiento está relacionado con diferentes dependencias y procesos dentro de la organización.

Un SGSI para la organización permitirá gestionar el riesgo en la seguridad de la información apoyando los requisitos de seguridad impuestos por la propia organización.

Un SGSI puede mejorar la eficiencia en la seguridad de la información y dar ventaja competitiva a la organización ya que entidades que poseen una certificación en seguridad de la información es mucho más competitiva y de confianza para los usuarios que una organización que no está certificada. Las organizaciones certificadas en ISO/IEC 27001 son organizaciones que dan más credibilidad en cuanto a la protección de los datos personales.

Un SGSI es indispensable para cualquier organización, si cualquier acceso no autorizado se presenta en la organización comprometería la reputación de esta además de generarle grandes pérdidas de dinero ya que existen leyes gubernamentales que la protegen como lo es la ley de protección de datos habeas Data. De ese modo la implementación de un SGSI aporta grandes beneficios a la organización, ya que evitara daños en la continuidad del negocio y al nombre institucional.

El procedimiento de desarrollo y mantenimiento de aplicaciones actualmente no cuenta con un SGSI que permita a la organización realizar las respectivas pruebas que para el caso deberían realizarse, se identifica en el procedimiento un déficit de apoyo por parte de las directivas. Al implementar un SGSI la organización tendrá grandes beneficios tales como permitir el desarrollo seguro de las actividades y al haber apoyo por la dirección se implementan los respectivos controles de seguridad.

- ✓ **Objetivos de negocio de la gestión de la seguridad de la información**

1. Conscientes de que existe un riesgo en el proceso de desarrollo y mantenimiento de aplicaciones se identifican como áreas críticas de la organización los desarrolladores. El implementar un sistema de gestión permitirá de una mejor manera gestionar el riesgo en la seguridad de la información, implementando los controles adecuados y realizando el seguimiento respectivo a las actividades de seguridad. De esta manera se logra reducir considerablemente el riesgo llevándolo a niveles por debajo del aceptable.

2. Un sistema de gestión de seguridad de la información permite mejorar la gestión de la seguridad ya que mediante una metodología clara y ordenada y el seguimiento de los requisitos básicos de la seguridad de la información, la implementación de controles y la mejora continua hacen eficiente el mantenimiento y la gestión de la seguridad en cualquier organización.

3. Un SGSI implica una ventaja competitiva puesto que genera confianza a los usuarios que hacen parte de la organización, por lo tanto empresas certificadas en ISO/IEC 27001 son mucho más confiables en cuanto a la

seguridad de la información ya que está avalado el organismo de estandarización internacional ISO/IEC.

- ✓ **Panorama general del proyecto**

Basado al objetivo de la organización y teniendo en cuanta algunos de los factores claves que se deben tener en cuenta para la seguridad de la información. Se propone implementar la fase de planeación de un SGSI al procedimiento de desarrollo y manteniendo de aplicaciones de la División TIC de la Universidad del Cauca, siguiendo los lineamientos de la serie de normas conocidas como ISO/IEC 27000 teniendo una metodología de análisis y evaluación de riesgos de los activos de la información la cual será MEHARI creada por la empresa CLUSIF la cual es de libre uso.

- ✓ **Antecedentes**

Se conoce que la implementación de un SGSI es cuestión de vital importancia para mantener seguros los activos de la información dentro de las organizaciones. Una organización que no cuente con un SGSI es una organización que tiene riesgos potencialmente altos para todos los activos de su información y conexo a esto, puede ser atacada por dentro o fuera de la misma, trayendo consigo pleitos jurídicos, desprestigio industrial, quedar por fuera de la competencia y numerosos gastos que la empresa no estaba esperando realizar.

Mientras que una organización que tenga correctamente implantado un SGSI, primeramente es una organización que ha tomado acciones frente a los posibles riesgos, que se ha realizado una evaluación de riesgos internos y externos, que se tiene un plan de tratamiento de riesgos, tiene controles para reducir los posibles riesgos para sus activos. Además, es una organización, que tiene una política clara de seguridad la cual puede referirse al personal para conocer exactamente como se debe tratar la información. Fuera de eso, esta organización aplica para la certificación de la norma ISO/IEC 27001 la cual le daría un importante sello de calidad y puede ser altamente competitiva en la industria.

- ✓ **Trabajo propuesto**

Claramente, se propone realizar la fase de planeación de la implementación de un SGSI para el procedimiento de desarrollo y mantenimiento de aplicaciones de la división TIC de la Universidad del Cauca. La completa implementación de un SGSI está determinado por el ciclo llamado “ciclo Deming”, el cual cuenta con cuatro fases la fase de planeación, implantación, verificación y actuación (o plan, do, check, act por sus siglas en ingles). Se llamada ciclo porque una vez se llegue a la actuación, el ciclo vuelve e inicia permitiendo tener constantes mejoras y modificaciones, para que la organización siempre cuente con políticas y plan de tratamientos actualizados.

Esta fase de planeación tiene como objetivos, valorar la situación actual de la organización, realizar una valoración de riesgos de los activos de la información para determinar cuáles de los activos críticos están en riesgo, realizar una implementación de una política de seguridad y por ultimo emitir dos documentos el primero un plan de tratamiento de riesgos y segundo una declaración de aplicabilidad de controles. Fuera de eso, entregar documentos (productos) que dicen la norma ISO/IEC 27003.

B.4. IMPORTANCIA Y BENEFICIOS DEL PROYECTO

- ✓ **Beneficios para la organización**

Un sistema de gestión de seguridad de la información (SGSI) permite la gestión del riesgo en cualquier organización protegiendo de manera adecuada los activos de información garantizando confidencialidad, integridad y disponibilidad de la información, preparando a la organización para cualquier incidente de seguridad.

La implementación de un SGSI en los procesos más críticos de la universidad tiene viabilidad y es adecuado ya que el implementar un SGSI a toda la organización es poco manejable, se deben identificar los procesos más críticos para considerar dentro del alcance y el proceso en consideración es uno de los más críticos dentro de la institución.

Los beneficios de la implementación de un SGSI también tienen que ver con la ventaja competitiva, una organización que gestione de manera adecuada el riesgo y cuide sus activos de información es mucho más confiable que una organización que no lo haga, en ese sentido la implementación de un SGSI es un beneficio para la organización.

Para el procedimiento de desarrollo y mantenimiento de aplicaciones la implementación de un SGSI permitirá llevar un mejor control del procedimiento incluyendo la seguridad, además obtener apoyo por parte de la dirección para la implementación de los controles, de esta manera permitir la continuidad del negocio y cumpliendo con los objetivos de la organización.

- ✓ **Proceso y factores críticos para alcanzar los objetivos del SGSI**

El procedimiento de desarrollo y mantenimiento de aplicaciones dentro del alcance es a quien se le aplicara el SGSI, este procedimiento está relacionado con otros procedimientos del área tecnológica, en el alcance se definirá claramente que abarca el SGSI.

Los factores críticos para alcanzar los objetivos del SGSI son:

1. *Concientización de parte de la dirección para implementar un SGSI:*
   Es muy importante que la dirección este consiente de la importancia de gestionar la seguridad de la información con un SGSI, sin el apoyo de la dirección es muy complicado que un SGSI siga adelante ya que es necesario apoyo humano y económico y es la dirección quien puede gestionar esto.

2. *Definir el alcance de manera correcta:*
   Una buena definición del alcance es clave para alcanzar el éxito en la implementación del SGSI. Definiendo claramente un alcance se delimita hasta donde abarca el SGSI.

3. *Una buena asesoría o acompañamiento para la implementación del SGSI:*
   Es necesario que para la implementación de un SGSI se cuente con personal capacitado para sacar adelante el proyecto. El personal capacitado es quien

dirigirá la implementación durante todo su proceso realizando el respectivo acompañamiento.

- ✓ **Limitaciones del alcance**

Dado el alcance de este trabajo de grado y no obstante el tiempo que se requiere para la completa implementación de un SGSI, se considera llevar a cabo el SGSI únicamente al procedimiento y mantenimiento de aplicaciones perteneciente al área de gestión de recursos tecnológicos en la fase de planeación del SGSI.

Una vez culminadas todas las salidas de esta fase de obtención de aprobación se procede a la siguiente fase, la cual es el alcance y límites del SGSI. Es necesario aclarar que adicional a todo lo anterior, existen dos precedentes, el primero el hecho de que las directivas propiamente de la Universidad del Cauca hayan emitido la Resolución 005 de 2015 [6], esto ya sería suficiente para determinar la aprobación y el compromiso con la implantación del SGSI. Y como segundo precedente, con el jefe de la División TIC y los autores de este trabajo de grado se firmó una carta de autorización y aprobación para iniciar el proceso del proyecto de la fase de planeación para el caso de estudio propuesto bajo las características que delimita este trabajo de grado. No obstante a estos dos precedentes, se cumplió cabalmente lo estipulado a la norma ISO/IEC 27003 en su fase 5.

B.5. PROCEDIMIENTOS RELACIONADOS CON EL CASO DE ESTUDIO

El área de recursos tecnológico de la división de las tecnologías de la información y las comunicaciones cuenta con 26 procedimientos bien definidos. Con el fin de poder determinar el alcance y los límites del SGSI se analizan cada uno de los 26 procedimientos identificando las relaciones con el procedimiento mantenimiento y desarrollo de aplicaciones.

La tabla muestra los 26 procedimientos resaltando los que están directamente relacionado con el procedimiento en estudio, estos procedimientos son categorizados dentro del diagrama de las elipses como procedimientos del área de

recursos tecnológicos, estos procedimientos son ubicados dentro de la elipse interior identificando sus interacciones y mostrando el flujo de la información.

Una vez identificados los procedimientos relacionados, se identifican que otra entidades o dependencia de la institución tiene alguna relación con el procedimiento, estas se ubicaran en la elipse intermedia del diagrama de las elipses, algunas dependencias involucradas con los procedimientos en cuestión están las facultades, DARCA, Vicerrectoría académica entre otros las cuales solicitan constantemente el desarrollo de aplicaciones para automatizar los procesos.

Finalmente se identifican las entidades externas a la institución que de alguna u otra forma tengan alguna relación con los procedimientos del área de recursos tecnológicos. Todas estas interacciones permitirán determinar los límites y el alcance del SGSI en la organización.

PROCEDIMIENTO	CÓDIGO	COMENTARIOS
Administración del centro de datos	PA-GA-5.3.PR-1	Es un procedimiento que está relacionado con el procedimiento de desarrollo y mantenimiento de aplicaciones(el procedimiento brinda las herramientas donde esta almacenada la información que manipulas las aplicaciones)
Gestión de servidores y servicio de Internet	PA-GA-5.3.PR-2	Es un procedimiento relacionado ya que es aquí donde se alojan las aplicaciones desarrolladas.
Gestión del servicio de acceso a internet	PA-GA-5.3.PR-3	Ninguna interacción.
Atención al Usuario	PA-GA-5.3.PR-4	Envió de peticiones a el procedimiento de desarrollo y mantenimiento de aplicaciones
Soporte y mantenimiento de sistemas de información	PA-GA-5.3.PR-5	Aquí existen sistemas de información con los cuales se comunica desarrollo y mantenimiento de aplicaciones (por ejemplo SQUID, o financiera) a veces se realizan cambios y eso afecta el procedimiento de DMA.
Implementación de nuevos servicios de infraestructura de red	PA-GA-5.3.PR-6	Ninguna interacción.
Desarrollo y mantenimiento de aplicaciones	PA-GA-5.3.PR-8	PROCEDIMIENTO EN ESTUDIO

Apropiación tecnológica "proteo"	PA-GA-5.3.PR-10	Ninguna interacción.
Plan de contingencia	PA-GA-5.3.PR-12	Información de eventos y anormalidades.
Gestión de proyectos TIC para la universidad del cauca	PA-GA-5.3.PR-13	El procedimiento solicita el desarrollo de proyectos a desarrollo y mantenimiento de aplicaciones.
Adquisición de aplicaciones Informáticas	PA-GA-5.3.PR-14	Ninguna interacción
Diseño y Desarrollo de productos y servicios Web	PA-GA-5.3.PR-15	Ninguna interacción
Vinculación de monitores	PA-GA-5.3.PR-16	El procedimiento solicita personal estudiantil para el apoyo a DMA o realizando pruebas.
Control de acceso físico a la división TIC	PA-GA-5.3.PR-17	Ninguna interacción
Adquisición de licencias de software para Datacenter	PA-GA-5.3.PR-18	Ninguna interacción
Auditorias de seguridad de la información	PA-GA-5.3.PR-19	Ninguna interacción
Seguridad de las redes de información	PA-GA-5.3.PR-20	Ninguna interacción
Creación de una nueva instancia en la base de datos	PA-GA-5.3.PR-21	Ninguna interacción
Recuperación de una Instancia	PA-GA-5.3.PR-22	Ninguna interacción
Monitoreo de dispositivos de la red de información	PA-GA-5.3.PR-23	Ninguna interacción
Optimización del funcionamiento de los dispositivos de la red de información	PA-GA-5.3.PR-24	Ninguna interacción
Acceso físico a centros de cableado	PA-GA-5.3.PR-25	Ninguna interacción
Configuración e instalación de dispositivos de red de información	PA-GA-5.3.PR-26	Ninguna interacción
Creación o modificación de datos y objetos en la base de datos	PA-GA-5.3.PR-27	Algunas veces se solicita colaboración a este procedimiento y realización de informes cuando lo haya realizado otra entidad.

Creación y verificación de copias de seguridad de los sistemas de información	PA-GA-5.3.PR-28	Ninguna interacción
Creación y verificación de copias de seguridad de bases de datos	PA-GA-5.3.PR-29	Ninguna interacción
Instalación y/o Activación de puntos de red	PA-GA-5.3.PR-30	Ninguna interacción

Tabla B-2. *Analisis de los activos del caso de estudio*

B.6. POLÍTICA DEL PROCEDIMIENTO DESARROLLO Y MANTENIMIENTO DE APLICACIONES

✓ **Políticas de seguridad de la información para el procedimiento desarrollo y mantenimiento de aplicaciones**

La información es el activo más importante en cualquier organización que haga uso de las tecnologías de la información y las comunicaciones, por lo tanto se debe garantizar la protección de los datos, la información cualquiera sea su forma en la que se encuentre: medios físicos, almacenada o en circulación por la red debe estar protegida contra accesos no autorizados a fin de garantizar Confidencialidad, Integridad y disponibilidad principios esenciales en la seguridad de la información.

Actualmente internet ha crecido de forma acelerada esto ha traído también gran cantidad de nuevos y sofisticados ataques. Estar bien protegidos debe ser objetivo primordial de las organizaciones para garantizar la continuidad del negocio, minimizar los riesgos y maximizar el retorno a la inversión.

✓ **Alcance**

Esta política apoya la política general de la Universidad del Cauca definida con respecto a la seguridad de la información y es válida solo para el procedimiento: **MANTENIMIENTO Y DESARROLLO DE APLICACIONES** del subproceso de Gestión de Recursos Tecnológicos de la Universidad del Cauca.

✓ **Objetivos**

1. Garantizar que los riesgos del procedimiento de desarrollo y mantenimiento de aplicaciones se traten adecuadamente a fin de que se mantenga el riesgo por debajo del nivel asumible por la organización.

2. Garantizar que los principios de seguridad de la información se apliquen en el procedimiento de desarrollo y mantenimiento de aplicaciones

3. Verificar que el procedimiento de desarrollo y mantenimiento de aplicaciones cumpla con la ley vigente en cuanto al tratamiento de los datos.

4. Proteger el procedimiento de desarrollo y mantenimiento de aplicaciones garantizando la continuidad de sus procesos de negocio.

✓ **Responsabilidades**

La dirección y el equipo de seguridad de la información deben garantizar la seguridad de la información y por lo tanto se debe velar por que la presente política sea de cumplimiento en el procedimiento de desarrollo y mantenimiento de aplicaciones.

Todos los miembros pertenecientes al procedimiento de desarrollo y mantenimiento de aplicaciones tienen las responsabilidades en cuanto a la seguridad de la información y estar consciente de esto en sus actividades de trabajo.

La respectiva dirección del área es responsable de asegurar que las personas que laboran bajo su control protejan la información de acuerdo con la normativa establecida por la organización y la que demanda el estado.

✓ **Beneficios**

La inversión en seguridad de la información suele ser por lo general muy elevada, el implementar un SGSI permitirá identificar los activos más críticos que requieren protección, permitiendo a la alta dirección invertir específicamente en los activos más importantes para la organización, minimizando costos de inversión.

La información estará debidamente protegida y se podrán tomar decisiones en caso de que ocurra un incidente de seguridad para poderse reparar en el menor tiempo posible de cualquier incidente de seguridad que afecte los procesos de negocio y la continuidad.

La organización estará protegida ante la pérdida de credibilidad y pérdidas económicas debido a cualquier fuga de información.

La organización mantendrá la disponibilidad, confidencialidad e integridad de la información evitando daños al nombre de la institución.

- ✓ **Políticas del procedimiento y Mantenimiento de Aplicaciones**

1. El procedimiento y mantenimiento de aplicaciones deberá ser responsable por la seguridad dentro de sus diferentes actividades a fin de garantizar los principios básicos de seguridad de la información, esto enmarcado dentro de la política general de seguridad de la información expedida por la universidad del cauca según resolución 785 de 2015.

2. Las responsabilidades de seguridad de la información deberán ser aceptadas por el personal involucrado en el procedimiento y mantenimiento de aplicaciones y deberán ser tenidas en cuenta dentro de sus actividades.

3. El procedimiento de desarrollo y mantenimiento de aplicaciones deberá velar por el control de acceso a los sistemas y aplicaciones.

4. El procedimiento y mantenimiento de aplicaciones protegerá la información que se genera dentro de sus actividades dentro de la organización desde documentación hasta código fuente de las aplicaciones entre otro tipo de información de carácter confidencial propio de la organización.

5. El procedimiento de desarrollo y mantenimiento de aplicaciones deberá garantizar la seguridad en los procesos de desarrollo y soporte.

6. El procedimiento de desarrollo y mantenimiento de aplicaciones deberá garantizar la seguridad en cuanto a la gestión de recursos humanos, en lo que

tiene que ver con la contratación, antes de la contratación, durante la contratación y finalizada la contratación del personal.

7. El procedimiento de desarrollo y mantenimiento deberá velar por el control y la gestión de claves de acceso a las aplicaciones, para el desarrollo de las aplicaciones así mismo para su mantenimiento.

8. El procedimiento de desarrollo mantenimiento deberá garantizar la seguridad en cuanto al control de acceso físico del personal a las instalaciones donde se llevan a cabo las actividades de desarrollo y mantenimiento de las aplicaciones.

9. El procedimiento de desarrollo y mantenimiento de aplicaciones deberá compartir documentación y código fuente de manera segura con el fin de garantizar la privacidad de la información evitando fuga de información.

B.7. REQUISITOS DE SEGURIDAD

Durante las entrevistas que se tuvieron con el encargo del procedimiento y el equipo de trabajo, se lograron identificar los activos. Respecto a lo que dice la norma ISO/IEC 27003, se le dio una clasificación en una escala de 1 a 5 respecto a:

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Disponibilidad

Para la clasificación de estos activos se tuvo en cuenta lo que recomienda el gobierno en su programa gobierno en línea [1]. También se tomó en cuenta el tipo de clasificación (primordial o no) y el propietario del activo.

NUMERO DE ACTIVO	PROCEDIMIENTO	NOMBRE DEL ACTIVOS	DESCRIPCIÓN	CLASIFICACIÓN	PROPIETARIO	VALORACIÓN		
						C	I	D

ACT01	DMA	Computador 1	Computador con alguna documentación	No primordial	Ing. oidor	3	3	2
ACT01	DMA	Computador 2	Computador donde se desarrollan las aplicaciones y se almacena el código fuente	primordial	Ing. oidor	5	5	3
ACT02	DMA	Computador 3	Computador donde se desarrollan las aplicaciones y se almacena el código fuente	primordial	Carlos C	5	5	3
ACT03	DMA	Computador 4	Computador donde se desarrollan las aplicaciones y se almacena el código fuente	primordial	Dustin M	5	5	3
ACT04	DMA	Computador 5	Computador donde se desarrollan las aplicaciones y se almacena el código fuente	primordial	Johani P	5	5	3
ACT05	DMA	Computador 6	Computador con información de carácter publico	No primordial	Rodrigo	2	2	1
ACT05	DMA	SIMCA DESKTOP	Servidor en donde se almacena el código fuente de SIMCA DESKTOP, los manejan los administrativos	primordial	Ing oidor	5	5	2
		Equipos de comunicación	Routers, switch para comunicación en la red local	primordial				5
ACT05	DMA	Unidades de backups	Copia de seguridad de SIMCA DESKTOP	primordial		5	5	2
ACT05	DMA	Código fuente de las aplicaciones	Se almacena el código en los PC			2	5	2
ACT05	DMA	Repositorios centralizado	Se almacena el código fuente de las aplicaciones			5	5	2
ACT05	DMA	Correo electrónico	Mediante correo electrónico se capturan los requisitos de desarrollo de las aplicaciones			3	4	1
ACT05	DMA	Almacenamiento online de la documentación (drive)	Medio mediante el cual se comparte documentación como código fuente de las aplicaciones	primordial		5	5	5

ACT05	DMA	aplicaciones	Aplicación objeto que se manda a los servidores para su puesta en funcionamiento			4	5	1
ACT05	DMA	provisional	Ingeniero encargado del área		Oidor	5		5
ACT05	DMA	Contratista 1	Personal de apoyo			2	2	2
ACT05	DMA	Contratista 2	Personal de apoyo			2	2	2
ACT05	DMA	Contratista 3	Personal de apoyo			2	2	2
ACT05	DMA	Contratista 4	Personal de apoyo			2	2	2
ACT05	DMA	Contratista 5	Personal de apoyo			2	2	2
ACT05	DMA	Provisional	Personal de apoyo		Rodrigo	2	2	2
ACT05	DMA	Monitorias de apoyo	Personal de apoyo			3	3	1
ACT05	DMA	Teléfono fijo						1
ACT05	DMA	Acceso a internet						3
ACT05	DMA	Energía						3

Tabla B-3. *inventario de activos respecto a los requisitos de seguridad*

B.8. NORMATIVA COLOMBIANA RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

B.8.1 Ley 1581 de 2012 protección de datos personales

La ley de protección de datos del gobierno nacional Colombiano garantiza que la información almacenada del ciudadano en cualquier base de datos de entidades de naturaleza pública o privada será única y exclusivamente de propiedad del usuario y no será divulgada para cualquier otro fin sin previa autorización.

La ley obliga a las organizaciones a tener en cuenta la seguridad de la información con el fin de evitar robo, perdida, fraude, adulteración, consulta no autorizada de la información de los usuarios. Cualquier falta a la información de los usuarios será

sancionada hasta por 2.000 salarios mínimos legales mensuales vigentes y suspensión del tratamiento de los datos hasta por un término de seis meses.

B.8.2 Conpes 3854 del 11 de abril de 2016

Colombia siempre ha presentado un déficit en cuanto a la seguridad de la información esto lo demuestran los estudios y encuestas realizadas por organizaciones internacionales, no obstante Colombia viene avanzando para que todas las organizaciones públicas y privadas del país tenga en cuenta la gestión del riesgo.

Un documento de política pública expedido actualmente por el gobierno Colombiano el 11 de abril de 2016 conocido como conpes 3854 rige las políticas nacionales de seguridad digital, es un avance del gobierno nacional con respecto a la seguridad de la información. El cambio de este conpes con respecto a la versión anterior, es que este obliga a las organizaciones a incluir dentro de sus procesos la gestión del riesgo en la seguridad de la información por los siguientes cuatro años a partir del regimiento de la norma.

B.8.3 Gobierno en línea.

El objetivo principal de gobierno en línea es prestar servicio al ciudadano colocando a su disposición diferentes medios electrónicos haciendo uso de las tecnologías de la información y comunicaciones, con el fin de que el ciudadano pueda hacer trámites y servicios, además de la publicación de datos abiertos y fomentar la participación en la toma de decisiones[1].

El programa tiene varios proyectos para su desarrollo como carpeta personal, en donde se pretende dar a cada ciudadano una carpeta en la nube en donde se lo pueda notificar, pueda tramitar entre otras cosas. Datos abiertos para que el

[1] Véase anexos A.4 y A.5.

ciudadano pueda estar enterado de todas las contrataciones de entidades públicas, y toma de decisiones. Urna virtual donde se fomenta la participación del ciudadano, entre muchos otros proyectos.

Gobierno en línea viene trabajando para que se gestione las TIC's[2] en las diferentes entidades públicas y privadas del país con el objetivo de tener información fácil y actualizada para el ciudadano, y en este sentido gobierno en línea en uno de sus objetivos fundamentales considera la seguridad de la información como un pilar fundamental en gobierno electrónico.

B.8.4 Normativa GEL

La normativa GEL es un programa de Gobierno en Línea que contiene todo el marco de norma general en cuanto a seguridad de la información. Este documento es la base normativa para todo lo relacionado con TIC's para el gobierno nacional, estas normas son un compendio de todas las normas vigentes para el territorio colombiano. No se trata exactamente de la creación de nuevas leyes o normativas, más bien, de la recopilación de ellas en cuanto a decretos, conpes, leyes constitucionales, etc.

Este documento tiene normativas respecto a:

- Acceso a la información
- Participación Ciudadana
- Privacidad, habeas data y protección de datos
- Seguridad de la información.
- Interoperabilidad
- Registros, expedientes y notificaciones electrónicas
- Documento y firma digital / electrónica
- Contratación electrónica

[2] Tecnologías de la Información y las Comunicaciones

B.8.5 Normativas a nivel institucional

La Universidad del Cauca consciente del cambio tecnológico y el incremento de la ciberdelincuencia ha tomado medidas para iniciar el proceso de gestión de la seguridad de la información, acordes a esto la Universidad del Cauca decreto las políticas de gestión de seguridad de la información según Resolución 785 de 2015 [6], que guía y son las directrices a seguir por las diferentes dependencias en donde se inicie el proceso de valoración y gestión del riesgo.

C. VALORACIÓN, TRATAMIENTO Y GESTIÓN DEL RIESGO MEHARI

C.1. FASE DE PREPARACIÓN PARA LA VALORACIÓN DE RIESGO

C.1.1 Evaluando el contexto

La metodología MEHARI exige tres puntos: Contexto Estratégico, Contexto Técnico y Contexto Estructural. Para satisfacer estas tres cosas en el documento [2], tiene una serie de pasos a realizar. Ahora si se compara con la norma ISO/IEC 27003 en la fase 5 “Obtener aprobación de la dirección para iniciar un proyecto de SGSI”. El cual esta fase tiene:

1. *Resumen de Objetivos del SGSI*
2. *Resumen de Características del negocio*
3. *Descripción de roles y responsabilidades a implementar el SGSI*
4. *Caso de Negocio*
5. *Propuesta de proyecto SGSI*
6. *Aprobación de un proyecto de SGSI*

Y MEHARI solicita:

1. *Contexto Estratégico.*
2. *Contexto Técnico.*
3. *Contexto Estructural.*

Los objetivos de MEHARI de este punto están escritos en la monografía 3.4.1 *"Evaluación del Contexto" pág. 44*.

En estos seis documentos[3] en la fase 5 de la norma se contemplan los pilares fundamentales para el conocimiento de la organización en todos los aspectos concernientes a un SGSI y por ende, a la seguridad de la información misma. Después de realizar un análisis entre los objetivos planteados por la metodología y los documentos de la norma en su fase 5, y después de verificar el contenido que tienen cada uno de ellos, se llega a la conclusión que la norma suple los requisitos básicos de la metodología. Debido a que, en la mayoría de los documentos de la norma se abarca una parte considerable de las exigencias de MEHARI, en estos documentos se conoce la organización.

C.1.2 Determinando el alcance y sus limites

Para completar este paso de MEHARI según lo dicho en el documento [2], se necesita determinar lo siguiente:

1. *Perímetros Técnicos*
2. *Perímetros Organizacionales*
3. *Estructura de Pilotaje*

Se entiende que la norma ISO/IEC 27003 en su fase 6 "Definir el alcance del SGSI, sus límites y la política de SGSI", contiene los siguientes documentos:

1. *Límites de la Organización para el SGSI*
2. *Alcance y Limites de las TIC*

[3] Estos documentos se traducen en actividades

3. *El alcance y los límites físicos*
4. *El alcance y límites del SGSI*
5. *Política del SGSI*

Los objetivos de MEHARI de este punto están escritos en la monografía 3.4.1 *"Determinar el alcance y límites" pág. 44*.

Los documentos solicitados para cumplir la norma representan claramente el alcance y límite del SGSI, ahora analizando estos documentos se puede ver que los objetivos de la metodología son cumplidos con estos documentos de la norma. Por lo tanto, se determina que la fase 6 de la norma este punto de la metodología.

C.1.3 Establecimiento los parámetros de riesgo principales

1. *Tabla de Aceptabilidad de Riesgo*
   Los valores de 1 y 2 son tolerables para MEHARI, pero los niveles 3 y 4 no lo son. El tratamiento de riesgo debe estar enfocado en aquellos escenarios que dieron como resultado de su valoración esta puntuación [3].

2. *Tabla de Exposición Natural*
   La tabla de exposición natural es una probabilidad intrínseca. Esta viene con eventos establecidos, estos eventos son seleccionados o no a consideración del auditor evaluador. MEHARI determina unos valores para esta tabla pero le da la opción al evaluador de determinar sus valores.

Tabla de eventos : Tipos de eventos y exposición natural				
Tipo de Familia	***Tipo de código***	***Descripción del Evento***	***Código***	***Exposición natural (estándar CLUSIF)***
	AB.P	Ausencia del personal socio	AB.P.Pep	3

Ausencia de personal debido a un accidente		Ausencia del personal interno	AB.P.Per	2
Ausencia o indisponibilidad de servicio, debido a un accidente	AB.S	Ausencia de servicio : Aire acondicionado	AB.S.Cli	2
		Ausencia de servicio : Fuente de alimentación	AB.S.Ene	3
		Ausencia de servicio : Imposibilidad de tener acceso a los establecimientos	AB.S.Loc	2
		Ausencia o imposibilidad de mantenimiento de software de aplicación	AB.S.Maa	3
		Ausencia o imposibilidad de mantenimiento del sistema de información	AB.S.Mas	2
Accidente grave del ambiente	AC.E	Tormenta Eléctrica	AC.E.Fou	2
		Fuego	AC.E.Inc	2
		Inundación	AC.E.Ino	3
Accidente de Hardware	AC.M	Averías del equipo	AC.M.Equ	3
		Averías de los accesorios del equipo	AC.M.Ser	3
Ausencia voluntaria del personal	AV.P	Conflicto social con huelga	AV.P.Gre	2
Error conceptual	ER.L	Software de bloqueo o mal funcionamiento debido a un diseño o error de programación (software interno)	ER.L.Lin	3
Error de Hardware o error de comportamiento por el personal	ER.P	Perdida u olvido de documento o media	ER.P.Peo	3
		Error de operación o de un no cumplimiento de un procedimiento	ER.P.Pro	3
		Error de ingreso datos o de estructura	ER.P.Prs	3
Incidente debido al ambiente	IC.E	Daños debidos al envejecimiento (de los equipos)	IC.E.Age	2
		Daños por agua	IC.E.De	3
		Daños por contaminación	IC.E.Pol	2
		Sobre carga eléctrica	IC.E.Se	2
Incidente lógico o funcional	IF.L	Incidente en producción	IF.L.Exp	3
		Software de bloqueo o mal funcionamiento (sistema de información o paquete de software)	IF.L.Lsp	2
		Saturación debido a una casa externa (gusano)	IF.L.Ver	3
		Virus	IF.L.Vir	4

Acción malévola (lógica o funcional)	MA.L	Bloqueo deliberado de cuentas	MA.L.Blo	2
		Eliminación deliberada o contaminación masiva de la configuración del sistema	MA.L.Cfg	2
		Eliminación deliberada de archivos, bases de datos o media	MA.L.Del	2
		Detector electromagnético	MA.L.Ele	3
		Corrupción deliberada de datos o funciones	MA.L.Fal	3
		Falsificación de mensajes o datos	MA.L.Fau	3
		Reproducción fraudulenta de transacción	MA.L.Rej	2
		Saturación deliberada de equipos TI o redes	MA.L.Sam	3
		Borrado total deliberado de archivos o copias de seguridad	MA.L.Tot	2
		Desviación de archivos o datos (tele-carga o copia)	MA.L.Vol	3
Acción malévola (física)	MA.P	Manipulación o falsificación de equipos	MA.P.Fal	2
		Terrorismo	MA.P.Ter	2
		Vandalismo o gamberrismo	MA.P.Van	2
		Robo de activos físicos	MA.P.Vol	2
Incumplimiento de los procedimientos	PR.N	Procedimientos inadecuados	PR.N.Api	2
		Procedimientos no aplicados debido a la falta de recursos o media	PR.N.Naa	2
		Procedimientos no aplicados debido a ignorancia	PR.N.Nam	2
		Procedimientos no aplicados deliberadamente	PR.N.Nav	2

Tabla C-1. *Valores de exposicion natural.*

3. Tabla de evaluación del riesgo

Se debe tener claro lo que dice en el documento en el numeral 3.4.1 de la monografía en *"Establecer parámetros de riesgos principales" pág. 47- 48* particularmente las definiciones que se proporcionan en cuento a paliativo, disuasión, prevención y confinamiento. Una vez se tenga claro que significa cada una de estas con sus respectivas tablas, se puede comprender mucho mejor las tablas de evaluación de riesgo.

En la *tabla C-3*, se observa arriba de cada sub tabla una nomenclatura “Expo” esto se refiere al punto anterior a la exposición natural. Según el valor que se le asignó a cada evento será el resultado de la disuasión, paliativo, prevención y confinamiento cuantitativamente.

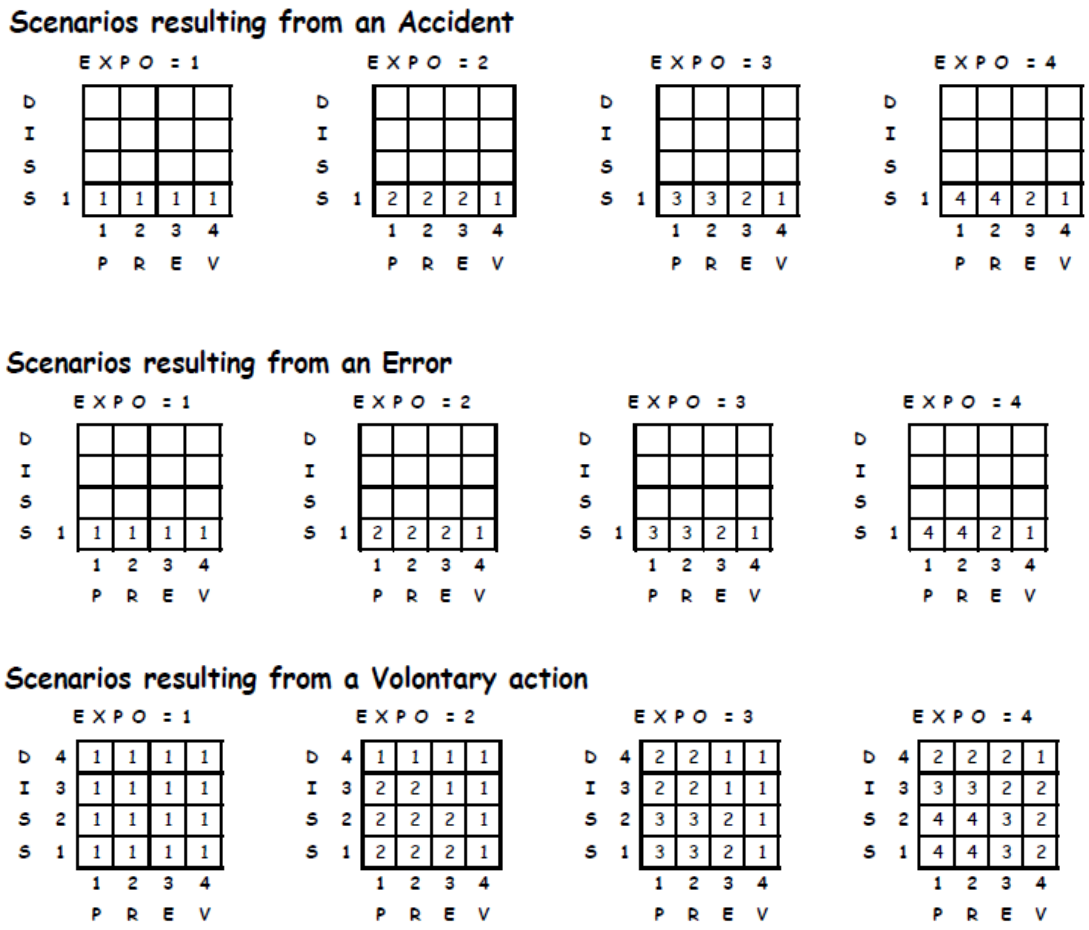
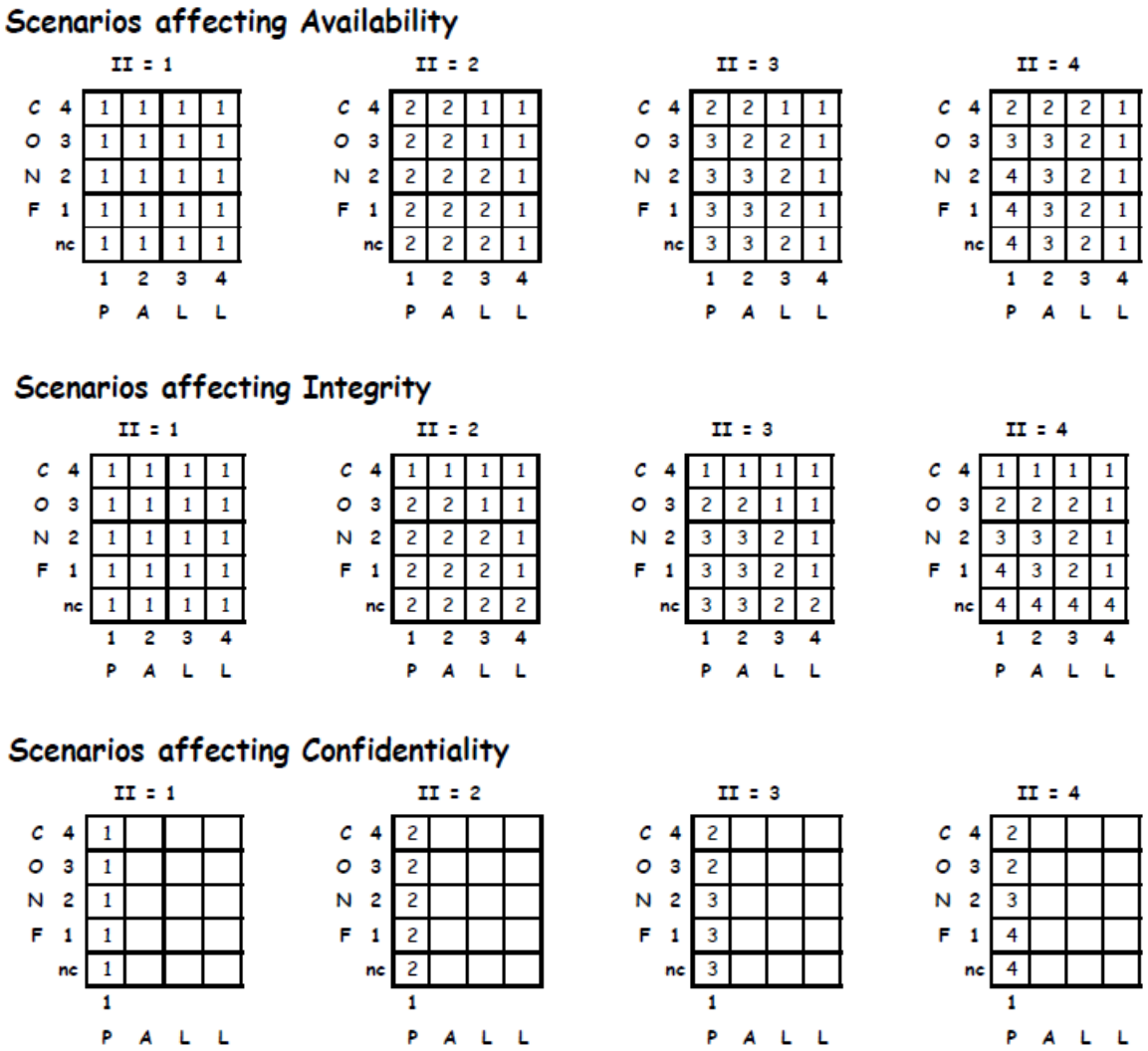


Tabla C-2. *Establecimiento de valores de aceptacion.*

Ahora para determinar la probabilidad y el impacto se utilizan las *tablas C-3 y C-4,* que según afirma el documento [5], la metodología tiene un cálculo automático de los valores que se determinen en la exposición natural, y la

valoración primaria de activos. Estos cálculos son automáticos de estas tablas y dan una valoración clara. Para desarrollar este punto mejor se puede dirigir al documento [3] en la sección 3.3.1 "*Proceso de identificación de un riesgo*" en la pág. 38-41.



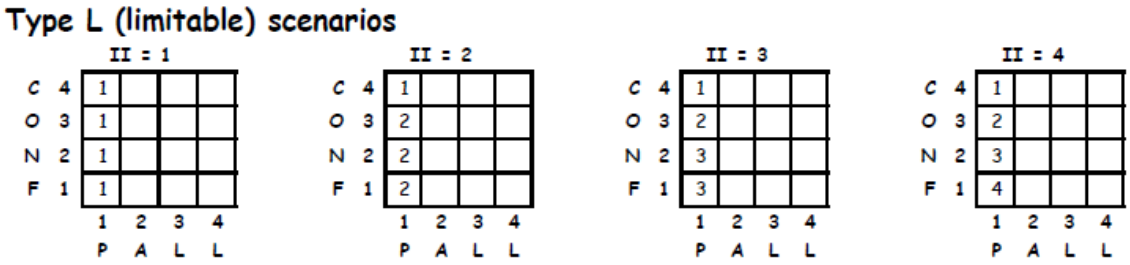


Tabla C-3. *Valores para determinacion de riesgos*

C.2. FASE OPERACIONAL – ANALIZANDO EL RIESGO

A continuación se presenta la guía de análisis y clasificación para el caso de estudio propuesto.

C.2.1 Clasificación de activos y análisis de cuestiones

1. *Escala de Valores de Malfuncionamiento*

   Las tablas se manejan de acuerdo a la importancia de los activos, estos se determinan según los requisitos de seguridad y según lo estipulado por MEHARI. Lo primero que se debe determinar son los valores de los mal funcionamientos. Para estos mal funcionamientos se deben tener en cuenta los activos de la organización y las actividades que se realizan en el procedimiento. Estas escalas de malfuncionamiento fueron determinadas por el personal del caso de estudio.

1.1. Identificación de las principales actividades y sus correspondientes objetivos

El enfoque de la metodología mehari en esta fase comienza con la identificación de las principales actividades en el dominio a ser analizado, que en este caso corresponde al procedimiento en estudio, en esta fase no solo se identifican las actividades sino que también los objetivos de las actividades y los resultados que se esperan de la actividad lo que se busca es reconocer los puntos de vista de la entidad con respecto a cada actividad.

Las funciones y los resultados esperados de cada función corresponden al procedimiento desarrollo y mantenimiento de aplicaciones.

Función	Objeticos y resultados esperados
Recepción de la solicitud del desarrollo de aplicación por parte de las dependencias universitarias, por medio de correo electrónico y de forma escrita.	Atender solicitudes de las diferentes dependencias universitarias, con el fin de iniciar los proyectos de desarrollo

***Tabla C-4**. Función 1 del procedimiento de estudio*

Función	Objeticos y resultados esperados
Registro y asignación de las solicitud en el sistema Help Desk al área de Desarrollo	Agilizar los procesos de solicitud de peticiones que permiten optimizar los tiempos de respuesta.

***Tabla C-5.** Función 2 del procedimiento de estudio*

Función	Objeticos y resultados esperados
Revisar y aprobar la viabilidad del proyecto a desarrollar	Revisar la viabilidad del proyecto y dar el visto bueno o no de la ejecución del proyecto.

***Tabla C-6.** Función 3 del procedimiento de estudio*

Función	Objeticos y resultados esperados
Enviar correo electrónico al solicitante, para definir los requerimientos del proyecto	Capturar los requisitos del cliente para la correcta ejecución de la aplicación.

***Tabla C-7.** Función 4 del procedimiento de estudio*

Función	Objeticos y resultados esperados
Realizar, diseñar y construir la arquitectura del aplicativo de acuerdo a las especificaciones del usuario.	Diseñar la solución como resultado final se tiene el diseño de la aplicación.

***Tabla C-8.** Función 5 del procedimiento de estudio*

Función	Objetivos y resultados esperados
Implementar la solución para adaptarse a las necesidades del usuario.	Implementación de la solución.

***Tabla C-9.** Función 6 del procedimiento de estudio*

Función	Objeticos y resultados esperados

Realizar las pruebas internas colocando el sistema en marcha. Verificar: Corrección de errores descubiertos. Mejoras de implementación, Identificar nuevos requisitos.	Realización de pruebas internas con el fin de detectar fallos en el software como resultado de esta actividad se tienen recomendaciones de mejoras.

Tabla C-10. *Función 7 del procedimiento de estudio*

Función	**Objeticos y resultados esperados**
Efectuar las modificaciones resultantes de la realización de pruebas.	Mejorar el software partiendo de errores encontrados como resultado de esta actividad se tiene el desarrollo de la aplicación con las modificaciones.

Tabla C-11. *Función 8 del procedimiento de estudio*

Función	**Objeticos y resultados esperados**
Entregar el proyecto desarrollado e implantado. **NOTA 4:** Todo proceso de desarrollo es documentado y guardado en forma virtual en un FTP y en la bodega de la División de Tic.	Entregar el aplicativo desarrollado que cumpla con las especificaciones del cliente.

Tabla C-12. *Función 9 del procedimiento de estudio*

Función	**Objeticos y resultados esperados**
Recibir la solicitud de cambio de aplicación por parte de las dependencias universitarias, por medio de correo electrónico y de forma escrita.	Mejora del aplicativo solicitado por el cliente.

Tabla C-13. *Función 10 del procedimiento de estudio*

Función	**Objeticos y resultados esperados**
Revisar y aprobar la viabilidad de la solicitud de cambio a desarrollar en la aplicación. **NOTA 6**: Si es factible hacer el cambio, se hace una copia a la aplicación, de lo contrario se informa por correo al usuario, Para seguir con la continuidad del procedimientos Ver actividades del ítem 6, 7, 8, 13	Revisión de solicitud de viabilidad de cambio

Tabla C-14. *Función 11 del procedimiento de estudio*

Función	**Objeticos y resultados esperados**
Entregar el proyecto con las modificaciones solicitadas e implantadas y con su respectivo manual de usuario.	Aplicativo desarrollado y entrega del manual de usuario.

NOTA 7: Todo proceso de desarrollo es documentado y guardado en forma virtual en un FTP y en la bodega de División de Tecnologías.	

Tabla C-15. *Función 12 del procedimiento de estudio*

1.2. Identificación de las malfunciones

Una vez que las principales actividades han sido identificadas se procede a identificar las malfunciones de cada actividad, una mal función es un proceso o actividad que no es realizada correctamente y que puede ser causante de que una amenaza se materialice.

La identificación de las malfunciones puede hacerse a nivel funcional o a nivel técnico, a nivel funcional se tiene un enfoque más general, a nivel técnico se entra en detalles en lo que tiene que ver con los activos de información que dan soporte a las actividades para poder llevar a cabo sus funciones, las malfunciones a nivel técnico serán descritas en términos de la degradación que puede ocurrir a nivel de los activos usados por los procesos y las consecuencias de tal degradación, en esta fase se realizara la identificación de las malfunciones a nivel técnico ya que esta provee un nivel más profundo de detalle.

Las malfunciones se deben identificar actividad por actividad, a continuación se identifican cada una de las actividades del procedimiento en estudio y las respectivas malfunciones identificadas, la descripción de las malfunciones ya sean definidas a nivel funcional o técnico pueden ser constituidas por medio de la entrevista con los administradores o responsables de las actividades. Las malfunciones presentadas a continuación se realizan a nivel técnico y con el criterio del personal del procedimiento en cuestión.

1. RECEPCIÓN DE LA SOLICITUD DEL DESARROLLO DE APLICACIÓN POR PARTE DE LAS DEPENDENCIAS UNIVERSITARIAS POR MEDIO DE CORREO ELECTRÓNICO Y DE FORMA ESCRITA.	
Malfunción	**consecuencias**
Indisponibilidad de correo electrónico	La indisponibilidad de correo electrónico no permite la recepción de la solicitud por parte del área de desarrollo.

Tabla C-16. *Malfuncionamientos de la actividad 1*

2. REGISTRO Y ASIGNACIÓN DE LAS SOLICITUD EN EL SISTEMA HELP DESK AL ÁREA DE DESARROLLO	
Malfunción	**consecuencias**
Divulgación de la información	La divulgación de la información del desarrollo de una aplicación por parte de help desk afectaría la confidencialidad de la información.
Error en el ingreso de la solicitud	El error en el ingreso de la solicitud retardaría las solicitudes de desarrollo.

Tabla C-17. *Malfuncionamientos de la actividad 2*

3. REVISAR Y APROBAR LA VIABILIDAD DEL PROYECTO A DESARROLLAR	
Malfunción	**consecuencias**
No relevante	no

Tabla C-18. *Malfuncionamientos de la actividad 3*

4. ENVIAR CORREO ELECTRÓNICO AL SOLICITANTE PARA DEFINIR LOS REQUERIMIENTOS DEL PROYECTO	
Mal función	**consecuencias**
Indisponibilidad de correo electrónico	La indisponibilidad del servicio de correo electrónico afectaría la comunicación para la captura de requisitos.
Robo de cuenta y captura de requisitos erróneo	El robo de cuenta podría afectar la correcta captura de requisitos lo que implicaría pérdida de trabajo en el desarrollo y pérdida de la confidencialidad.

Tabla C-19. *Malfuncionamientos de la actividad 4*

5. REALIZAR, DISEÑAR Y CONSTRUIR LA ARQUITECTURA DEL APLICATIVO DE ACUERDO A LAS ESPECIFICACIONES DEL USUARIO.	
Malfunción	**consecuencias**
Divulgación del sistema o arquitectura	La divulgación del sistema o la arquitectura de la aplicación tendrían consecuencia en cuanto a la confidencialidad.

Tabla C-20. *Malfuncionamientos de la actividad 5*

6. IMPLEMENTAR LA SOLUCIÓN PARA ADAPTARSE A LAS NECESIDADES DEL USUARIO.

Malfunción	consecuencias
Herramientas de desarrollo no disponibles (software y hardware)	La indisponibilidad de las herramientas y equipos de desarrollo no permitirían la realización de las actividades
Personal de desarrollo no disponible	Si el personal de desarrollo no está disponible la respuesta a las solicitudes de desarrollo no se puede llevar a cabo, esto sería muy crítico para la organización.
Indisponibilidad de la red interna	La indisponibilidad de la red interna no permite accede a el almacenamiento en los repositorios internos y la comunicación interna.
Fallas en el suministro energético	Las fallas en el suministro eléctrico no permiten que las actividades se lleven a cabo.
Errores o bugs en el código fuente	Una mala codificación de las aplicaciones podría ocasionar fallas en los sistemas que podrían ser explotadas por una amenaza, cuando sean ejecutados por los servidores
Indisponibilidad de internet	La indisponibilidad de la red para el acceso a internet no permite llevar a cabo las tareas de forma eficiente, debido a que no se permite la búsqueda de información ni acceder a los repositorios en línea.
Divulgación de la información(almacenamiento en línea)	El almacenamiento de la documentación y el código fuente de las aplicaciones podría perderse o divulgarse debido a un mal almacenamiento.
Perdida de archivos almacenados a nivel interno	El almacenamiento no seguro pude ocasionar la perdida de la información(confidencialidad e integridad)

Tabla C-21. *Malfuncionamientos de la actividad 6*

7. REALIZAR LAS PRUEBAS INTERNAS COLOCANDO EL SISTEMA EN MARCHA. VERIFICAR: CORRECCIÓN DE ERRORES DESCUBIERTOS. MEJORAS DE IMPLEMENTACIÓN, IDENTIFICAR NUEVOS REQUISITOS.	
Malfunción	**consecuencias**
Perdida de la documentación almacenada en línea	La pérdida de documentación almacenada en línea podría ocasionar la divulgación de la información.
Perdida de integridad y privacidad de la información almacenada localmente	La pedida de la información en cuanto a privacidad e integridad tiene consecuencias graves para la organización.

Tabla C-22. *Malfuncionamientos de la actividad 7*

8. EFECTUAR LAS MODIFICACIONES RESULTANTES DE LA REALIZACIÓN DE PRUEBAS.	
Malfunción	**consecuencias**
Herramientas de desarrollo no disponibles (software y hardware)	La indisponibilidad de las herramientas y equipos de desarrollo no permitirían la realización de las actividades
Personal de desarrollo no disponible	Si el personal de desarrollo no está disponible la respuesta a las solicitudes de desarrollo no se puede llevar a cabo, esto sería muy crítico para la organización.

Tabla C-23. *Malfuncionamientos de la actividad 8*

9. ENTREGAR EL PROYECTO DESARROLLADO E IMPLANTADO. NOTA: TODO PROCESO DE DESARROLLO ES DOCUMENTADO Y GUARDADO EN FORMA VIRTUAL EN UN FTP Y EN LA BODEGA DE LA DIVISIÓN DE TIC.	
Malfunción	**consecuencias**
Perdida del almacenamiento en línea	El acceso al desarrollo de las aplicaciones y la documentación desde cualquier dispositivo incluso teléfonos móviles, puede ocasionar la perdida de la información afectando la privacidad y la integridad de la información.
Perdida del almacenamiento local	El almacenamiento en medios físicos o discos extraíbles a nivel local puede perderse y ser robado si no se almacena adecuadamente.

Tabla C-24. *Malfuncionamientos de la actividad 9*

10. RECIBIR LA SOLICITUD DE CAMBIO DE APLICACIÓN POR PARTE DE LAS DEPENDENCIAS UNIVERSITARIAS, POR MEDIO DE CORREO ELECTRÓNICO Y DE FORMA ESCRITA.	
Mal función	**consecuencias**
Indisponibilidad de correo electrónico	No grave

Tabla C-25. *Malfuncionamientos de la actividad 10*

11. REGISTRAR Y ASIGNAR LA SOLICITUD EN EL SISTEMA HELP DESK AL ÁREA DE DESARROLLO.	
Malfunción	**consecuencias**
Divulgación de la información	La divulgación de la información del desarrollo de una aplicación por parte de help desk afectaría la confidencialidad de la información.
Error en el ingreso de la solicitud	El error en el ingreso de la solicitud retardaría las solicitudes de desarrollo.

Tabla C-26. *Malfuncionamientos de la actividad 11*

12. REVISAR Y APROBAR LA VIABILIDAD DE LA SOLICITUD DE CAMBIO A DESARROLLAR EN LA APLICACIÓN. NOTA : SI ES FACTIBLE HACER EL CAMBIO, SE HACE UNA COPIA A LA APLICACIÓN, DE LO CONTRARIO SE INFORMA POR CORREO AL USUARIO, PARA SEGUIR CON LA CONTINUIDAD DEL PROCEDIMIENTOS VER ACTIVIDADES DEL ÍTEM 6, 7, 8, 13	
Malfunción	**consecuencias**
No relevante	ninguna

Tabla C-27. *Malfuncionamientos de la actividad 12*

13. ENTREGAR EL PROYECTO CON LAS MODIFICACIONES SOLICITADAS E IMPLANTADAS Y CON SU RESPECTIVO MANUAL DE USUARIO. NOTA: TODO PROCESO DE DESARROLLO ES DOCUMENTADO Y GUARDADO EN FORMA VIRTUAL EN UN FTP Y EN LA BODEGA DE DIVISIÓN DE TECNOLOGÍAS.	
Malfunción	**consecuencias**
Acceso a la información almacenada debido a la inexistencia de instalaciones físicas seguras para el almacenamiento de la información.	El acceso a la información almacenada por parte de personal no autorizado puede afectar de manera grave la integridad de la información y la confidencialidad.
Acceso a la información almacenada en drive de las aplicaciones y la documentación.	El acceso a las aplicaciones almacenada y la documentación desde diferentes dispositivos puede ocasionar las perdida de integridad y confidencialidad incluso la disponibilidad al existir la posibilidad del borrado de toda la información

Tabla C-28. *Malfuncionamientos de la actividad 13*

1.3. Evaluación de la gravedad de las malfunciones identificadas

La tercera fase en la escala de valores de malfuncionamiento es evaluar la gravedad de cada una de las malfunciones identificadas anteriormente, para hacer esto una escala estándar de gravedad es usada como referencia la cual la provee mehari y se describe a continuación. Mehari maneja cuatro niveles de la gravedad o criticidad, estos son etiquetados de 1 a 4 como se muestra en la tabla con su correspondiente significado.

Escala estándar del nivel de impacto	
Nivel 4 vital	A este nivel el impacto es muy serio incluso para la continuidad de la organización (o al menos una de sus principales actividades) está en peligro, estaría la organización acarreando con un malfuncionamiento, esto sería grave y las consecuencias muy críticas.
Nivel 3 muy serio	A este nivel el impacto es considerado muy serio para la entidad, pero en un futuro no sería un riesgo, en términos económicos esto tendría un impacto negativo sobre las

	ganancias por un periodo de tiempo, aunque no sería una enorme pérdida para los socios.
Nivel 2 serio	Las malfunciones a este nivel tendrían un claro impacto sobre las operaciones de la entidad, resultados o imagen, pero es globalmente manejable
Nivel1 insignificante	A este nivel cualquier resultado dañino no tendría un impacto significativo sobre los resultados o imagen de la entidad, incluso si algún miembro de empleados fuera fuertemente involucrado en el restablecimiento del estado original.

Tabla C-29. *Escala del nivel de impacto*

La identificación del criterio de las malfunciones y la identificación de los limites críticos se lleva a cabo con los administradores de la organización del procedimiento en estudio es sucesivas entrevistas y encuestas.

1. RECEPCIÓN DE LA SOLICITUD DEL DESARROLLO DE APLICACIÓN POR PARTE DE LAS DEPENDENCIAS UNIVERSITARIAS POR MEDIO DE CORREO ELECTRÓNICO Y DE FORMA ESCRITA.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Indisponibilidad de correo electrónico	Indisponibilidad por un más de una hora			

Tabla C-30. *Valoración de malfuncionamientos de la actividad 1*

2. REGISTRO Y ASIGNACIÓN DE LAS SOLICITUD EN EL SISTEMA HELP DESK AL ÁREA DE DESARROLLO				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Divulgación de la información	La información es divulgada dentro de la institución por una persona	La información es divulgada dentro de la institución y conocida por muchas personas	La información es divulgada fuera de la institución	

Tabla C-31. *Valoración de malfuncionamientos de la actividad 2*

3. REVISAR Y APROBAR LA VIABILIDAD DEL PROYECTO A DESARROLLAR				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
no				

Tabla C-32. *Valoración de malfuncionamientos de la actividad 3*

4. ENVIAR CORREO ELECTRÓNICO AL SOLICITANTE PARA DEFINIR LOS REQUERIMIENTOS DEL PROYECTO				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Indisponibilidad de correo electrónico	Indisponibilidad por una hora	Indisponibilidad por más de dos horas		
Robo de cuenta y captura de requisitos erróneo				

Tabla C-33. *Valoración de malfuncionamientos de la actividad 4*

5. REALIZAR, DISEÑAR Y CONSTRUIR LA ARQUITECTURA DEL APLICATIVO DE ACUERDO A LAS ESPECIFICACIONES DEL USUARIO.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Divulgación del sistema o arquitectura, almacenamiento en línea de la información.	La información es accedida y divulgada por personal dentro de la institución			La información es accedida y divulgada por fuera de la institución

Tabla C-34. *Valoración de malfuncionamientos de la actividad 5*

6. IMPLEMENTAR LA SOLUCIÓN PARA ADAPTARSE A LAS NECESIDADES DEL USUARIO.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Herramientas de desarrollo no disponibles (software y hardware)	Las herramientas no están disponibles por más de una hora	Las herramientas no están disponibles por más de 3 horas	Las herramientas no están disponibles por un día	Las herramientas no están disponibles por una semana
Personal de desarrollo no disponible			Falta de un personal de desarrollo	Falta de todo el personal de desarrollo
Indisponibilidad de la red interna	Indisponibilidad de la red interna por más de una hora	Indisponibilidad de la red por más de dos horas	Indisponibilidad de la red interna por más de 6 oras	Indisponibilidad de la red interna por más de un día
Fallas en el suministro energético	Falla por una hora	Falla por más de una hora	Falla por más de 6 horas	Fala por más de un día

Errores o bugs en el código fuente	Involucra solo un modulo		Involucra todos los módulos	Involucra todo el sistema
Indisponibilidad de internet		Indisponibilidad por una hora	Indisponibilidad por más de 6 horas	Indisponibilidad por más de un día
Divulgación de la información(almacenamiento)		La información del desarrollo es divulgada dentro de la organización		La información del desarrollo pude ser divulgada por fuera de la institución
Perdida de archivos almacenados			Perdida de algunos archivos de información	Perdida de todos los archivos de la aplicación

Tabla C-35. *Valoración de malfuncionamientos de la actividad 6*

7. REALIZAR LAS PRUEBAS INTERNAS COLOCANDO EL SISTEMA EN MARCHA. VERIFICAR: CORRECCIÓN DE ERRORES				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Perdida de la documentación almacenada en línea			Perdida de parte de la información almacenada en línea	Perdida de toda la información almacenada
Perdida de integridad y privacidad de la información almacenada localmente			Perdida de parte de la información almacenada localmente	Perdida de toda la información almacenada localmente

Tabla C-36. *Valoración de malfuncionamientos de la actividad 7*

8. EFECTUAR LAS MODIFICACIONES RESULTANTES DE LA REALIZACIÓN DE PRUEBAS.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Herramientas de desarrollo no disponibles (software y hardware)	Las herramientas no están disponibles por más de una hora	Las herramientas no están disponibles por más de 3 horas	Las herramientas no están disponibles por un día	Las herramientas no están disponibles por una semana
Personal de desarrollo no disponible			Falta de un personal de desarrollo	Falta de todo el personal de desarrollo

Tabla C-37. *Valoración de malfuncionamientos de la actividad 8*

9. ENTREGAR EL PROYECTO DESARROLLADO E IMPLANTADO. NOTA: TODO PROCESO DE DESARROLLO ES DOCUMENTADO Y GUARDADO EN FORMA VIRTUAL EN UN FTP Y EN LA BODEGA DE LA DIVISIÓN DE TIC.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Perdida del almacenamiento en línea			Perdida de parte de la información almacenada en línea	Perdida de toda la información almacenada
Perdida del almacenamiento local			Perdida de parte de la información almacenada localmente	Perdida de toda la información almacenada localmente

Tabla C-38. *Valoración de malfuncionamientos de la actividad 9*

10. RECIBIR LA SOLICITUD DE CAMBIO DE APLICACIÓN POR PARTE DE LAS DEPENDENCIAS UNIVERSITARIAS, POR MEDIO DE CORREO ELECTRÓNICO Y DE FORMA ESCRITA.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
no				

Tabla C-39. *Valoración de malfuncionamientos de la actividad 10*

11. REGISTRAR Y ASIGNAR LA SOLICITUD EN EL SISTEMA HELP DESK AL ÁREA DE DESARROLLO.				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Divulgación de la información	La información es divulgada dentro de la institución por una persona	La información es divulgada dentro de la institución y conocida por muchas personas	La información es divulgada fuera de la institución	

Tabla C-40. *Valoración de malfuncionamientos de la actividad 11*

12. REVISAR Y APROBAR LA VIABILIDAD DE LA SOLICITUD DE CAMBIO A DESARROLLAR EN LA APLICACIÓN. NOTA : SI ES FACTIBLE HACER EL CAMBIO, SE HACE UNA COPIA A LA APLICACIÓN, DE LO CONTRARIO SE INFORMA POR CORREO AL USUARIO, PARA SEGUIR CON LA CONTINUIDAD DEL PROCEDIMIENTOS VER ACTIVIDADES DEL ÍTEM 6, 7, 8, 13				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**

no				

Tabla C-41. *Valoración de malfuncionamientos de la actividad 12*

13. ENTREGAR EL PROYECTO CON LAS MODIFICACIONES SOLICITADAS E IMPLANTADAS Y CON SU RESPECTIVO MANUAL DE USUARIO. **NOTA: TODO PROCESO DE DESARROLLO ES DOCUMENTADO Y GUARDADO EN FORMA VIRTUAL EN UN FTP Y EN LA BODEGA DE DIVISIÓN DE TECNOLOGÍAS.**				
Malfunción	**Nivel 1 insignificante**	**Nivel 2 serio**	**Nivel 3 muy serio**	**Nivel 4 vital**
Acceso a la información almacenada debido a la inexistencia de instalaciones físicas seguras para el almacenamiento de la información.			Se obtiene un acceso por parte de personal no autorizado dentro de la institución.	Se obtiene un acceso por parte del personal no autorizado fuera de la institución
Acceso a la información almacenada en drive de las aplicaciones y la documentación.			Se obtiene un acceso por parte de personal no autorizado dentro de la institución.	Se obtiene un acceso por parte del personal no autorizado fuera de la institución

Tabla C-42. *Valoración de malfuncionamientos de la actividad 13*

2. *Clasificación de Activos*

De los documentos [3] y [5] se tiene:

Exposición natural para el riesgo	
Nivel 1 exposición muy baja	Independientemente de cualquier medida de seguridad la probabilidad de que un escenario dado pueda ocurrir es muy bajo y prácticamente insignificante.
Nivel 2 baja exposición	Incluso sin ninguna medida de seguridad en absoluto la combinación de los entornos (culturales, humanos, geográficos etc.) y el contexto (estratégico, competitivo, social etc.) hacen que la probabilidad de un escenario dado ocurra en un corto o mediano plazo, pero igualmente bajo
Nivel 3 medio expuesto	El entorno y contexto de la empresa son tales que, si nada se ha hecho para evítalo un escenario dado está obligado a suceder en un plazo más o menos corto
Nivel 4 altamente expuesto	El entorno y contexto de la empresa son tales que, si nada se ha hecho para evitar un escenario dado es probable que suceda en un plazo corto.

Tabla C-43. *Niveles para medición los riesgos de exposición natural*

Escala estándar del nivel de impacto

Nivel 4 vital	A este nivel el impacto es muy serio incluso para la continuidad de la organización (o al menos una de sus principales actividades) está en peligro, estaría la organización acarreando con un malfuncionamiento, esto sería grave y las consecuencias muy críticas.
Nivel 3 muy serio	A este nivel el impacto es considerado muy serio para la entidad, pero en un futuro no sería un riesgo, en términos económicos esto tendría un impacto negativo sobre las ganancias por un periodo de tiempo, aunque no sería una enorme pérdida para los socios.
Nivel 2 serio	Las malfunciones a este nivel tendrían un claro impacto sobre las operaciones de la entidad, resultados o imagen, pero es globalmente manejable
Nivel 1 no significativo	A este nivel cualquier resultado dañino no tendría un impacto significativo sobre los resultados o imagen de la entidad, incluso si algún miembro de empleados fuera fuertemente involucrado en el restablecimiento del estado original.

Tabla C-44. *Escala estándar del nivel de impacto*

Escala estándar del nivel de probabilidad	
Nivel 4 muy probable	A este nivel es razonable que el escenario pueda suceder casi certeramente y probablemente a corto plazo. Cuando el riesgo ocurra a nadie debería tomar por sorpresa.
Nivel 3 probable	Este nivel corresponde a los escenarios que podrían suceder en un plazo más o menos corto. Se podría esperar aún que los riesgos no sucedieran pero más bien siendo optimistas. El entorno y contexto de la empresa estaría como que: *si nada se ha hecho para evitar el riesgo, el escenario dado es obligado a suceder en un plazo más o menos corto.*
Nivel 2 improbable	A este nivel es razonable pensar que estos escenarios podrían no ocurrir. Las experiencias pasadas muestra que no pueden ocurrir, sin embargo se pueden listar como irrealista.
Nivel 1 muy improbable	En este nivel la potencialidad del riesgo aparece como muy bajo. Pero estos escenarios no son estrictamente imposibles porque siempre hay un pequeño residuo de probabilidad de ocurrencia

Tabla C-45. *Escala para probabilidad*

Con la información recolectada en el inciso anterior, se procede a realizar la valoración de activos y análisis de cuestiones con sus tres categorías:

Clasificación de Datos

Tabla T1			**CLASIFICACIÓN DE DATOS**																													
Actividades de la Organización o procesos, **Servicios comunes**	**FUNCIÓN** **(descripción)**	**Selección si 1**	**Datos de Aplicación (bases de datos)**			**Datos de aplicación sensible de forma individual (transitoria, Mensajes)**			**Datos de oficina compartidos**			**Datos de oficina Personal**			**Documentos personales**		**Listados o impresiones**	**Correo electrónico**			**Correo postal Fax**			**Documentos archivados**		**Archivos digitalizados**			**Datos de web en línea (exteno o interno)**		
			A	**I**	**C**	**A**	**I**	**C**	**A**	**I**	**C**	**A**	**I**	**C**	**A**	**C**	**C**	**A**	**I**	**C**	**A**	**I**	**C**	**A**	**C**	**A**	**I**	**C**	**A**	**I**	**C**
	Tipo de Activo		**D 01**	**D 01**	**D 01**	**D 06**	**D 06**	**D 06**	**D 02**	**D 02**	**D 02**	**D 03**	**D 03**	**D 03**	**D04**	**D04**	**D05**	**D 07**	**D 07**	**D 07**	**D 08**	**D 08**	**D 08**	**D09**	**D09**	**D 10**	**D 10**	**D 10**	**D 11**	**D 11**	**D 11**
Procesos o actividades de la organización																																
Actividad 1: recepción solicitud de desarrollo (correo y escrito)	Correo Electrónico	1													2	2		**3**	**3**	**3**												
Actividad 2: registrar solicitud en HELP DESK	Correo Electrónico	1																														
Actividad 3: revisar y aprobar Viabilidad proyecto	Correo Electrónico	1																														
Actividad 4: envío de correo para definir los requerimientos del proyecto	Correo Electrónico	1				**3**	**3**	**3**	2	2	2	2	2	2				**3**	**3**	**3**												
Actividad 5: realizar, diseñar, construir la arquitectura del aplicativo de acuerdo a los requerimientos	PC de Desarrollo, Unidades de Backups	1	**3**	**3**	**3**	**3**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	2	2		**3**	**3**	**3**												

Actividad 6: implementar la solución para adaptarse a la necesidades del usuario	PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositorio Centralizado, SIMCA DESKTOP	1	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**			2	2	2															
Actividad 7: realizar pruebas internas (corrección de errores mejoras de implementación, identificación de nuevos requisitos)	Aplicaciones	1	2	2	2	2	2	2	**3**	**3**	**3**	**3**	**3**	**3**	2				**3**	**3**	**3**															
Actividad 8: efectuar modificaciones de la anterior actividad	PC de Desarrollo	1	**3**	**3**	**3**	2	2	2	**3**	**3**	**3**	**3**	**3**	**3**	**3**				**3**	**3**	**3**															
Actividad 9: entrega del proyecto desarrollado	Aplicaciones, Código Fuente de las Aplicaciones, Repositorios Centralizados	1	**4**	**4**	**4**	**3**	**3**	**3**	2	2	2	**3**	**3**	**3**	**3**	**3**																			
Actividad 10: solicitud de cambio de aplicación.	Correo Electrónico	1	2	2	2	2	2	2	2	2	**3**	**3**	**3**	**4**	**4**	**3**			**3**	**3**	2	2	2	2	2	1									
Actividad 11: registrar solicitud anterior en el sistema help desk al área de desarrollo	Correo Electrónico	1																																
Actividad 12: renviar y aprobar la viabilidad de la solicitud del cambio	Correo Electrónico	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3																		

Actividad 13: entrega del proyecto desarrollado e implantado (documentación y copias de seguridad)	Correo Electrónico, Help Desk, Repositorios Centralizado	1																														
Procesos Transversales		1																														
Monitorias de Apoyo(vinculación de monitores)	Monitoria de Apoyo	1	2	2	3	2	2	2	1	1	1	1	1	1	1	1		1	1	1												
Atención al Usuario (Atención al Usuario)	Correo Electrónico	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1		1	1	1												
Equipos de Comunicación y Soporte (soporte y mantenimiento de sistemas de información)	SIMCA DESKTOP, Equipos de Comunicación	1	4	4	4	4	4	4	2	2	2	2	2	2	2	2		2	2	2												
Contratación de Personal (vicerrectoría académica)	Personal Área de Desarrollo y Mantenimiento	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2		2	2	2												
Administración / política general		1																														
Clasificación Junta			4	4	4	4	4	4	4	4	4	4	4	4	4	3		3	3	3	2	2	2	2	1							
Clasificación por actividades seleccionadas			4	4	4	4	4	4	4	4	4	4	4	4	4	3		3	3	3	2	2	2	2	1							

Tabla C-46. *Tabla de clasificacion de datos T1*

Clasificación de Servicios

Tabla T2			**CLASIFICACIÓN DE SERVICIOS**

Actividades de la Organización o procesos, **Servicios comunes**	**FUNCIÓN (descripción)**	**Selección**	**Servicios de redes extendidas**		**Servicios de redes de área local**		**Servicios de aplicación**			**Servicios compartidos de oficina**		**Eliminación de los equipos de los usuarios**	**Servicios TI (Sistemas, periféricos, etc.)**		**Servicio de edición de Web**		**Servicios comunes, ambiente de trabajo**	**Serivicios de Telecomunicaciones**	
			A	**I**	**A**	**I**	**A**	**I**	**C**	**A**	**I**	**A**	**A**	**I**	**A**	**I**	**A**	**A**	**I**
	Tipo de Activo		**R01**	**R01**	**R02**	**R02**	**S01**	**S01**	**S01**	**S02**	**S02**	**S03**	**S04**	**S04**	**S05**	**S05**	**G01**	**G02**	**G02**
Procesos o actividades de la organización																			
Actividad 1: recepción solicitud de desarrollo (correo y escrito)	Correo Electrónico	1	2	2	2	2	**3**	**3**	**3**	2	2	2	2	2			2		
Actividad 2: registrar solicitud en HELP DESK	Correo Electrónico	1	2	2	2	2	2	2	2	2	2	2	2	2			2	2	2
Actividad 3: revisar y aprobar Viabilidad proyecto	Correo Electrónico	1																	
Actividad 4: envío de correo para definir los requerimientos del proyecto	Correo Electrónico	1	**3**	**3**						**3**	**3**								
Actividad 5: realizar, diseñar, construir la arquitectura del aplicativo de acuerdo a los requerimientos	PC de Desarrollo, Unidades de Backups	1	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**3**					
Actividad 6: implementar la solución para adaptarse a la necesidades del usuario	PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositorio Centralizado, SIMCA DESKTOP	1			**3**	**3**	**3**	**3**	**3**	**3**	**3**	**4**							
Actividad 7: realizar pruebas internas (corrección de errores mejoras de implementación, identificación de nuevos requisitos)	Aplicaciones	1					2	2	2	2	2								

Actividad 8: efectuar modificaciones de la anterior actividad	PC de Desarrollo	1			**3**	**3**	**3**	**3**	**3**	2	2	**4**					2	2	2
Actividad 9: entrega del proyecto desarrollado	Aplicaciones,Código Fuente de las Aplicaciones, Repositorios Centralizados	1	**3**	**3**	**3**	**3**													
Actividad 10: solicitud de cambio de aplicación.	Correo Electrónico	1	2	2	2	2	2	2	2	2	2	2	2	2					
Actividad 11: registrar solicitud anterior en el sistema help desk al área de desarrollo	Correo Electrónico	1																	
Actividad 12: renviar y aprobar la viabilidad de la solicitud del cambio	Correo Electrónico	1	**3**	**3**	**3**	**3**													
Actividad 13: entrega del proyecto desarrollado e implantado (documentación y copias de seguridad)	Correo Electrónico, Help Desk, Repositorios Centralizado	1																	
Procesos Transversales		1																	
Monitorias de Apoyo(vinculación de monitores)	Monitoria de Apoyo	1	2	2	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**				**3**	**3**
Atención al Usuario (Atención al Usuario)	Correo Electrónico	1	**3**	**3**	2	2	**3**	**3**	**3**	1	1	1	1	1				1	1
Equipos de Comunicación y Soporte (soporte y mantenimiento de sistemas de información)	SIMCA DESKTOP, Equipos de Comunicación	1	**3**	**3**	**4**	**4**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**			**3**	**3**	**3**
Contratación de Personal (vicerrectoría académica)	Personal Área de Desarrollo y Mantenimiento	1	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**			**3**	**3**	**3**
Administración / política general		1																	
Clasificación Junta			3	3	4	4	4	4	4	4	4	4	3	3			3	3	3

Clasificación por actividades seleccionadas			3	3	4	4	4	4	4	4	4	4	3	3			3	3	3

Tabla C-47. *Valoracion de la clasificacion de Servicios T2*

Clasificación de Cumplimientos

Tabla T3			**CLASIFICACIÓN DEL CUMPLIMIENTO DE LA LEGISLACIÓN Y LA REGULACIONES RELACIONADAS A:**					
Actividades de la Organización o procesos, Servicios comunes	**FUNCIÓN (descripción)**	**Selección**	**Protección de datos personales**	**Comunicación financiera**	**Control contable digital**	**Propiedad intelectual**	**Protección de sistemas de información**	**Seguridad de las personas y protección del ambiente**
			E	**E**	**E**	**E**	**E**	**E**
	Tipo de Activo		**C01**	**C02**	**C03**	**C04**	**C05**	**C06**
Procesos o actividades de la organización								
Actividad 1: recepción solicitud de desarrollo (correo y escrito)	Correo Electrónico	1						
Actividad 2: registrar solicitud en HELP DESK	Correo Electrónico	1						
Actividad 3: revisar y aprobar Viabilidad proyecto	Correo Electrónico	1						
Actividad 4: envío de correo para definir los requerimientos del proyecto	Correo Electrónico	1						
Actividad 5: realizar, diseñar, construir la arquitectura del aplicativo de acuerdo a los requerimientos	PC de Desarrollo, Unidades de Backups	1	**4**		**3**	**3**	**4**	**3**

Actividad 6: implementar la solución para adaptarse a la necesidades del usuario	PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositorio Centralizado, SIMCA DESKTOP	1	**2**					
Actividad 7: realizar pruebas internas (corrección de errores mejoras de implementación, identificación de nuevos requisitos)	Aplicaciones	1	**3**					
Actividad 8: efectuar modificaciones de la anterior actividad	PC de Desarrollo	1						
Actividad 9: entrega del proyecto desarrollado	Aplicaciones, Código Fuente de las Aplicaciones, Repositorios Centralizados	1						
Actividad 10: solicitud de cambio de aplicación.	Correo Electrónico	1						
Actividad 11: registrar solicitud anterior en el sistema help desk al área de desarrollo	Correo Electrónico	1						
Actividad 12: renviar y aprobar la viabilidad de la solicitud del cambio	Correo Electrónico	1						
Actividad 13: entrega del proyecto desarrollado e implantado (documentación y copias de seguridad)	Correo Electrónico, Help Desk, Repositorios Centralizado	1						
Procesos Transversales		1						
Monitorias de Apoyo(vinculación de monitores)	Monitoria de Apoyo	1	**3**			**3**	**3**	
Atención al Usuario (Atención al Usuario)	Correo Electrónico	1	**3**					

Equipos de Comunicación y Soporte (soporte y mantenimiento de sistemas de información)	SIMCA DESKTOP, Equipos de Comunicación	1	4			2	3	
Contratación de Personal (vicerrectoría académica)	Personal Área de Desarrollo y Mantenimiento	1	4			3		
Administración / política general		1						
Clasificación Junta			4		3	3	4	3
Clasificación para actividades seleccionadas			4		3	3	4	3

Tabla C-48. *Valoracion del cumplimiento T3*

Exposición Natural

Tabla of eventos : Tipos de eventos y exposición natural							
Tipo de Familia	***Tipo de código***	***Descripción del Evento***	***Código***	***Exposición natural (estándar CLUSIF)***	***Exposición natural (decidido)***	***Exposición natural (resultante)***	***1 = Selección***
Ausencia de personal debido a un accidente	AB.P	Ausencia del personal socio	AB.P.Pep	3	2	2	1
		Ausencia del personal interno	AB.P.Per	2	4	4	1
Ausencia o indisponibilidad de servicio, debido a un accidente	AB.S	Ausencia de servicio : Aire acondicionado	AB.S.Cli	2		2	0
		Ausencia de servicio : Fuente de alimentación	AB.S.Ene	3	4	4	1
		Ausencia de servicio : Imposibilidad de tener acceso a los establecimientos	AB.S.Loc	2	4	4	1

		Ausencia o imposibilidad de mantenimiento de software de aplicación	AB.S.Maa	3	4	4	1
		Ausencia o imposibilidad de mantenimiento del sistema de información	AB.S.Mas	2	2	2	1
Accidente grave del ambiente	AC.E	Tormenta Eléctrica	AC.E.Fou	2		2	0
		Fuego	AC.E.Inc	2	4	4	1
		Inundación	AC.E.Ino	3		3	0
Accidente de Hardware	AC.M	Averías del equipo	AC.M.Equ	3	3	3	1
		Averías de los accesorios del equipo	AC.M.Ser	3	3	3	1
Ausencia voluntaria del personal	AV.P	Conflicto social con huelga	AV.P.Gre	2	3	3	1
Error conceptual	ER.L	Software de bloqueo o mal funcionamiento debido a un diseño o error de programación (software interno)	ER.L.Lin	3	4	4	1
Error de Hardware o error de comportamiento por el personal	ER.P	Perdida u olvido de documento o media	ER.P.Peo	3	2	2	1
		Error de operación o de un no cumplimiento de un procedimiento	ER.P.Pro	3	3	3	1
		Error de ingreso datos o de escritura	ER.P.Prs	3	4	4	1
Incidente debido al ambiente	IC.E	Daños debidos al envejecimiento (de los equipos)	IC.E.Age	2	3	3	1
		Daños por agua	IC.E.De	3		3	0
		Daños por contaminación	IC.E.Pol	2		2	0
		Sobre carga eléctrica	IC.E.Se	2	2	2	1
Incidente lógico o funcional	IF.L	Incidente en producción	IF.L.Exp	3	4	4	1
		Software de bloqueo o mal funcionamiento (sistema de información o paquete de software)	IF.L.Lsp	2	3	3	1
		Saturación debido a una casa externa (gusano)	IF.L.Ver	3	4	4	1
		Virus	IF.L.Vir	4	4	4	1
	MA.L	Bloqueo deliberado de cuentas	MA.L.Blo	2	3	3	1

Acción malévola (lógica o funcional)		Eliminación deliberada o contaminación masiva de la configuración del sistema	MA.L.Cfg	2	3	3	1
		Eliminación deliberada de archivos, bases de datos o media	MA.L.Del	2	4	4	1
		Detector electromagnético	MA.L.Ele	3		3	0
		Corrupción deliberada de datos o funciones	MA.L.Fal	3	3	3	1
		Falsificación de mensajes o datos	MA.L.Fau	3	3	3	1
		Reproducción fraudulenta de transacción	MA.L.Rej	2	4	4	1
		Saturación deliberada de equipos TI o redes	MA.L.Sam	3	3	3	1
		Borrado total deliberado de archivos o copias de seguridad	MA.L.Tot	2	4	4	1
		Desviación de archivos o datos (tele-carga o copia)	MA.L.Vol	3	3	3	1
Acción malévola (física)	MA.P	Manipulación o falsificación de equipos	MA.P.Fal	2	4	4	1
		Terrorismo	MA.P.Ter	2	4	4	1
		Vandalismo o gamberrismo	MA.P.Van	2	4	4	1
		Robo de activos físicos	MA.P.Vol	2	4	4	1
Incumplimiento de los procedimientos	PR.N	Procedimientos inadecuados	PR.N.Api	2	2	2	1
		Procedimientos no aplicados debido a la falta de recursos o media	PR.N.Naa	2	2	2	1
		Procedimientos no aplicados debido a ignorancia	PR.N.Nam	2	2	2	1
		Procedimientos no aplicados deliberadamente	PR.N.Nav	2	2	2	1

Tabla C-49. *Valores de exposicion natural*

C.2.2 Evaluando la calidad del servicio

1. *Estableciendo los esquemas de auditoria*
   Debido a que no se tienen controles de seguridad y no se cuentan con ningún sistema de gestión implantado actualmente, no se puede desarrollar este punto. No se puede determinar un esquema de auditoria de seguridad de la información porque no hay controles que valorar. Primero debe realizarse las cuatro fases del ciclo Deming para la implementación de un SGSI o por lo mínimo, la primera fase de planeación para determinar los controles y la segunda fase de ejecución para implantar los controles.

2. *Evaluar la calidad de los servicios de seguridad*
   De la misma manera que no se puede determinar un esquema de auditoria, tampoco se puede evaluar ningún servicio de seguridad, estos servicios de seguridad tienen un pilar y son los controles de la norma ISO/IEC 27002 en su anexo A. Pero debido a que no existen ninguno de los dos no se puede realizar la valoración.

C.2.3 Evaluando el riesgo

1. *Seleccionando los escenarios para el análisis*
   Como primer paso para la evaluación del riesgo, es seleccionar de los 800 escenarios cuales aplican al caso de estudios y cuáles no.

2. *Evaluando los escenarios de riesgo*

Resumen de Valoración de Eventos

Número de escenarios por típo de evento y nivel de gravedad: Actual				**Número de escenarios por cada nivel de gravedad**			
Tipo	***Tipo de Código***	***Evento***	***Código***	***N. 1***	***N. 2***	***N. 3***	***N. 4***
Ausencia de personal debido a un accidente	AB.P	Ausencia del personal socio	AB.P.Pep	0	5	0	0
		Ausencia del personal interno	AB.P.Per	0	0	**5**	0
Ausencia o indisponibilidad de servicio, debido a un accidente	AB.S	Ausencia de servicio : Aire acondicionado	AB.S.Ene	0	0	**8**	0
		Ausencia de servicio : Fuente de alimentación	AB.S.Cli	0	0	0	0
		Ausencia de servicio : Imposibilidad de tener acceso a los establecimientos	AB.S.Loc	0	0	**1**	0
		Ausencia o imposibilidad de mantenimiento de software de aplicación	AB.S.Maa	0	0	**3**	0
		Ausencia o imposibilidad de mantenimiento del sistema de información	AB.S.Mas	0	5	0	0
Accidente grave del ambiente	AC.E	Tormenta Eléctrica	AC.E.Fou	0	0	0	0
		Fuego	AC.E.Inc	0	0	**20**	0
		Inundación	AC.E.Ino	0	0	0	0
Accidente de Hardware	AC.M	Averías del equipo	AC.M.Equ	0	0	**15**	0
		Averías de los accesorios del equipo	AC.M.Ser	0	0	**6**	0
Ausencia voluntaria del personal	AV.P	Conflicto social con huelga	AV.P.Gre	0	0	**5**	0
Error conceptual	ER.L	Software de bloqueo o mal funcionamiento debido a un diseño o error de programación (software interno)	ER.L.Lin	0	0	**2**	0
Error de Hardware o error de comportamiento por el personal	ER.P	Perdida u olvido de documento o media	ER.P.Peo	0	11	0	0

		Error de operación o de un no cumplimiento de un procedicmiento	ER.P.Pro	0	2	**93**	0
		Error de ingreso datos o de escrutura	ER.P.Prs	0	0	**1**	0
Incidente debido al ambiente	IC.E	Daños debidos al envejecimiento (de los equipos)	IC.E.Age	0	0	**4**	0
		Daños por agua	IC.E.De	0	0	0	0
		Daños por contaminación	IC.E.Pol	0	0	0	0
		Sobre carga eléctrica	IC.E.Se	0	12	0	0
Incidente lógico o funcional	IF.L	Incidente en producción	IF.L.Exp	0	0	**22**	0
		Software de bloqueo o mal funcionamiento (sistema de información o paquete de software)	IF.L.Lsp	0	0	**3**	0
		Saturación debido a una casa externa (gusano)	IF.L.Ver	0	0	**2**	0
		Virus	IF.L.Vir	0	0	**3**	0
Acción malevola (lógica o funcional)	MA.L	Bloqueo deliberado de cuentas	MA.L.Blo	0	0	**3**	0
		Eliminación deliberada o contaminación masiva de la configuración del sistema	MA.L.Cfg	0	0	**8**	0
		Eliminación deliberada de archivos, bases de datos o media	MA.L.Del	0	0	**42**	0
		Detector electromagnético	MA.L.Ele	0	0	0	0
		Corrupción deliberada de datos o funciones	MA.L.Fal	0	3	**77**	0
		Falsificación de mensajes o datos	MA.L.Fau	0	0	**1**	0
		Reproducción fraudulenta de transacción	MA.L.Rej	0	0	**1**	0
		Saturación deliberada de equipos TI o redes	MA.L.Sam	0	0	**3**	0
		Borrado total deliberado de archivos o copias de seguridad	MA.L.Tot	0	0	**7**	0
		Desviación de archivos o datos (tele-carga o copia)	MA.L.Vol	0	0	**39**	0
Acción malevola (física)	MA.P	Manipulación o falsificación de equipos	MA.P.Fal	0	0	**9**	0
		Terrorismo	MA.P.Ter	0	0	**6**	0
		Vandalismo o gamberrismo	MA.P.Van	0	0	**26**	0

		Robo de activos físicos	MA.P.Vol	4	4	**84**	0
Incumplimiento de los procedimientos	PR.N	Procedimientos inadecuados	PR.N.Api	0	5	0	0
		Procedimientos no aplicados debido a la falta de recursos o media	PR.N.Naa	0	5	0	0
		Procedimientos no aplicados debido a ignorancia	PR.N.Nam	0	5	0	0
		Procedimientos no aplicados deliberadamente	PR.N.Nav	0	5	0	0

Tabla C-50. *Resultado de la valoracion en terminos de eventos*

C.3. FASE DE PLANIFICACIÓN Y TRATAMIENTO DEL RIESGO

C.3.1 Medidas de planificación inmediatas

1. *Selección de Riesgos para tratamiento Inmediato*
   Aquí se pide, que seleccionemos aquellos riesgos que en la tabla del Excel principal de la herramienta hayan dado una puntuación de 4. Debido a que ninguno de los escenarios dio esta calificación se procede al siguiente paso.

2. *Selección de medidas para la implementación Inmediata*
   No se requiere tomar una medida de implementación inmediata, porque ningún riesgo dio puntuación de 4.

C.3.2 Planificación de medidas en contextos específicos

Aquí se debe tener en cuenta lo que se dice en el documento [4].

1. *Selección de Medidas y planes*
   Según lo que dice MEHARI para el tratamiento del riesgo, se pueden seleccionar diversas maneras para gestionarlos. En este trabajo se utiliza el plan de acción y los planes que sugiere la metodología para el tratamiento del riesgo. Para cada activo primario MEHARI recomienda un plan de tratamiento, por lo tanto, se va a seguir esta recomendación para determinar la mejor forma de tratar el riesgo.

   En la siguiente tabla está el plan de acción que se utilizará a consideración de los autores de este trabajo de grado y lo sugerido por la metodología en cuanto al tratamiento del riesgo. El número 1 en “decisión” representa el plan seleccionado que posteriormente en el anexo D.2 se explicará en que consiste este plan.

Plan de Acción

Familia de Escenarios	Número de Escenarios					Medidas que necesitan mejoras	Tipo de Plan	Decisión
	N 1	N 2	N 3	N 4	Tot			
D01-A	**Pérdida de datos usados por Aplicaciones**							
	33	**1**	**0**	**0**	**34**	Disuasión :	Plan de tipo A	
						Disuasión :	Plan de tipo A	
						Prevención :	Plan de tipo A	
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo A	
						Confinación :	Plan de tipo A	
						Paliación :	**Plan de tipo E**	1
D02-A	**Pérdida de datos compartidos en oficina**							
	20	**1**	**0**	**0**	**21**	Disuasión :	Plan de tipo A	
						Disuasión :	Plan de tipo A	
						Prevención :	Plan de tipo A	
						Prevención :	Plan de tipo A	
						Prevención :	Plan de tipo A	
						Confinación :	Plan de tipo A	
						Paliación :	**Plan de tipo E**	1
D03-A	**Pérdida de datos personales en oficina**							
	24	**0**	**0**	**0**	**24**	Disuasión :	Plan de tipo A	
						Disuasión :	Plan de tipo B	
						Prevención :	Plan de tipo A	
						Prevención :	Plan de tipo B	
						Confinación :		
						Paliación :	**Plan de tipo E**	1
D04-A	**Pérdida de documentos**							
	0	**2**	**2**	**0**	**4**	Disuasión :	Plan de tipo B	1
						Prevención :	**Plan de tipo E**	
						Confinación :		

						Paliación :	
D06-A	**Pérdida de datos durante una transferencia de mensajes**						
	5	**0**	**0**	**0**	**5**	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo D	1
						Confinación :	
						Paliación : **Plan de tipo E**	
D07-A	**Pérdida de Correos Electrónicos (durante el envío o recepción)**						
	8	**0**	**0**	**0**	**8**	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo C	
						Confinación :	
						Paliación : **Plan de tipo E**	1
D08-A	**Pérdida de documentos mientras se transfiere (durante envío o recepción)**						
	0	**1**	**0**	**0**	**1**	Disuasión :	
						Prevención :	
						Confinación :	
						Paliación : **Plan de tipo E**	
D09-A	**Pérdida o inutilización de documentos archivados**						
	0	**0**	**0**	**0**	**0**	Disuasión : Plan de tipo D	
						Prevención : **Plan de tipo E**	
						Confinación :	
						Paliación :	
D10-A	**Pérdida de archivos digitales**						
	0	**0**	**0**	**0**	**0**	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo B	
						Confinación : Plan de tipo A	1
						Paliación : Plan de tipo D	
D11-A	**Indisponibilidad o Pérdida de datos publicados en sitios web internos o públicos**						
	0	**0**	**0**	**0**	**0**	Disuasión :	
						Prevención :	
						Confinación :	
						Paliación : **Plan de tipo E**	1
D01-I	**Distorsión (no detectada) de archivos de datos**						
	15	**0**	**0**	**0**	**15**	Disuasión :	
						Prevención : Plan de tipo B	
						Prevención : Plan de tipo B	
						Prevención : Plan de tipo B	

						Prevención : Plan de tipo B	
						Prevención : Plan de tipo B	
						Confinación : **Plan de tipo E**	1
						Paliación :	
D02-I	**Distorsión (no detectada) de archivos compartidos**						
	0	**9**	**0**	**0**	**9**	Disuasión :	
						Prevención : Plan de tipo D	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo D	
						Prevención : Plan de tipo C	1
						Confinación :	
						Paliación :	
D03-I	**Distorsión (no detectada) de archivos personales de oficina**						
	0	**7**	**0**	**0**	**7**	Disuasión :	
						Prevención : Plan de tipo C	1
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo D	
						Prevención : Plan de tipo B	
						Confinación :	
						Paliación :	
D06-I	**Distorsión (no detectada) de datos o de datos de transmisión que son sensibles individualmente**						
	13	**1**	**0**	**0**	**14**	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo D	
						Prevención : Plan de tipo C	
						Prevención : Plan de tipo C	
						Prevención : Plan de tipo A	
						Confinación : **Plan de tipo E**	1
						Confinación : Plan de tipo A	
						Paliación :	
D07-I	**Distorsión de Correos Electrónicos durante su envío o recepción**						
	0	**3**	**0**	**0**	**3**	Disuasión :	
						Prevención : **Plan de tipo E**	1
						Confinación :	
						Paliación :	
D08-I	**Distorsión de Faxes durante su envío o recepción**						
	0	**1**	**0**	**0**	**1**	Disuasión :	

						Prevención :	**Plan de tipo E**	
						Confinación :		
						Paliación :		
D10-I	**Distorsión de archivos computarizados**							
	0	**0**	**0**	**0**	**0**	Disuasión :	Plan de tipo B	
						Prevención :	Plan de tipo D	
						Confinación :		
						Paliación :		
D11-I	**Distorsión de datos publicados en sitios internos o públicos**							
	0	**0**	**0**	**0**	**0**	Disuasión :		
						Prevención :	Plan de tipo D	
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo C	
						Prevención :	Plan de tipo B	
						Confinación :	**Plan de tipo E**	1
						Paliación :		
D01-C	**Divulgación de archivos de datos**							
	0	**20**	**0**	**0**	**20**	Disuasión :	Plan de tipo B	
						Disuasión :	Plan de tipo A	
						Prevención :	**Plan de tipo D**	
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo A	
						Prevención :	Plan de tipo B	1
						Confinación :		
						Paliación :		
D02-C	**Divulgación de archivos compartidos de oficina**							
	0	**17**	**1**	**0**	**18**	Disuasión :	Plan de tipo B	
						Prevención :	**Plan de tipo E**	1
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo B	
						Prevención :	Plan de tipo A	
						Confinación :		
						Paliación :		
D03-C	**Divulgación de archivos personales de oficina**							
	0	**17**	**0**	**0**	**17**	Disuasión :	Plan de tipo C	

						Prevención : **Plan de tipo E**	1
						Prevención : Plan de tipo C	
						Prevención : Plan de tipo B	
						Confinación :	
						Paliación :	
D04-C	**Divulgación de Documentos**						
	0	**12**	**0**	**0**	**12**	Disuasión : Plan de tipo B	
						Prevención : **Plan de tipo E**	
						Prevención : Plan de tipo B	1
						Confinación :	
						Paliación :	
D05-C	**Divulgación de listas o Impresiones**						
	0	**0**	**0**	**0**	**0**	Disuasión : Plan de tipo C	
						Prevención : **Plan de tipo E**	1
						Confinación :	
						Paliación :	
D06-C	**Divulgación de datos después de consulta o aprovechamiento**						
	0	**13**	**0**	**0**	**13**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo B	
						Prevención : Plan de tipo C	
						Prevención : Plan de tipo B	
						Prevención : Plan de tipo B	
						Prevención : Plan de tipo B	1
						Prevención : Plan de tipo A	
						Confinación :	
						Paliación :	
D07-C	**Divulgación de Correos Electrónicos durante su envío o recepción**						
	0	**4**	**0**	**0**	**4**	Disuasión :	
						Prevención : **Plan de tipo E**	1
						Confinación :	
						Paliación :	
D08-C	**Divulgación de Correo Postal o Faxes durante su envío o recepción**						
	0	**7**	**0**	**0**	**7**	Disuasión :	
						Prevención : **Plan de tipo E**	
						Confinación :	
						Paliación :	
D09-C	**Divulgación de impresiones o archivos escritos**						

	4	0	0	0	4	Disuasión : Plan de tipo C	
						Prevención : Plan de tipo D	
						Confinación :	
						Paliación :	
D10-C	**Divulgación de Archivos o archivos digitalizados**						
	0	0	0	0	0	Disuasión : **Plan de tipo E**	
						Prevención : **Plan de tipo E**	1
						Confinación :	
						Paliación :	
G01-A	**Indisponibilidad del ambiente de trabajo de los usuarios**						
	3	0	0	0	3	Disuasión :	
						Prevención : Plan de tipo D	
						Confinación : Plan de tipo C	
						Paliación : **Plan de tipo E**	1
G02-A	**Indisponibilidad de servicios de telecomunicación (voz, faxes, vídeo, conferencia)**						
	14	1	0	0	15	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo B	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo B	
						Paliación : **Plan de tipo E**	1
R01-A	**Indisponibilidad de servicio extendido de red**						
	13	11	0	0	24	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo B	
						Paliación : **Plan de tipo E**	1
R02-A	**Indisponibilidad de servicio de red de área local**						
	22	2	0	0	24	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo B	
						Paliación : **Plan de tipo E**	1

						Paliación : Plan de tipo A	
S01-A	**Indisponibilidad de servicio de Aplicación**						
	52	**3**	**0**	**0**	**55**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo A	
						Paliación : Plan de tipo B	
						Paliación : Plan de tipo D	1
S02-A	**Indisponibilidad de servicios comunes de oficina**						
	50	**3**	**0**	**0**	**53**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo A	
						Paliación : Plan de tipo A	
						Paliación : Plan de tipo E	1
S03-A	**Indisponibilidad de servicios de interfaz o terminales de usuarios (PC, impresoras locales, periféricos, interfaces especiales, etc.)**						
	9	**0**	**1**	**0**	**10**	Disuasión : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo B	
						Confinación : Plan de tipo B	
						Paliación : **Plan de tipo E**	1
S04-A	**Indisponibilidad de servicios de sistemas comunes: mensajes, archivos, impresiones, ediciones, etc.**						
	50	**3**	**0**	**0**	**53**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo A	
						Paliación : Plan de tipo B	

						Paliación : Plan de tipo D	1
S05-A	**Indisponibilidad de servicio de publicación en sitios web (internos o públicos)**						
	0	**0**	**0**	**0**	**0**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Prevención : Plan de tipo A	
						Confinación : Plan de tipo A	
						Paliación : Plan de tipo A	
						Paliación : **Plan de tipo D**	1
G02-I	**Alteración de funciones de telecomunicación**						
	0	**4**	**2**	**0**	**6**	Disuasión : Plan de tipo B	
						Prevención : **Plan de tipo D**	1
						Confinación :	
						Paliación :	
R01-I	**Alteración de servicios de red extendida**						
	0	**5**	**0**	**0**	**5**	Disuasión : Plan de tipo C	
						Prevención : **Plan de tipo E**	1
						Confinación :	
						Paliación :	
R02-I	**Alteración del servicio de red de área local**						
	0	**5**	**0**	**0**	**5**	Disuasión : Plan de tipo C	
						Prevención : **Plan de tipo E**	1
						Confinación :	
						Paliación :	
S01-I	**Alteración de servicios de aplicación**						
	8	**10**	**0**	**0**	**18**	Disuasión : Plan de tipo C	
						Prevención : **Plan de tipo E**	1
						Prevención : Plan de tipo B	
						Confinación : Plan de tipo C	
						Paliación :	
S02-I	**Alteración de servicios comunes de oficinas**						
	0	**9**	**0**	**0**	**9**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo D	
						Prevención :	
						Confinación :	

						Paliación :	
S04-I	**Alteración de servicios comunes de sistemas**						
	0	**9**	**0**	**0**	**9**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo D	
						Confinación :	
						Paliación :	
S05-I	**Alteración del servicio de publicación de en sitios web (internos o públicos)**						
	0	**0**	**0**	**0**	**0**	Disuasión : Plan de tipo C	
						Prevención : **Plan de tipo E**	1
						Prevención : Plan de tipo B	
						Confinación : Plan de tipo C	
						Paliación :	
S01-C	**Divulgación linked to the Aplicación service**						
	0	**16**	**0**	**0**	**16**	Disuasión : Plan de tipo B	
						Prevención : **Plan de tipo E**	1
						Prevención : Plan de tipo A	
						Paliación :	
C01-E	**Ningún proceso de cumplimiento adjunto a la protección de datos personales**						
	0	**4**	**0**	**0**	**4**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo D	
						Prevención :	
						Paliación :	
C02-E	**Ningún proceso de cumplimiento adjunto a la comunicación financiera**						
	0	**0**	**0**	**0**	**0**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo D	
						Prevención :	
						Paliación :	
C03-E	**Ningún proceso de cumplimiento adjunto para la verificación contable**						
	0	**4**	**0**	**0**	**4**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo D	
						Prevención :	
						Paliación :	
C04-E	**Ningún proceso de cumplimiento adjunto para la protección de la propiedad intelectual**						
	0	**4**	**0**	**0**	**4**	Disuasión : Plan de tipo B	
						Prevención : Plan de tipo D	
						Prevención :	
						Paliación :	

C05-E	**Ningún proceso de cumplimiento adjunto para la protección de sistemas de computación**							
	0	**4**	**0**	**0**	**4**	Disuasión : Plan de tipo B		
						Prevención : Plan de tipo D		
						Prevención :		
						Paliación :		

TOTAL	**343**	**217**	**6**	**0**	**566**			**37**

Tabla C-51. *Planes de tratamientos seleccionados*

C.3.3 Vigilancia de la implementación del tratamiento del riesgo

1. *Selección de Indicadores, dashboards y gráficos*
   Después de haber configurado lo anterior, se procede a verificar como cambian las tablas de resultado con unos controles "plenamente implantados"[4]. Los resultados son los siguientes:

Número de escenarios por típo de evento y nivel de gravedad: Para Plan de Acción el que se decidió en 1				**Número de escenarios por cada nivel de gravedad**			
Tipo	***Tipo de Código***	***Evento***	***Código***	***N. 1***	***N. 2***	***N. 3***	***N. 4***
Ausencia de personal debido a un accidente	AB.P	Ausencia del personal socio	AB.P.Pep	5	0	0	0
		Ausencia del personal interno	AB.P.Per	5	0	0	0
Ausencia o indisponibilidad de servicio, debido a un accidente	AB.S	Ausencia de servicio : Aire acondicionado	AB.S.Ene	2	6	0	0
		Ausencia de servicio : Fuente de alimentación	AB.S.Cli	0	0	0	0
		Ausencia de servicio : Imposibilidad de tener acceso a los establecimientos	AB.S.Loc	1	0	0	0
		Ausencia o imposibilidad de mantenimiento de software de aplicación	AB.S.Maa	3	0	0	0
		Ausencia o imposibilidad de mantenimiento del sistema de información	AB.S.Mas	6	0	0	0
	AC.E	Tormenta Eléctrica	AC.E.Fou	0	0	0	0

[4] Esta implantación es producto de la simulación que se realiza para verificar como se reducirían los riesgos en caso tal se implemente el plan y los controles que se dijeron.

Accidente grave del ambiente		Fuego	AC.E.Inc	20	0	0	0
		Inundación	AC.E.Ino	0	0	0	0
Accidente de Hardware	AC.M	Averías del equipo	AC.M.Equ	13	1	**1**	0
		Averías de los accesorios del equipo	AC.M.Ser	6	0	0	0
Ausencia voluntaria del personal	AV.P	Conflicto social con huelga	AV.P.Gre	5	0	0	0
Error conceptual	ER.L	Software de bloqueo o mal funcionamiento debido a un diseño o error de programación (software interno)	ER.L.Lin	2	0	0	0
Error de Hardware o error de comportamiento por el personal	ER.P	Perdida u olvido de documento o media	ER.P.Peo	10	1	0	0
		Error de operación o de un no cumplimiento de un procedicmiento	ER.P.Pro	56	39	0	0
		Error de ingreso datos o de escrutura	ER.P.Prs	1	0	0	0
Incidente debido al ambiente	IC.E	Daños debidos al envejecimiento (de los equipos)	IC.E.Age	4	0	0	0
		Daños por agua	IC.E.De	0	0	0	0
		Daños por contaminación	IC.E.Pol	0	0	0	0
		Sobre carga eléctrica	IC.E.Se	12	0	0	0
Incidente lógico o funcional	IF.L	Incidente en producción	IF.L.Exp	22	0	0	0
		Software de bloqueo o mal funcionamiento (sistema de información o paquete de software)	IF.L.Lsp	3	0	0	0
		Saturación debido a una casa externa (gusano)	IF.L.Ver	1	1	0	0
		Virus	IF.L.Vir	3	0	0	0
Acción malevola (lógica o funcional)	MA.L	Bloqueo deliberado de cuentas	MA.L.Blo	3	0	0	0
		Eliminación deliberada o contaminación masiva de la configuración del sistema	MA.L.Cfg	7	1	0	0
		Eliminación deliberada de archivos, bases de datos o media	MA.L.Del	41	1	0	0
		Detector electromagnético	MA.L.Ele	0	0	0	0
		Corrupción deliberada de datos o funciones	MA.L.Fal	35	43	**2**	0
		Falsificación de mensajes o datos	MA.L.Fau	0	1	0	0
		Reproducción fraudulenta de transacción	MA.L.Rej	1	0	0	0
		Saturación deliberada de equipos TI o redes	MA.L.Sam	0	3	0	0
		Borrado total deliberado de archivos o copias de seguridad	MA.L.Tot	0	7	0	0
		Desviación de archivos o datos (tele-carga o copia)	MA.L.Vol	0	38	**1**	0
Acción malévola (física)	MA.P	Manipulación o falsificación de equipos	MA.P.Fal	6	3	0	0
		Terrorismo	MA.P.Ter	5	1	0	0
		Vandalismo o gamberrismo	MA.P.Van	24	2	0	0
		Robo de activos físicos	MA.P.Vol	41	49	**2**	0
	PR.N	Procedimientos inadecuados	PR.N.Api	0	5	0	0

Incumplimiento de los procedimientos		Procedimientos no aplicados debido a la falta de recursos o media	PR.N.Naa	0	5	0	0
		Procedimientos no aplicados debido a ignorancia	PR.N.Nam	0	5	0	0
		Procedimientos no aplicados deliberadamente	PR.N.Nav	0	5	0	0

Tabla C-52. *Valoración de eventos después de tratamiento*

D. RESULTADOS OBTENIDOS

D.1. DECLARACIÓN DE APLICABILIDAD

ISO 27002 : 2013 Correspondencia y puntuación (SOA) **Un valor de 1, al lado, indica que las preguntas asociadas a la evaluación de puntuación se llenarán con color amarillo en el cuestionario**			**ISO 27001 2013 SGSI** **SGSI**	**Justificación para la inclusión en el SOA**
Preguntas o servicios utilizados para la puntuación		***Puntuación***		
5 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.				
5.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información.				
5.1.1 Políticas para la Seguridad de la Información.	01A02-01	0,0	0	
5.1.2 Revisión de las Políticas para seguridad de la información.	01A02-02;01A02-08	0,0	0	
6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.				
6.1 Organización Interna.				
6.1.1 Seguridad de la Información Roles y Responsabilidades.	01A02-03:07;01A02-09;01C03-01	10,0	1	Se debe tener definido los roles y responsabilidades dentro del marco de la seguridad de la información

6.1.2 Separación de deberes.	06C01-03:06;08F01-01:04;11E01-01:04;11E02-01:04;12E01-01:04;12E02-01:04	10,0	1	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
6.1.3 Contacto con las autoridades.	01A02-10	0,0	0	
6.1.4 Contacto con grupos de interés especial.	01A02-11	0,0	0	
6.1.5 Seguridad de la información en Gestión de Proyectos.	01B02-06;10A01-01:06;10A02-01;10A02-05	0,0	0	
6.2 Dispositivos Móviles y Teletrabajo.				
6.2.1 Política para dispositivos móviles.	01B02-08;11B02-01;11B02-03;11C01-01;11D05-01	10,0	1	Debido al alto uso de los dispositivos móviles en el procedimiento, se debe adoptar una política y medidas de seguridad para el uso de datos a través de ellos.
6.2.2 Teletrabajo.	11B02-01:02;11B02-04;11B03-04	0,0	0	
7 SEGURIDAD DE LOS RECURSOS HUMANOS.				
7.1 Antes de asumir el empleo.				
7.1.1 Selección.	01C03-02:04	10,0	0	Verificación de antecedentes de los candidatos aun empleo, se deben llevar a cabo de acuerdo con los requisitos de negocio para determinar la competencia del aspirante referente al requerimiento
7.1.2 Términos y condiciones del empleo.	01C01-01:02	0,0	0	
7.2 Durante la ejecución del empleo.				
7.2.1 Responsabilidades de la Dirección.	01C01-06	0,0	0	

7.2.2 Toma de conciencia, educación y formación de la Seguridad de la Información.	01C04-01:05	0,0	0	
7.2.3 Proceso disciplinario.	01B01-07	0,0	0	
7.3 Terminación y cambio de empleo.				
7.3.1 Terminación o cambio de responsabilidades de empleo.	01B01-09	0,0	0	
8 GESTIÓN DE ACTIVOS.				
8.1 Responsabilidad por los Activos.				
8.1.1 Inventario de Activos.	01B04-01:02	0,0	0	
8.1.2 Propiedad de los activos.	01B04-03	0,0	0	
8.1.3 Uso Aceptable de los Activos.	01B01-05;01B04-04	0,0	0	
8.1.4 Devolución de Activos.	01B04-05	0,0	0	
8.2 Clasificación de la Información.				
8.2.1 Clasificación de la Información.	01B03-01:04;01B03-10	0,0	0	
8.2.2 Etiquetado de la Información.	01B02-04;01B03-02	0,0	0	
8.2.3 Manejo de Activos.	01B01-04;01B02-10:11	0,0	0	
8.3 Manejo de medios de soporte.				
8.3.1 Gestión de medios de Soporte Removibles.	02D02-01;08C01-01:05;08C03-11	10,0	1	Se debe adoptar un procedimiento claro para la gestión de medios removibles, debido al uso de ellos en el procedimiento.
8.3.2 Disposición de los medios de soporte.	07B01-08;08C01-04	10,0	1	Se debe disponer de forma segura los medios de soporte a través de medidas de seguridad

8.3.3 Transferencia de medios de soporte físicos.	08C04-03;08C07-01	10,0	1	Los medios de soporte que contentan información del procedimiento deben tener medidas contra accesos no autorizados.
9 CONTROL DE ACCESO.				
9.1 Requisitos del Negocio para Control de Acceso.				
9.1.1 Política de Control de Acceso.	02C01-01;05B01-01;06C01-01;07A01-01;09A01-01	10,0	1	Se debería establecer y documentar una política de acceso con base a los objetivos del procedimiento
9.1.2 Acceso a redes y a servicios en red.	01B02-05;05B02-01:07	10,0	1	Solo se debe permitir el acceso a la red y todos los servicios de red a personal autorizado.
9.2 Gestión de Acceso de Usuarios.				
9.2.1 Registro y cancelación del registro de usuarios.	01C06-01:06	0,0	0	
9.2.2 Suministro de acceso de usuarios.	07A02-01:07	10,0	1	Se debe implementar un procedo de suministrode acceso formal de usuarios para asignar o cancelar los derechos de acceso.
9.2.3 Gestión de derechos de acceso privilegiado.	05B01-02;05B02-03;06C01-03;06C01-07;07A01-02;07A02-03;08F01-01;08F01-05;09A01-02;09A02-03;11E01-01;11E01-05;12E01-01;12E01-05	10,0	1	Se debe restringir y controlar la asignacion y uso de derechos privilegiados
9.2.4 Gestión de información de autenticación secreta de usuarios.	01B01-02;07A03-01:05;07A03-08:09	10,0	1	Se debe controlar por medio de un procedimiento de gestion formal la autenticación secreta

9.2.5 Revisión de los derechos de acceso de usuarios.	05B01-08;05B02-04:05;05B02-07;06C01-08:09;06C02-07;07A01-08;07A02-04:05;07A02-08;08F01-06:07;08F02-06;09A01-08;09A02-04:05;09A02-08;11E01-06:07;12E01-06:08	10,0	1	Los dueños o propietarios de los activos deben revisar los derechos de acceso
9.2.6 Cancelación o ajuste de los derechos de acceso.	01B01-10	0,0	0	
9.3 Responsabilidades de los usuarios.				
9.3.1 Uso de información secreta.	01B01-02	0,0	0	
9.4 Control de Acceso a Sistemas y Aplicaciones.				
9.4.1 Restricción de acceso a información.	09A01-02;09A02-01:02;09A04-01:02;09A04-07	10,0	1	Se debe restringir el acceso a la información de acuerdo con las políticas de control de acceso
9.4.2 Procedimiento de Conexión Segura.	07A01-04:05;07A03-03:07;07A04-04:06;09A01-04;09A04-05:06	10,0	1	Según lo que determine la política se debe tener un procedimiento de conexión segura
9.4.3 Sistema de Gestión de Contraseñas.	07A03-01:09;09A03-01:08	10,0	1	Debe asegurarse la calidad de las contraseñas cumplan según la política establecida
9.4.4 Uso de programas utilitarios privilegiados.	08A02-03:07	0,0	0	
9.4.5 Control de Acceso a Códigos Fuente de Programas.	10B02-04	10,0	1	Se debe restringir el acceso a los códigos fuentes
10 CRIPTOGRAFÍA				
10.1 Controles Criptográficos.				
10.1.1 Política sobre el uso de controles Criptográficos.	04C01-01;05C01-01;05C03-01;08C06-05;09C01-01;09C02-01;09F01-01;11C01-01	10,0	1	Se debe implementar una política sobre el uso de controles criptográficas para la protección de la información

10.1.2 Gestión de Claves.	04C01-03;05C01-03;05C03-03;08D03-10;09C01-03;09C02-05;09F01-04	10,0	1	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas
11 SEGURIDAD FÍSICA Y AMBIENTAL.				
11.1 Áreas Seguras.				
11.1.1 Perímetro de Seguridad Física.	02A03-01:02;02A03-06;02A04-01	10,0	1	Se debe definir perímetros de seguridad para proteger áreas que contengan información confidencial o critica
11.1.2 Controles Físicos de entrada.	02C06-01:04;03B01-01;03B01-07;03B03-01	10,0	1	Para las áreas seguras se deben proteger mediente controles de entrada apropiados
11.1.3 Seguridad de oficinas, salones e instalaciones.	03B08-01:03	0,0	0	
11.1.4 Protección contra amenazas externas y ambientales.	02B01-01:03;03C01-01;03C02-01:03;03D01-01;03D02-01;03D03-06	10,0	1	Se debe diseñar una protección física contra desastres naturales, ataques maliciosos o accidentes
11.1.5 Trabajo en áreas seguras.	03B02-08;03B03-01;03B06-01	10,0	1	Se debe diseñar un procedimiento para trabajo en áreas seguras
11.1.6 Áreas de despacho y carga.	02A05-01:03	0,0	0	
11.2 Equipos.				
11.2.1 Ubicación y protección de los equipos.	06A02-03;08A01-01;08A03-03;12A01-01;12A02-03	10,0	1	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y de accesos no autorizados
11.2.2 Servicios Públicos de soporte.	03A01-01:03;03A02-01:02;03A03-01;03A03-03	0,0	0	
11.2.3 Seguridad del cableado.	03A04-01:04	0,0	0	

11.2.4 Mantenimiento de equipos.	04A02-01;05A03-01;06A03-01;06A07-01:02;08A04-01;08A05-01:02;08D01-01;11D01-01;12A03-01;12C01-01	10,0	1	Se deben mantener correctamente los equipos para asegurar la disponibilidad e integridad continua
11.2.5 Retiro de Activos.	01B04-06	0,0	0	
11.2.6 Seguridad de equipos y activos fuera del predio.	11B02-01;11B02-03	0,0	0	
11.2.7 Disposición segura o reutilización de equipos.	06A07-01;08A05-01:02;08C01-05;11C03-01	10,0	1	Se debe tener una política para la disposición o reutilización de los equipos para extraer licencias y datos confidenciales que puedan tener
11.2.8 Equipos sin supervisión de los usuarios.	01B01-03;11B01-08	10,0	1	Los usuarios deben asegurar que los equipos sin supervisión tengan la seguridad apropiada
11.2.9 Política de escritorio limpio y pantalla limpia.	01B02-07	10,0	1	Se debe contar con una política de escritorio limpio para papeles y medios de almacenamiento y evitar accesos no autorizados
12 SEGURIDAD DE LAS OPERACIONES.				
12.1 Procedimientos operacionales y responsabilidades.				
12.1.1 Procedimientos de operación documentadas.	06A05-01:04;08A08-01:04;12A05-01:04	0,0	0	
12.1.2 Gestión de Cambios.	06A02-01;08A03-01;11A01-01;12A02-01	10,0	1	Se debe tener un proceso de gestión para que los cambios realizados dentro de la organización no afecten la seguridad de la información

12.1.3 Gestión de Capacidad.	06A02-02;08A03-02;11A01-01;12A02-01:02	10,0	1	Se debe tener un seguimiento para tener la capacidad de optimizar los recursos actuales e intentar ajustar para determinar los recursos requeridos en un futuro
12.1.4 Separación de los ambientes de desarrollo, ensayo y operación.	06B01-07:09;10B01-04:10	10,0	1	Se debe separar los ambientes de desarrollo, ensayo y operación con el fin de garantizar calidad en los productos
12.2 Protección contra códigos maliciosos.				
12.2.1 Controles contra códigos maliciosos.	08D07-01:02;11D06-01;11D06-05;11D06-07	10,0	1	Se deben tener controles de detección y prevención junto con una toma de conciencia para prevenir intrusiones de códigos maliciosos
12.3 Copias de Respaldo.				
12.3.1 Copias de respaldo de la información.	04A04-01:07;05A05-01:07;08D04-01:07;08D05-01:13;11D03-01:04;11D04-01:04;11D05-01:05;12C03-01:06	10,0	1	Se debe generar una política que contemple las copias de respaldo y disponerlas de manera segura
12.4 Registro y Seguimiento.				
12.4.1 Registro de eventos.	04D01-01:03;04D01-08;04D02-01:02;04D03-01:05;05D01-01:03;05D01-08;05D02-01:02;05D03-01:05;07C01-01:02;07C01-05:07;07C02-01:02;07C02-05:07	10,0	1	Se deben revisar y elaborar regularmente los registros de eventos
12.4.2 Protección de la información de registro.	04D01-09;04D02-06;04D02-08:09;05D01-09;05D02-06;05D02-08:09;07C01-07:08;07C02-07:08	10,0	1	Las instalaciones e informacion debe protegerse contra alteraciones y accesos no autorizados

12.4.3 Registros del administrador y del operador.	06C03-01:07;08F03-01:07;11E03-01:09;12E03-01:09	10,0	1	Deben protegerse con regularidad los registros de la actividad del operador o administrador
12.4.4 Sincronización de relojes.	06B01-03;08B01-04;12B01-05	10,0	1	Las actividades del sistema y el administrador de sistema deben registrar y los registros deben estar seguros
12.5 Control de Software Operacional.				
12.5.1 Instalación de software en sistemas operativos.	06A02-04:05;06A02-13:14;08A03-04:06;08A03-13:15;08B03-01;10B01-03;11A04-01;12A02-14:15	10,0	1	Se debe tener procedimientos claros para la instalación de software en los equipos de desarrollo
12.6 Gestión de vulnerabilidad técnica.				
12.6.1 Gestión de las vulnerabilidades técnicas.	01A01-02:04;01A03-07;06A01-01:05;08B01-03;08B02-04;09G01-02;12B01-04	10,0	1	Se debe tener una gestión de vulnerabilidades para corregir a tiempo todo aquello que ponga en peligro a los activos
12.6.2 Restricciones sobre la instalación de Software.	08A02-01:05;08A03-01:02;08A03-04:06;11A01-01:06	10,0	1	Se debe tener una política clara que restrinja la instalación de softwares en equipo con contenido importante
12.7 Consideraciones sobre auditorías de sistemas de información.				
12.7.1 Controles sobre auditorías de Sistemas de Información.	01A04-01:06;06D01-01:04;08G01-01:04	0,0	0	
13 SEGURIDAD DE LAS COMUNICACIONES.				
13.1 Gestión de Seguridad de Redes.				
13.1.1 Controles de redes.	06C01-03:04;06C03-01:02	10,0	1	Se debe tener un control interno de las redes para proteger los sistemas y las aplicaciones
13.1.2 Seguridad de los servicios de red.	06A08-01:03	0,0	0	
13.1.3 Separación en las redes.	01B02-02;05A01-02:06	0,0	0	

13.2 Transferencia de información.				
13.2.1 Políticas y procedimientos de transferencia de información.	01B02-03:05;01B02-07:08	10,0	0	Se debe tener medidas de seguridad para las transferencias formales con el fin de proteger la información de accesos no autorizados o alteración de ella mientras dura la transferencia
13.2.2 Acuerdos sobre transferencia de información.	01C05-03	0,0	0	
13.2.3 Mensajes electrónicos.	11C05-01;11C05-04:06	10,0	1	Toda información que se incluya en los mensajes electrónicos debe estar segura
13.2.4 Acuerdos de confidencialidad o de no divulgación.	01C01-01:05	0,0	0	
14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.				
14.1 Requisitos de seguridad de los sistemas de información.				
14.1.1 Análisis y especificación de requisitos de seguridad de la información.	09H01-02;09H01-06;09H01-09;10A01-01:03	0,0	0	
14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.	09H01-01;09H01-03;09H01-05;09H01-08;09H01-10	0,0	0	
14.1.3 Protección de transacciones de servicios de aplicaciones.	09H02-01:04	0,0	0	
14.2 Seguridad en los procesos de desarrollo y de soporte.				
14.2.1 Política de desarrollo seguro.	10B01-05;10B01-08:11;10B02-01:04	10,0	1	Se debe establecer políticas claras y reglas para el desarrollo de software y de sistemas
14.2.2 Procedimiento de control de cambios en sistemas.	08A03-03:04;10A02-01:03	10,0	1	Se debe tener un procedimiento claro para evidenciar que cambios se realiza dentro del sistema
14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones.	10A02-05:07	0,0	0	

14.2.4 Restricciones sobre los cambios de paquetes de software.	10A05-01:04	0,0	0	
14.2.5 Principios de construcción de sistemas de seguros.	10A01-01:03;10A02-01;10A03-01:02	0,0	0	
14.2.6 Ambiente de desarrollo seguro.	10A01-05:07;10A02-06;10A04-01;10B01-01;10B01-08:12;10B03-01	10,0	1	Se debe asegurar la integración y todo lo relacionado con el ambiente seguro para el desarrollo de las aplicaciones
14.2.7 Desarrollo contratado externamente.	10A03-01:05	0,0	0	
14.2.8 Pruebas de seguridad de sistemas.	10A02-05:06;10B01-09:12;10B04-01;10B05-04	10,0	1	Dentro del desarrollo se debe tener claro las pruebas de seguridad para las aplicaciones y sistemas
14.2.9 Pruebas de aceptación de sistemas.	06A02-04:05;06A02-08:11;08A03-05:06;08A03-09:12;11A01-04:06;12A02-05:06;12A02-09:12	10,0	1	Se debe tener una política clara para la aceptación de actualizaciones o cambios dentro de los sistemas
14.3 Datos de ensayo.				
14.3.1 Protección de datos de ensayo.	10B04-01:05	10,0	1	Los datos de ensayo se deben proteger muy cuidadosamente
15 RELACIONES CON LOS PROVEEDORES.				
15.1 Seguridad de la información en las relaciones con los proveedores.				
15.1.1 Política de seguridad de la información para las relaciones con proveedores.	01C01-05;01C05-01:05	0,0	0	
15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores.	01C05-04:05	0,0	0	
15.1.3 Cadena de suministro de tecnología de información y comunicación.	04A06-01:02;05A07-01:02;08A09-01:03;11A05-01:04	0,0	0	
15.2 Gestión de la prestación de servicios de proveedores.				

15.2.1 Seguimiento y revisión de los servicios de los proveedores.	06A06-03:05;08A09-03:05;11A05-03:05;12A06-03:05	0,0	0	
15.2.2 Gestión de cambios a los servicios de los proveedores.	06A06-06;08A09-06;11A05-06;12A06-06	0,0	0	
16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.				
16.1 Gestión de incidentes y mejoras en la seguridad de la información.				
16.1.1 Responsabilidades y procedimientos.	01A02-12;01A03-04;04D03-08;05D03-08;08E03-08	10,0	1	Se deben tener claro los procedimientos y las responsabilidades para tener una respuesta rápida y eficaz a los incidentes presentados
16.1.2 Informe de eventos de seguridad de la información.	01A02-12;01A03-01:04	0,0	0	
16.1.3 Informe de debilidades de seguridad de la información.	01C04-06	0,0	0	
16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	04D01-01:03;05D01-01:03;08E01-01:05;09G01-01:08	10,0	1	Se debe tener una clasificación para los incidentes de seguridad
16.1.5 Respuesta a incidentes de seguridad de la información.	04D03-01:06;05D03-01:06;08E03-01:06	10,0	1	Según la clasificación de los incidentes de seguridad se debe tener cuales deberían ser las respuestas
16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información.	01A03-05	0,0	0	
16.1.7 Recolección de evidencia.	01A03-06;02D06-01:02;08H01-04	0,0	0	
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.				
17.1 Continuidad de seguridad de la información				
17.1.1 Planificación de la continuidad de la seguridad de la información.	01E01-01:02	10,0	1	Se debe crear una política que planifique la seguridad de la información para la continuidad del SGSI durante crisis o desastres

17.1.2 Implementación de la continuidad de la seguridad de la información.	01E01-03;01E02-01:05;01E02-08:11;04A05-01:05;05A06-01:05;08D04-05;08D05-09;08D06-01:08;09E02-01:09;10A02-07;11D03-03;11D07-01:08;12C03-04;12C04-01:08	10,0	1	Se debe tener documentada toda la parte de la continuidad de la seguridad de la información en cualquier escenario
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	01E02-08:11;04A05-04:05;05A06-04:05;08D04-05;08D05-09;08D06-07:08;09E02-09;10A02-07;11D03-03;11D07-07:08;12C03-04;12C04-07:08	10,0	1	Se debe revisar constantemente el procedimiento de la continuidad de la seguridad de la información
17.2 Redundancia				
17.2.1 Disponibilidad de instalaciones de procesamiento de información.	05A06-01:05	10,0	1	Los sitios donde se procese la información deben estar siempre disponibles
18 CUMPLIMIENTO.				
18.1 Cumplimiento de requisitos legales y contractuales.				
18.1.1 Identificación de los requisitos de legislación y contractuales aplicables.	01B02-10	0,0	0	
18.1.2 Derechos de Propiedad Intelectual.	11A03-01:03;13D01-01:10;13D02-01:04;13D04-01	0,0	0	
18.1.3 Protección de registros.	01B02-09;08H01-04:06	0,0	0	
18.1.4 Privacidad y protección de la información identificable personalmente.	13A01-01:06;13A02-01:04;13A04-01	0,0	0	
18.1.5 Reglamentación de Controles Criptográficos.	13G01-01:06;13G02-01:02;13G03-01	0,0	0	
18.2 Revisiones de seguridad de la información				
18.2.1 Revisión independiente de la seguridad de la información.	01A02-13	0,0	0	

18.2.2 Cumplimiento con las políticas y normas de seguridad.	01B01-12	0,0	0	
18.2.3 Revisión del Cumplimiento Técnico.	05B07-10;06B01-06:08;08B01-06:08;08B02-06:08;11A02-05:06;12B01-07:09	10,0	1	Todas a las aplicaciones y sistemas se deben revisar con regularidad para determinar el cumplimiento de las políticas y normas de la seguridad

Tabla D-1. *Declaración de aplicabilidad*

D.2. PLAN DE TRATAMIENTO

1	**Activo**	D01-A									
	Servicios de Seguridad a mejorar	08D05	08D09	09D02							
2	**Activo**	D02-A									
	Servicios de Seguridad a mejorar	08D09	11D04	11D08							
3	**Activo**	D03-A									
	Servicios de Seguridad a mejorar	11D05	11D08								
4	**Activo**	D04-A									
	Servicios de Seguridad a mejorar	02C05									
5	**Activo**	D06-A									
	Servicios de Seguridad a mejorar	03C01	03D01	07A03	07A04	08A03	08F02				
6	**Activo**	D07-A									
	Servicios de Seguridad a mejorar	11C05									
7	**Activo**	D10-A									
	Servicios de Seguridad a mejorar	08C05									

8	**Activo**	D11-A									
	Servicios de Seguridad a mejorar	08D05	08D09								
9	**Activo**	D01-I									
	Servicios de Seguridad a mejorar	09B04									
10	**Activo**	D02-I									
	Servicios de Seguridad a mejorar	07A01	07A02	07A03	07A04	08F01	08F02				
11	**Activo**	D03-I									
	Servicios de Seguridad a mejorar	11C01									
12	**Activo**	D06-I									
	Servicios de Seguridad a mejorar	09B04									
13	**Activo**	D07-I									
	Servicios de Seguridad a mejorar	11C05									
14	**Activo**	D11-I									
	Servicios de Seguridad a mejorar	09B04									
15	**Activo**	D01-C									
	Servicios de Seguridad a mejorar	03B03	03B04	08C03	08C04	08C07					
16	**Activo**	D02-C									
	Servicios de Seguridad a mejorar	11C01									
17	**Activo**	D03-C									
	Servicios de Seguridad a mejorar	11C01	11C02								
18	**Activo**	D04-C									
	Servicios de Seguridad a mejorar	02C01	02C02	02C03	02C06						
19	**Activo**	D05-C									
	Servicios de Seguridad a mejorar	08A07									
20	**Activo**	D06-C									

	Servicios de Seguridad a mejorar	06A02	06A04	06C01	06C02						
21	**Activo**	D07-C									
	Servicios de Seguridad a mejorar	11C05									
22	**Activo**	D10-C									
	Servicios de Seguridad a mejorar	09C02									
23	**Activo**	G01-A									
	Servicios de Seguridad a mejorar	01E03									
24	**Activo**	G02-A									
	Servicios de Seguridad a mejorar	03A02	03A06	12C01	12C03	12C04	12C05				
25	**Activo**	R01-A									
	Servicios de Seguridad a mejorar	01C02	01E02	03A02	03A06						
26	**Activo**	R02-A									
	Servicios de Seguridad a mejorar	01C02	01E01	01E02	05A03	05A04	05A05	05A06			
27	**Activo**	S01-A									
	Servicios de Seguridad a mejorar	01E01	01E02	03A02	03A03	03A06	07D01	08D04	08D06	09E01	09E02
28	**Activo**	S02-A									
	Servicios de Seguridad a mejorar	01E01	01E02	03A02	03A06	07D01	08D04	08D06	09E01	09E02	
29	**Activo**	S03-A									
	Servicios de Seguridad a mejorar	01E03	11D03	11D07							
30	**Activo**	S04-A									
	Servicios de Seguridad a mejorar	01E01	01E02	03A02	03A03	03A06	07D01	08D04	08D06	09E01	09E02
31	**Activo**	S05-A									
	Servicios de Seguridad a mejorar	01E01	01E02	03A02	03A06	07D01	08D04	08D06	09E01	09E02	
32	**Activo**	G02-I									
	Servicios de Seguridad a mejorar	12A02	12B01	12B02	12E01	12E02					

33	**Activo**	R01-I									
	Servicios de Seguridad a mejorar	06A02	06B01	06C01	06C02						
34	**Activo**	R02-I									
	Servicios de Seguridad a mejorar	06A02	06B01	06C01	06C02						
35	**Activo**	S01-I									
	Servicios de Seguridad a mejorar	08A03	08A04	08B01	08B02	08B03	08C02	09A05	09B05	10B01	10B05
36	**Activo**	S05-I									
	Servicios de Seguridad a mejorar	08A03	08A04	08B01	08B02	08B03	08C02	09A05	09B05	10B01	10B05
37	**Activo**	S01-C									
	Servicios de Seguridad a mejorar	10B02									
38	**Servicios de Seguridad a mejorar a consideración de autores.**	Servicios acorde a controles ISO/IEC 27002 seleccionados									
		01B02-0	01C03	02A01	02A02	02A03	02A04	02C04	02D02	02D03	12E02
		12C02	03A05	03B01	03B02	03B05	03B06	03B07	03C02	03C03	03D02
		03D03	04B02	04B03	04C01	04C02	05B01	05B02	05B03	05B04	05B05
		05B06	05B07	05B08	05B09	05C01	05C02	05C03	05C04	05D02	05D03
		06A01	06B02	06C03	07B01	07C01	07C02	08A05	08A06	08C06	08D01
		08D02	08D03	08D07	08D08	08D10	08E01	08E02	08E03	08F03	09A01
		09A02	09A03	09A04	09B01	09B02	09B03	09B05	09C01	09D01	09E03
		09F01	09F02	10A04	10B01	10B02	10B04	10B05	10B06	11B01	11C04
		11D05	11D06	11E01	11E02	11E03	12E01				

Tabla D-2. *Plan de tratamiento del riesgo*

La tabla D.2 muestra la nomenclatura de los servicios a mejorar, estos servicios son los siguientes: Además, de los servicios de la tabla D.2 los autores de este trabajo de grado consideraron algunos otros que tienen relación con los controles seleccionados en la tabla D.1.

Nomenclatura	Significado
01B02-07	Obligaciones y responsabilidades del personal y la administración.
01C02	Gestión de personal estratégico, socios y proveedores.
01C03	Proceso de chequeo del personal.
01E01	Tomar en cuenta las necesidades para la continuidad del negocio.
01E02	Plan de continuidad del negocio.
01E03	Plan de recuperación del espacio de trabajo.
02A01	Gestión de derechos de acceso a la instalación o lugar de trabajo.
02A02	Gestión de autorización de acceso otorgado a la instalación o lugar de trabajo.
02A03	Control de acceso a la instalación o a la organización.
02A04	Detección de intrusión a la instalación o a la organización.
02C01	División de áreas en zonas de oficina protegidas.
02C02	Control de acceso físico a las zonas de oficina protegidas.
02C03	Gestión de autorización de acceso a áreas de oficina protegidas.
02C04	Detección de intrusión en áreas de oficina protegida.
02C05	Monitoreo de áreas de oficina protegidas.
02C06	Control de movimiento de proveedores de servicios ocasionales que requieren trabajar en las oficinas.
02D02	Protección de documentos y medios de soporte removibles.
02D03	Papelera de recolección y destrucción de documentos.
03A01	Calidad en el suministro de energía.
03A02	Continuidad en el suministro de energía.
03A05	Protección contra rayos.
03A06	Fiabilidad de los equipos de servicios.
03B01	Gestión de los derechos de acceso a los lugares sensibles.
03B02	Gestión de las autorizaciones de acceso otorgado a los lugares sensibles.
03B03	Control de acceso a los lugares sensibles
03B04	Detección de intrusos a los lugares sensibles
03B05	Monitoreo del perímetro. (vigilancia de los puntos de entrada y los alrededores de lugares sensibles)
03B06	Vigilancia de los lugares sensibles.
03B07	Control de acceso al cableado.
03C01	Prevención de riesgos a daños por agua.
03C02	Detección de daños por agua.
03C03	Evacuación de agua.
03D01	Prevención de riesgo en contra de incendios.
03D02	Detección de fuego.
03D03	Extinguidor de incendios.
04B02	Autenticación de una entidad para un acceso entrante a la WAN (red de área extensa)
04B03	Autenticación de la entidad que accede para un acceso de salida a través de la WAN
04C01	Cifrado de intercambio sobre las redes de área amplia WAN
04C02	Control de integridad del intercambio sobre las redes de área amplia WAN
05A03	Organización del mantenimiento del equipamiento de las redes de área local LAN
05A04	Proceso y recuperación siguiendo el plan de incidentes sobre la LAN
05A05	Plan de guardado y restablecimiento de las configuraciones de la LAN
05A06	Plan de recuperación de desastres (DRP) de la red de área local LAN

05B01	Gestión de perfiles de acceso sobre la red de área local
05B02	Gestión de privilegios y autorización de acceso (otorgamiento, delegación, revocación)
05B03	Autenticación de usuarios o entidades para requerimientos de acceso a la red de área local LAN de un punto de acceso interno, (este mecanismo corresponde por ejemplo a la implementación de autenticación en un controlador de dominios de Windows)
05B04	Autenticación de usuarios o solicitantes antes del acceso a la red de área local LAN de un sito remoto atreves de la red extendida
05B05	Autenticación de usuarios o solicitantes para el acceso desde el exterior a la red de área local LAN
05B06	Autenticación de usuarios o solicitantes para el acceso requerido a la red de área local LAN desde una subred wifi
05B07	Filtrado general de acceso a la red de área local
05B08	Control de enrutamiento de peticiones salientes
05B09	Autenticación de acceso a entidades externas para el ingreso saliente a sitios sensibles
05C01	Cifrado de las comunicaciones que se intercambian sobre las redes de rea local
05C02	Control de la integridad para el intercambio sobre las redes de área local
05C03	Cifrado del intercambio en el caso de acceso remoto hacia las redes de área local LAN
05C04	Protección de la integridad en el intercambio en el caso de acceso remoto a la red de área local LAN
05D02	Análisis off-line de la ruta, log de archivos y registro de eventos sobre la red de área local.
05D03	Gestión de incidentes sobre las redes de área local
06A01	Seguridad en la relación con el personal operacional (empleados, abastecedores o proveedores de servicios)
06A02	Control de la implementación o actualización del software o hardware
06A04	Control de mantenimiento remoto.
06B02	Control de las configuraciones de acceso a la red de equipos de usuario
06C01	Control de derechos especiales de acceso al equipamiento de red
06C02	Autenticación del administrador y personal operacional
06C03	Vigilancia de acciones administrativas sobre la red
07A01	Gestión de perfiles de acceso (derechos y privilegios concedidos por perfiles funcionales)
07A02	Gestión de autorización de acceso y privilegios (otorgamiento, delegación, revocación)
07A03	Autenticación de solicitantes de acceso (usuarios o entidades)
07A04	Filtrado de acceso y gestión de asociaciones
07B01	Control de acceso a datos residuales
07C01	Registro de loa accesos a recursos sensitivos
07C02	Registro confidencial del sistema de llamadas
07D01	Continuidad del servicio de la arquitectura y sus componentes
08A03	Control de aceptación de introducción o modificación de sistemas, los sistemas aquí incluyen sistemas operativos, aplicaciones y software intermedio asociado.
08A05	Consideraciones de confidencialidad durante el mantenimiento de los sistemas de producción
08A06	Control de mantenimiento remoto
08A07	Protección de documentos impresos sensible y reportes
08C03	Seguridad física de los medios mantenidos en sitio
08C04	Seguridad física de medios de almacenamiento (mantenidos en un sitio externo)
08C05	Verificación e importe de registro de medios de almacenamiento
08C06	Seguridad de almacenamiento de red (SAN: área de red de almacenamiento y NAS)
08C07	Seguridad física de los medios de transición
08D01	Organización del mantenimiento del hardware (para equipamiento operacional)
08D02	Organización del software de mantenimiento (sistemas, middleware y aplicaciones)
08D03	Proceso de recuperación de aplicaciones y plan de seguimiento de incidentes durante la operación

08D04	Backup de configuración del software (sistemas, aplicaciones y configuración de parámetros)
08D05	Backup de aplicaciones de datos
08D06	Plan de recuperación de desastres para funciones de IT
08D07	Antivirus para la protección de servidores de producción
08D08	Gestión de sistemas críticos (respecto al mantenimiento de la continuidad)
08D09	Emergencias fuera del sitio (recurso) backup
08D10	Mantenimiento de cuentas de usuario
08E01	Detección en línea y tratamiento de IT relacionado con eventos anormales e incidentes
08E02	Gestión fuera de línea u offline de rutas, logs y registro de eventos
08E03	Gestión de sistemas e incidentes de aplicaciones
08F01	Control de derechos de acceso administrativo otorgados sobre un sistema
08F02	Autenticación de administradores y personal operacional.
08F03	Vigilancia de las acciones del administrador de sistemas
09A01	Gestión de perfiles de acceso a aplicaciones de datos
09A02	Gestión de autorización de acceso a aplicaciones de datos (otorgamiento, delegación, revocación)
09A03	Autenticación del acceso a solicitantes
09A04	Filtros de acceso y gestión de asociaciones
09B01	Autenticación de la aplicación para el acceso a aplicaciones sensibles
09B02	Protección de la integridad en el intercambio de datos
09B03	Control de datos de entrada
09B04	Verificación permanente (exactitud, etc.) relacionados con datos
09B05	Continuo (plausibilidad,…) verificación del procesamiento de datos
09C01	Cifrado de los datos intercambiados, aquí nosotros consideramos el cifrado efectuado directamente por las aplicaciones (ISO CAPA 6-7 previo a o durante la transmisión)
09C02	Cifrado de datos guardados
09D01	Elevado registro de seguridad
09D02	Gestión de acceso a los archivos de datos
09E01	Reconfiguración del hardware
09E02	Plan de continuidad de servicios de aplicaciones
09E03	Gestión de aplicaciones críticas (con respecto al mantenimiento de la continuidad)
09F01	Prueba de origen, firma digital o electrónica
09F02	prevención de duplicación de mensajes y reenvío (numeración, secuencia)
10A04	Organización de mantenimiento de aplicaciones
10B01	Garantía de la seguridad en la organización por el desarrollo de aplicaciones
10B02	Garantía de confidencialidad en el desarrollo de aplicaciones
10B04	Protección de los datos durante la realización de pruebas
10B05	Seguridad del mantenimiento de aplicaciones
10B06	Mantenimiento en caliente
11B01	Control de acceso a las estaciones de trabajo
11C01	Protección de la confidencialidad de los datos sobre las estaciones de trabajo o sobre los servidores de datos (discos lógicos para las estaciones de trabajo)
11C02	Protección de la confidencialidad de los datos almacenados sobre medios removibles
11C04	Protección de la integridad de los archivos almacenados sobre las estaciones de trabajo o servidores de datos (discos lógicos para las estaciones de trabajo)
11C05	Seguridad del correo electrónico e intercambio de información electrónica
11D03	Plan de copias de respaldo de la configuración de los usuarios
11D04	Plan de copias de respaldo para datos de usuarios almacenados en los servidores de datos
11D05	Plan de copias de respaldo para los datos guardados sobre las estaciones de trabajo de los usuarios

11D06	Antivirus (malware, código ejecutable no autorizado, etc.) protección para las estaciones de trabajo de los usuarios
11D07	Plan de recuperación para las estaciones de trabajo de los usuarios
11D08	Gestión de acceso a oficinas de datos y archivos
11E01	Gestión de derechos de acceso privilegiado otorgado a los usuarios de las estacione de trabajo (derechos administrativos)
11E02	Autenticación y control de derechos de acceso de administradores y personal operacional
11E03	Vigilancia de las acciones de los administradores de los sistemas sobre las estaciones de trabajo de los usuarios
12A02	Control de la implementación de equipamiento nuevo o actualización de sistemas existentes
12B01	Personalización de equipamiento de red y cumplimiento de control de configuraciones
12B02	Adecuado control de software operacional a una versión de referencia
12E01	Gestión de privilegio de derechos de acceso otorgados a equipamientos o sistema (derechos administrativos)
12E02	Autenticación y control de derechos de acceso de administradores y personal operacional
12C01	Organización de mantenimiento de equipamiento operacional
12C02	Organización del mantenimiento del software (sistemas y servicios adjuntos)
12C03	copias de respaldo de la configuración del software (sistemas, servicios y parámetros de configuración)
12C04	Plan de recuperación de desastres
12C05	Gestión de sistemas críticos (respecto al mantenimiento de la continuidad)
12E01	
12E02	

Tabla D-3. *Nomenclatura de servicios de seguridad*

E. BIBLIOGRAFÍA

[1]"Anexo 1: Metodología de Clasificación de Activos – Modelo de Seguridad de la Información para Estrategia de Gobierno en Línea", Ministerio de Tecnología de la Información y las Comunicaciones, 2011. [En línea]. Disponible: http://css.mintic.gov.co/ap/gel4/images/SeguridaddelaInformacion2_0_Anexo7_Clasificacion-de-Activos.pdf. [Última Búsqueda: 29-Abril-2016].

[2]MEHARI 2010 Processing guide for risk analysis and management, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Processing-Guide.pdf. [Última Búsqueda: 27-Abril-2016].

[3]MEHARI 2010 Fundamental concepts and functional specifications, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf. [Última Búsqueda: 27-Abril-2016].

[4]MEHARI 2010 strategies for risk seriousness reduction and setting security level targets, v. 36. Paris: Clusif, 2016.

[5]MEHARI 2010 Risk Analysis and Treatment Guide, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf. [Última Búsqueda: 27-Abril-2016].

[6] "Implantación y Certificación del Sistema de gestión de la Seguridad de la Información – SGSI de la Universidad del Cauca", R-005, Universidad del Cauca, 2015.