DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA EL INSTITUTO NACIONAL DE VÍAS TERRITORIAL NARIÑO

CÉSAR ENRIQUE MORÁN FERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD
FACULTAD DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2016

DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA EL INSTITUTO NACIONAL DE VÍAS TERRITORIAL NARIÑO

CÉSAR ENRIQUE MORÁN FERNÁNDEZ

Proyecto de grado presentado como requisito para optar por el título de:
Especialista en Seguridad Informática

FRANCISCO NICOLAS JAVIER SOLARTE SOLARTE
Director

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD
FACULTAD DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2016

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

San Juan de Pasto, noviembre de 2016

DEDICATORIA

A mi esposa Adriana, a mis hijos Laura Marcela y César Alejandro, por su apoyo incondicional.

AGRADECIMIENTOS

Al Ing. Especialista en Seguridad Informática Francisco Nicolás Javier Solarte Solarte de la Universidad Nacional Abierta y a Distancia por brindar su asesoría valiosa y constante en la dirección, programación, realización y consecución de resultados a lo largo del proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

RESUMEN

El Instituto Nacional de Vías es un establecimiento público del orden nacional, con personería jurídica, autonomía administrativa y patrimonio propio, tiene como "objetivo la ejecución de las políticas, estrategias, planes, programas y proyectos de la infraestructura no concesionada de la Red Vial Nacional de carreteras primaria y terciaria, férrea, fluvial y de la infraestructura marítima, de acuerdo con los lineamientos dados por el Ministerio de Transporte"[1].

La Territorial Nariño de la entidad, produce y procesa diariamente datos inherentes a la infraestructura vial del departamento de Nariño, la cual es procesada para poder brindar información consistente, fiable y oportuna con el fin de facilitar la toma de decisiones que redundan en la ejecución de obras para el mantenimiento, construcción o rehabilitación de las carreteras a su cargo.

El desarrollo de herramientas informáticas en el mercado, la globalización de la economía, la apertura de datos, los servicios al ciudadano y las tendencias de apertura de la información, han obligado a las entidades a replantear los esquemas estratégicos en materia de tecnología; debido al aumento de los riesgos, por ello el diagnosticar las redes, la plataforma tecnológica, el software y sus posibles vulnerabilidades se ha convertido en una importante tarea de los especialistas del área a partir de la generación de las acciones tendientes a disminuir y mitigar los riesgos informáticos.

El Gobierno Nacional, a través de la estrategia de Gobierno en Línea, ha considerado el factor de seguridad como fundamental en toda la necesidad de democratización de la información y de los servicios al ciudadano; el Instituto Nacional de Vías Territorial Nariño no es ajeno a ello, por lo tanto, se pretende diseñar políticas y controles de seguridad para proteger la información; mejorar la atención a sus clientes, brindándoles eficiencia y calidad en la prestación de su servicio.

[1] COLOMBIA. Presidencia de la república. Decreto 2618 de 2013 por el cual se modifica la estructura del Instituto Nacional de Vías (Invías) y se determinan las funciones de sus dependencias. ART. 1 [En línea]. Disponible en: https://www.mintransporte.gov.co/descargar.php?idFile=13029 [citado en 20 de abril de 2016]

El presente proyecto tiene como objetivo fundamental, diseñar un Sistema de Gestión de Seguridad de la Información SGSI en el Instituto Nacional de Vías Territorial Nariño, bajo la Norma ISO/IEC 27001:2013 con el fin de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento de la entidad, instrucciones de los procedimientos a realizarse y la documentación que se debe desarrollar en todo el proceso para la posterior recomendación de implementación del SGSI, aplicando el modelo PHVA (Planificar, hacer, verificar y actuar).

Como primera medida se recolecta información de la Territorial Nariño del instituto a través de la observación, y encuesta que permiten tener una idea general del manejo de la seguridad en la entidad.

A continuación, se realiza un análisis de riesgos paso a paso desarrollando el inventario de activos, la valoración cualitativa de los activos, identificación de amenazas, identificación de salvaguardas para los activos, valoración y evaluación del riesgo y el informe de calificación del riesgo, que permiten identificar los riesgos más apremiantes a los que está expuesta la entidad.

Finalmente se establecerán las políticas y controles de seguridad requeridos en el sistema tendiente a la disminución de riesgos en el área de informática, para así contribuir al fortalecimiento de las medidas que se ven reflejadas al interior de la entidad y la prestación de un servicio oportuno y de calidad.

Palabras claves. Sistemas de Gestión de la Seguridad de la Información (SGSI), Estándar ISO/IEC 27001:2013, Metodología de Riesgos Informáticos, Seguridad informática.

INTRODUCCIÓN

La administración pública en general debe adelantar todos sus procesos teniendo en cuenta los principios orientadores de economía, celeridad, eficacia, imparcialidad, publicidad, moralidad e igualdad toda vez que la función pública se encuentra al servicio de los intereses generales, con el fin de cumplir con los fines del Estado, y un insumo importante para lograr este objetivo es la información

Con el avance de las tecnologías de la información y comunicaciones TIC, el compartir información a diario a través de los diferentes sistemas tecnológicos y electrónicos es una necesidad, pero también convierte la información en un activo vulnerable, por lo tanto, cada organización asume el reto de proteger su activo más preciado.

El Instituto Nacional de Vías Territorial Nariño, a través del diseño de un SGSI busca minimizar los riesgos a los que se encuentra expuesta la información de la entidad, para el desarrollo de la primera fase se aplica la metodología MAGERIT con la cual se realiza el análisis de riesgos que es uno de los procesos más importantes que se debe realizar dentro de la entidad, ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales esta expuestos, identificando amenazas y vulnerabilidades.

Para el análisis de riesgos se realiza un inventario de activos, valoración cualitativa de dichos activos, identificación de amenazas, riesgos y definición de salvaguardas. Una vez identificado claramente los activos que se encuentran en riesgo y que generarían mayor impacto en caso de sufrir un ataque, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles y el plan de gestión del riesgo, para cada uno de estos activos teniendo en cuenta lo expuesto por la Norma ISO/IEC 27001:2013.

1. TÍTULO

Diseño de un Sistema de Gestión de Seguridad de la Información SGSI basado en la norma ISO/IEC 27001:2013 para el Instituto Nacional de Vías Territorial Nariño.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA.

En la actualidad el manejo de la información es una de las herramientas necesarias para la operación de las organizaciones empresariales, lo anterior exige que se deba proteger los activos más importantes, entre ellos los relacionados con la información contenida en medios informáticos, a fin de garantizar su integridad, oportunidad, trazabilidad y confiabilidad de la misma.

Los problemas presentados y las fallas de seguridad registradas en las entidades, en ocasiones se deben al poco conocimiento que tienen las organizaciones del concepto de seguridad informática, ya que la mayoría de las veces las personas ignoran que existe un procedimiento para realizar una actividad. En ocasiones, si este procedimiento existe, lo omiten y operan de la manera que ellos mejor consideran creyendo que así es la forma correcta, siendo esto un aspecto negativo para la entidad.

El Instituto Nacional de Vías INVIAS Territorial Nariño, es un establecimiento público del orden nacional, adscrito al Ministerio de Transporte, que tiene como objetivo ejecutar las políticas y proyectos relacionados con la infraestructura vial a cargo de la Nación en la jurisdicción del departamento de Nariño, utiliza un gran volumen de información ya sea administrativa, contractual, etc., la cual en muchas ocasiones se ve expuesta a terceros, de ahí la importancia de realizar un análisis detallado de los errores que se pueden cometer, ya sea por la parte de los funcionarios o por parte del manejo de la seguridad que se lleva a cabo en la entidad, y también las deficiencias de la planta física.

2.2 FORMULACIÓN DEL PROBLEMA.

¿Cómo el Sistema de Gestión de Seguridad de la Información SGSI basado en la Norma ISO/IEC 27001:2013 mejorará la seguridad de la información en el Instituto Nacional de Vías – Territorial Nariño?

3. JUSTIFICACIÓN

Basados en las estrategias de Gobierno en Línea GEL del Estado Colombiano 2012-2015, la administración pública colombiana no puede quedarse atrás de los avances tecnológicos, especialmente cuando contribuyen a mejorar la transparencia y eficiencia en la gestión estatal y la apertura de datos, se establece que cada entidad debe desarrollar mecanismos para garantizar la seguridad de la información y controlar los riesgos que se derivan del modelo de datos abiertos orientados al ciudadano.

Dentro de las estrategias GEL, se establece que cada entidad debe establecer su Sistema de Gestión de Seguridad de la Información tanto para sus procesos misionales como para los de apoyo. De igual forma, dicho sistema debe contemplar el análisis de riesgos y las medidas a implementar en el modelo de apertura de datos de la entidad.

Preparar la Declaración de aplicabilidad que conlleven al Instituto Nacional de Vías Territorial Nariño, a mejorar la calidad y el acceso a los usuarios, así como el acceso a mayor información y datos, y que permita el aseguramiento de la información y el control de riesgos informáticos y de la información a la luz de la Norma ISO/IEC 27001:2013.

Es obligación de la administración pública adelantar todos sus procesos con observancia de los principios orientadores de economía, celeridad, eficacia, imparcialidad, publicidad, moralidad e igualdad toda vez que la función pública se encuentra al servicio de los intereses generales, con el fin de cumplir con los fines del Estado.

La ventajas de trabajar con un Sistema de Gestión de Seguridad de la Información SGSI en una entidad estatal, es alcanzar una mayor eficiencia administrativa, como la mejora en el desarrollo organizacional, en el desempeño, en proporcionar servicios que respondan a las necesidades y expectativas de los clientes internos y externos, con un mayor compromiso del nivel directivo y de los servidores públicos de la entidad, generando un punto de vista de la mejora y el desarrollo organizacional en las entidades públicas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información SGSI basado en la norma ISO/IEC 27001:2013 en el Instituto Nacional de Vías – Territorial Nariño, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos informáticos para establecer los dominios del estándar ISO/IEC 27001:2013.

- Determinar las vulnerabilidades, amenazas y riesgos de seguridad existentes para hacer la valoración de los mismos aplicando la metodología MAGERIT.

- Verificar la existencia de controles de acuerdo a la norma ISO 27002:2013 que ayude a definir la existencia de políticas y procedimientos de seguridad.

- Diseñar el SGSI para la empresa de acuerdo a los resultados de la evaluación realizada anteriormente, que permita obtener confidencialidad, integridad y disponibilidad de la información.

5. ALCANCES Y DELIMITACIÓN

El Sistema de Gestión de Seguridad de la Información SGSI basado en la norma ISO/IEC 27001:2013 se aplicará específicamente al sistema de información del Instituto Nacional de Vías INVIAS en la Territorial Nariño, la infraestructura tecnológica que lo soporta y los usuarios del sistema

El desarrollo del proyecto se llevará a cabo en las instalaciones del Instituto Nacional de Vías INVIAS Territorial Nariño en la ciudad de Pasto, durante el periodo de tiempo comprendido entre enero y mayo de 2016.

6. MARCO REFERENCIAL

Es importante conocer conceptos que están relacionados directamente con el tema a desarrollar en el presente proyecto, con un soporte teórico que permita clarificar definiciones y de esta manera dar respuesta a los requerimientos del proyecto, cada uno de los procesos en el desarrollo del proyecto significa la búsqueda de resultados y está acompañada de una buena investigación necesaria para alcanzar los objetivos propuestos.

6.1 MARCO TEÓRICO

6.1.1 Seguridad Informática

6.1.1.1 Conceptos de seguridad informática y seguridad de la información

La seguridad de la información se ha convertido en un tema muy importante en la actualidad debido al impacto que esta genera en las pequeñas, medianas y grandes empresas, lo que ha conllevado a que la información sea uno de los activos más importantes de las compañías.

La preocupación de una compañía en proteger la información, cada vez toma más fuerza debido al creciente desarrollo en la actualidad de las Tecnologías de Información y Comunicaciones TIC, las nuevas plataformas de sistematización existentes que facilitan la interconexión a través de las redes, permitiendo explorar más allá de las fronteras de la compañía. Esto ha conllevado a la aparición de nuevas amenazas en los sistemas de información, por lo que es una prioridad proteger la información más importante de las compañías; con la premisa de integrar los sistemas de información, para lo cual debe estar armonizado, y ajustado y con un plan de seguridad entre los diferentes procesos de una organización con el objeto de brindar confianza frente al negocio.

Debe existir una aceptación clara de cada uno de los miembros de la compañía en conocer las Políticas de Seguridad Informática PSI, toda vez que esta es un instrumento que permite adoptar una cultura de seguridad informática, encaminado a proteger los activos de información estratégicos de la organización, los cuales deben estar formados con los objetivos del negocio.

6.1.1.2 Conceptos de vulnerabilidad, amenazas y riesgos

- **Vulnerabilidad Informática.** La vulnerabilidad informática es un componente de un sistema informático que puede ser utilizado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

- ✓ Vulnerabilidad Física**.** Corresponden a la vulnerabilidad del entorno físico del sistema, hardware y servidores.

- ✓ Vulnerabilidad Natural. Corresponden a los acontecimientos imprevistos en el medio ambiente, que ocasiona a daños en los sistemas informáticos por, inundaciones, terremotos, en general por desastres naturales.

- ✓ Vulnerabilidad de Hardware. Se refiere básicamente a las fallas de las piezas físicas por mal uso, descuido, o por la desprotección de los equipos informáticos.

- ✓ Vulnerabilidad de Software. Referentes a errores del software, lo cual permite acceder a la aplicación por conocimiento del código fuente, lo que permite accesar la información.

- ✓ Vulnerabilidad de Medios y Dispositivos. Las vulnerabilidades de los dispositivos tales como discos duros, impresoras, memorias USB, equipos informáticos, entre otros.

- ✓ Vulnerabilidad de las Comunicaciones. Referentes a las redes y sus tipologías de conexión, lo que puede facilitar que los datos pueden ser capturados durante los procesos de transmisión.

- ✓ Vulnerabilidad Humana. Referente a la falta de conocimiento sobre la protección de datos e información por parte de los usuarios de los sistemas informáticos.

- ✓ Vulnerabilidad Económica. Referente a los recursos económicos que no son suficientes para la protección de los sistemas informáticos"[2].

- **Amenazas Informáticas.** Las amenazas informáticas son incidentes que pueden causar variaciones a la información de la entidad, las cuales pueden ocasionar su pérdida, con la consiguiente repercusión económica y del buen nombre de la entidad.

  Las amenazas se consideran como exteriores al sistema, es factible establecer medidas para minimizarlas y protegerse de las mismas, siendo imposible controlarlas y menos aún eliminarlas. Las amenazas se pueden clasificar en:

  - ✓ "Amenaza criminal. Referente a la violación de las normas y leyes por parte de los usuarios.

[2] Ibíd., p. 40.

- ✓ Negligencia. Referente a la falta de conocimiento por parte de los usuarios, lo que puede conllevar a las omisiones, acciones y decisiones que afectan a los sistemas informáticos.

- ✓ Amenazas de origen natural o físico. Es cuando el usuario propicia las condiciones para la ocurrencia de un hecho físico, que amenace el sistema informático.

- ✓ Intercepción. Se refiere a la penetración de los sistemas informáticos sin autorización para la manipulación de los archivos confidenciales de las organizaciones.

- ✓ Modificación. Se refiere al ingreso al sistema de información, y en donde se manipula la información para lograr el funcionamiento inadecuado del sistema informático.

- ✓ Interrupción. Se refiere a la saturación del sistema por inyección SQL, virus, troyanos, gusanos, código malicioso, para ocasionar el mal funcionamiento del sistema informático.

- ✓ Ingeniería social. Se refiere a las técnicas de engaño, donde a través del teléfono, correo electrónico, redes sociales se logra obtener datos personales de usuarios, claves de sistemas informáticos, con los cuales pueden obtener beneficios económicos, o de alguna otra naturaleza.

- ✓ Ingeniería social inversa. Se refiere cuando es el usuario quien busca la ayuda del atacante, y este último por intermedio de la de ingeniería social, se gana la confianza del usuario, la cual aprovecha para obtener toda la información necesaria, para posteriormente lograr el acceso no autorizado de los sistemas informáticos"[3].

- **Riesgos Informáticos.** Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información de una organización, si no se poseen las medidas adecuadas para proteger la información, los riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, de acuerdo a lo anterior los riesgos se pueden clasificar en:

  - ✓ "Riesgos de acceso. Se refiere cuando datos podrían estar expuestos y son vulnerables al ataque externo, por una inadecuada configuración de los sistemas, la falta de metodología de protección, entre otros.

[3] Ibíd. p. 42.

- ✓ Riesgos de integridad. Son los riesgos relacionados con el acceso, a los reportes de las organizaciones, destinados a sus sistemas de operaciones, tales como interfaz de usuario, procesamiento, administración de cambios.

- ✓ Riesgo de infraestructura. Se refiere a la existencia de una estructura tecnológica que no es segura a la hora de enfrentar alguna contingencia en sus sistemas de información, en el cual el hardware, software, procesos, canales de comunicación y redes son los elementos que soportan las necesidades de operación"[4].

6.1.1.3 Familia Normas de Seguridad Informática

La evolución de los rangos de numeración reservados por ISO va de 27000 a 27019 y de 27030 a 27044 con 27799 finalizando la serie formalmente en estos momentos.
La serie de normas de referencia y su estado de aprobación de Ediciones a lo largo del tiempo se indican a continuación:

- **ISO/IEC 27000:** Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI. Existen versiones traducidas al español, aunque hay que prestar atención a la versión descargada.

- **ISO/IEC 27001:2013.** Estándar que fue elaborado para suministrar un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La ISO/IEC 27001:2013, deja en libertad para determinar los criterios para constituir el proceso global de seguridad y adoptar el método para analizar, evaluar y gestionar los riesgos. En un proyecto de SGSI, la libertad puede convertirse en una deficiencia, pues en cierta forma está encadenando estos proyectos a la propia experiencia de diseño de técnicas de seguridad de los ejecutores del mismo.

  Para gestionar la información e implementar el Sistema de Gestión de Seguridad de la Información SGSI, se van a utilizar los 14 dominios de la ISO/IEC 27001:2013, a saber:

[4] Ibíd. p. 45.

- ✓ “Políticas de seguridad.
- ✓ Organización de la información.
- ✓ Seguridad en recursos humanos.
- ✓ Gestión de activos.
- ✓ Control de accesos.
- ✓ Criptografía.
- ✓ Seguridad física y ambiental.
- ✓ Seguridad en las operaciones.
- ✓ Transferencia de información.
- ✓ Adquisición de sistemas, desarrollo y mantenimiento.
- ✓ Relación con proveedores.
- ✓ Gestión de los incidentes de seguridad.
- ✓ Continuidad del negocio.
- ✓ Cumplimiento con requerimientos legales y contractuales”[5].

- **ISO/IEC 27002:2013.** A partir del año 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. En general se trata de una guía de buenas prácticas que describe los objetivos de control referentes a seguridad de la información. Es No certificable. Contiene 39 objetivos de control 133 controles, agrupados en 11 dominios. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.[6]

- **ISO/IEC 27003.** Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- **ISO/IEC 27004.** Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

[5] Ibíd. p. 54.
[6] Ibíd. p. 56.

- **ISO/IEC 27005.** Publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

- **ISO/IEC 27006.** Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007) y revisada el 30 de septiembre de 2015. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- **ISO/IEC 27007.** Publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

- **ISO/IEC TR 27008.** Publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

- **ISO/IEC 27009.** Publicada el 15 de junio de 2016. No certificable. define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A.

- **ISO/IEC 27010.** Publicada el 20 de octubre de 2012 y revisada el 10 de noviembre de 2015. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.

- **ISO/IEC 27011.** Publicada el 15 de diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005. Está publicada también como norma ITU-T X.1051.

- **ISO/IEC 27013.** Publicada el 15 de octubre de 2012 y actualizada el 24 de noviembre de 2015. Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI). Actualmente finalizando el proceso de revisión para su actualización.

- **ISO/IEC 27014.** Publicada el 23 de abril de 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

- **ISO/IEC TR 27015.** Publicada el 23 de noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.

- **ISO/IEC TR 27016.** Publicada el 20 de febrero de 2014. Es una guía de valoración de los aspectos financieros de la seguridad de la información.

- **ISO/IEC 27017.** Publicada el 15 de diciembre de 2015. Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.

- **ISO/IEC 27018.** Publicada el 29 de Julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

- **ISO/IEC TR 27019.** Publicada el 17 de Julio de 2013. Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía. Actualmente en proceso de revisión para su actualización.

- **ISO/IEC TR 27023.** Publicada el 02 de Julio de 2015. No certificable. Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.

- **ISO/IEC 27031.** Publicada el 01 de marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

- **ISO/IEC 27032.** Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

- **ISO/IEC 27033.** Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (Publicada el 15 de Diciembre de 2009 y revisada el 10 de Octubre de 2015); 27033-2, directrices de diseño e implementación de seguridad en redes (Publicada el 27 de Julio de 2012); 27033-3, escenarios de referencia de redes (Publicada el 3 de Diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (Publicada el 21 de Febrero de 2014); 27033-5, aseguramiento de comunicaciones mediante VPNs (Publicada el 29 de Julio de 2013); 27033-6, convergencia IP (en desarrollo); 27033-7, redes inalámbricas (en propuesta de desarrollo).

- **ISO/IEC 27034.** Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 6 partes: 27034-1, conceptos generales (Publicada el 21 de Noviembre de 2011); 27034-2, marco normativo de la organización (Publicada el 15 de Agosto de 2015); 27034-3, proceso de gestión de seguridad en aplicaciones (en desarrollo); 27034-4, validación de la seguridad en aplicaciones (en desarrollo); 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (en desarrollo); 27034-6, guía de seguridad para aplicaciones de uso específico (en desarrollo).

- **ISO/IEC 27035.** Publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes adicionales actualmente en fase de desarrollo.

- **ISO/IEC 27036.** Guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos (Publicada el 24 de marzo de 2014); 27036-2, requisitos comunes (Publicada el 27 de Febrero de 2014); 27036-3, seguridad en la cadena de suministro TIC (Publicada el 08 de Noviembre de 2013); 27036-4, seguridad en entornos de servicios Cloud (en desarrollo).

- **ISO/IEC 27037.** Publicada el 15 de octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

- **ISO/IEC 27038.** Publicada el 13 de marzo de 2014. Es una guía de especificación para seguridad en la redacción digital.

- **ISO/IEC 27039.** Publicada el 11 de febrero de 2015. Es una guía para la selección, despliege y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).

- **ISO/IEC 27040.** Publicada el 05 de enero de 2015. Es una guía para la seguridad en medios de almacenamiento.

- I**SO/IEC 27041.** Publicada el 19 de junio de 2015. Es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

- **ISO/IEC 27042.** Publicada el 19 de junio de 2015. Es una guía con directrices para el análisis e interpretación de las evidencias digitales.

- **ISO/IEC 27043.** Publicada el 04 de marzo de 2015. Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

- **ISO/IEC 27044.** En fase de desarrollo. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).

- I**SO 27799.** Publicada el 12 de junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. Actualmente en proceso de actualización.

6.1.1.4 Metodologías de Análisis y Evaluación de Riesgos. Actualmente hay varias metodologías para llevar a cabo el proceso de análisis, evaluación y gestión de riesgos informáticos, todos ellos tienen unos componentes y actividades comunes, tales como:

- **Identificar las Amenazas.** Identifica las posibles amenazas a la seguridad de la información.

- **Identificar las Vulnerabilidades.** Identifica las vulnerabilidades que podrían ser explotadas por las amenazas que se han identificado.

- **Identificar los Activos.** Identifica los activos críticos que impactan directamente en la confidencialidad, integridad y disponibilidad de la información.

- **Determinar el Impacto.** Determina y mide el impacto de una amenaza sobre un activo, en forma cuantitativa o cualitativa.

- **Determinar la Probabilidad.** Mide la posibilidad de ocurrencia de una amenaza asignándole un valor probable.

- **Identificar los Controles.** Identifica los controles que se están efectuando sobre un activo y el efecto sobre la amenaza que se está evaluando.

- **Tratamiento de Riesgos.** Está enfocado principalmente en los riesgos que representen un impacto importante que afecte considerablemente a personas o servicios, es decir, que sean clasificados como moderados o catastróficos. Para mitigar estos riesgos es necesario desarrollar estrategias para reducirlos a niveles aceptables, entre las estrategias están las siguientes:

  - ✓ **Mitigar o Reducir el Riesgo.** Utiliza varios mecanismos que pueden ser técnicos, administrativos o físicos y el objetivo es reducir la probabilidad o impacto del riesgo.
  - ✓ Asignar o Transferir del Riesgo. Transfiere el riesgo de una organización a otra entidad.
  - ✓ Aceptar el Riesgo. Las organizaciones conocen y aceptan los riesgos, pero el valor económico para mitigarlos supera al valor del activo a proteger.
  - ✓ Eliminar el Riesgo. La organización decide no tomar el riesgo, y elimina la amenaza por medio del cambio de los recursos o de la infraestructura informática.

Algunas de las metodologías para el análisis, gestión y evaluación de riesgos informáticos son las siguientes:

- **MAGERIT.** Es una metodología para facilitar el análisis y aplicación del sistema general de riesgos, proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

  MAGERIT persigue los siguientes objetivos:

"Que los responsables de los sistemas de información conozcan la existencia de riesgos y de la necesidad de mitigarlos a tiempo.
Metodología para analizar sistemáticamente tales riesgos.
Planificar las medidas oportunas para mantener los riesgos bajo control.
Que la organización se prepare para los procesos de evaluación, auditoría, certificación o acreditación"[7].

- **ISO/IEC 27005.** Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Describe el proceso completo de gestión de riesgos dividiéndolo en 6 fases: Establecimiento del Alcance, Valoración de Riesgos (formada por las tareas de Análisis y Evaluación), Tratamiento de Riesgos, Aceptación de Riesgos, Comunicación de Riesgos y Monitorización y Revisión de Riesgos.

- **EBIOS. Metodología Francesa de Análisis y Gestión de Riesgos.** Permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI), posibilitando también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos SSI. Fue desarrollada en un comienzo por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado no solo de Francia sino en otros países. La metodología EBIOS consta de un ciclo de 5 fases:

  - ✓ Fase 1: Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.
  - ✓ Fase 2 y 3: Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.
  - ✓ Fase 4 y 5: Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

- **COSO (Committee of Sponsoring Organizations of the Treadway Commission):** Es un modelo creado por la iniciativa de cinco organizaciones, American Accounting Association, AICPA, FEI, IMA y el instituto interno de auditores, enfocándose sobre la gestión de los riesgos empresariales.

[7] DORIA CORCHO, Andrés Felipe. Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la Universidad de Córdoba. Montería, 2015, 267 p. Trabajo de Grado. Universidad Nacional Abierta y a Distancia.

COSO permite relacionar las necesidades de alto nivel de efectividad y eficiencia en la operación, confiabilidad de los reportes financieros y cumplimiento con leyes y regulaciones, con requerimientos de administración de riesgo genéricos y específicos para los distintos procesos de negocio de una organización, incluyendo los procesos de apoyo como las Tecnologías de Información.

- **OCTAVE.** Es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo. Fue desarrollada por CERT y la Universidad Carnegie Mellon. El método OCTAVE se enfoca en tres fases, identificación de la información a nivel gerencial, identificación de la información a nivel operacional e identificación de la información a nivel de usuario final. OCTAVE posee tres versiones distintas: Método OCTAVE, fue desarrollado teniendo en cuenta grandes organizaciones de 300 o más empleados, OCTAVE-S, fue desarrollado en respuesta a las necesidades de organizaciones más pequeñas de alrededor de 100 personas o menos, y OCTAVE ALLEGRO que es una variante simplificada del método de OCTAVE que se centra en los activos de información.

- **DAFP.** Fue creado por el gobierno colombiano mediante el decreto 1599 del 20 de mayo del 2005, mediante el cual se adoptó el Modelo Estándar de Control Interno para todas las entidades del estado, este modelo presenta tres subsistemas de control: el estratégico, el de gestión y el de evaluación. El objetivo general de esta metodología es fortalecer la implementación y desarrollo de la política de la administración del riesgo a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de la misión y objetivos institucionales de las entidades de la Administración Pública. Esta metodología plantea que, con el fin de asegurar el manejo de los riesgos, es importante que se establezca el entorno de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos mediante: contexto estratégico, identificación de riesgos, análisis de riesgos, valoración de riesgos y políticas de administración de Riesgos

- **COBIT (Control Objectives for Information and related Technology):** Es un modelo de gobierno para administrar el riesgo y controlar las Tecnologías de Información. Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT Governance Institute, COBIT enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT.

El propósito de COBIT es brindar a la Alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan. COBIT permite entender como dirigir y gestionar el uso de tales sistemas, así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. COBIT suministra las herramientas para supervisar todas las actividades relacionadas con tecnologías de la información.

COBIT está divido por dominios que agrupan procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible. En la actualidad se encuentra la versión 5.

- **Análisis de riesgos Informáticos.** El análisis de riesgos informáticos es un acercamiento metodológico para determinar el riesgo siguiendo unos procedimientos normalizados, tales como:

  - ✓ Determinar los activos más importantes para la organización, su interrelación y su valor.
  - ✓ Determinar el de amenazas están expuestos los activos.
  - ✓ Estimar el impacto o daño sobre los activos determinados.
  - ✓ Estimar el riesgo, expresado como el impacto ponderado de la expectativa de materialización de la amenaza.

La administración del riesgo es utilizada para minimizar el riesgo aplicando indudablemente medidas de seguridad según las:

- ✓ Amenazas.
- ✓ Vulnerabilidades y
- ✓ El valor de los activos a ser protegidos

Con el Análisis se logra:

- ✓ Identificar los riesgos.
- ✓ Evaluar del posible daño que pueden causar.
- ✓ Justificación de las medidas de seguridad.

Objetivos del análisis del riesgo.

- ✓ Considerar el impacto de las amenazas permisibles.
- ✓ Establecer un valor del costo de la pérdida de un negocio por la manifestación de un riesgo.
- ✓ Identificación de los riesgos.

- ✓ El valor que justifica la seguridad y control.

Características del análisis de riesgo.

- ✓ Considera el costo de los sistemas informáticos, de acuerdo al impacto de la pérdida o modificación de la información.
- ✓ Establece un método de comparación de las vulnerabilidades individuales.
- ✓ Define e implementa requerimientos de seguridad.
- ✓ Evaluación de las amenazas y vulnerabilidades conocidas.

El análisis de riesgos es una herramienta que permite entender los riesgos y las vulnerabilidades asociadas a la información y la tecnología que la habilita, para establecer una arquitectura que reduzca el nivel del riesgo.

Gestión de riesgo.

Para la gestión de un riesgo, se puede tomar varias alternativas.

- ✓ "Aceptarlo
- ✓ Transferirlo
- ✓ Mitigarlo, con la implementación de políticas de seguridad.
- ✓ Evitarlo"[8].

6.1.1.5 Metodología Magerit. "El CSAE (Consejo Superior Administración Electrónica) de España ha elaborado y promueve MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios"[9].

La elección de MAGERIT se debe a que:

- Los pasos para su ejecución están claramente definidos.

[8] SARRIA CUELLAR, Mercedes. Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. Florencia, 2015, 175 p. Trabajo de Grado. Universidad Nacional Abierta y a Distancia.

[9] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

- La documentación es clara, amplia y permite realizar una identificación adecuada del entorno donde va a ser aplicada.

- Permite enfocar los esfuerzos al análisis de riesgos críticos para la empresa, por lo tanto, se puede trabajar más claramente en las posibles soluciones para dichos riesgos.
- Se puede decir que por estar incluida en los estándares ISO, sirve como punto de partida para procesos de certificación y mejoramiento del sistema de gestión para la empresa.

- Permite el análisis a riesgos, donde se identifican y valoran los diferentes componentes que pueden tener los riesgos.

- Permite la minimización de riesgos mediante la implementación de medidas de seguridad.

- MAGERIT le permita una empresa saber cuánto valor está en juego y le ayudará a protegerlo.

- Con MAGERIT los resultados de análisis de riesgos se pueden expresar en valores cualitativos y cuantitativos, lo que permite a los directivos tomar decisiones.

6.1.1.6 Sistema de Gestión de la Seguridad de la Información SGSI. "Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta estratégica como soporte a las organizaciones para implementar políticas de seguridad informática, controles y procedimientos de seguridad informática alineados con los objetivos del negocio, con el objeto de valorarse y de esta forma obtener un panorama general sobre el estado de los riesgos y que estos sean conocidos, apropiados, minimizados y gestionados por la organización, este proceso debe ser de una forma organizada, es decir, estructurado, sistemático y adaptado a los cambios de la organización, todo este proceso debe ser documentado"[10].

De acuerdo a la norma ISO 27001, la seguridad de la información se fundamenta en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas comprometidos en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

[10] ISO 27001. (2005). ¿Qué es un SGSI? El portal de ISO 27001 en español. [en línea]. disponible en: http://www.iso27000.es [citado en 25 de abril de 2016].

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

"En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI"[11]

Figura 1. SGSI

Fuente. http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

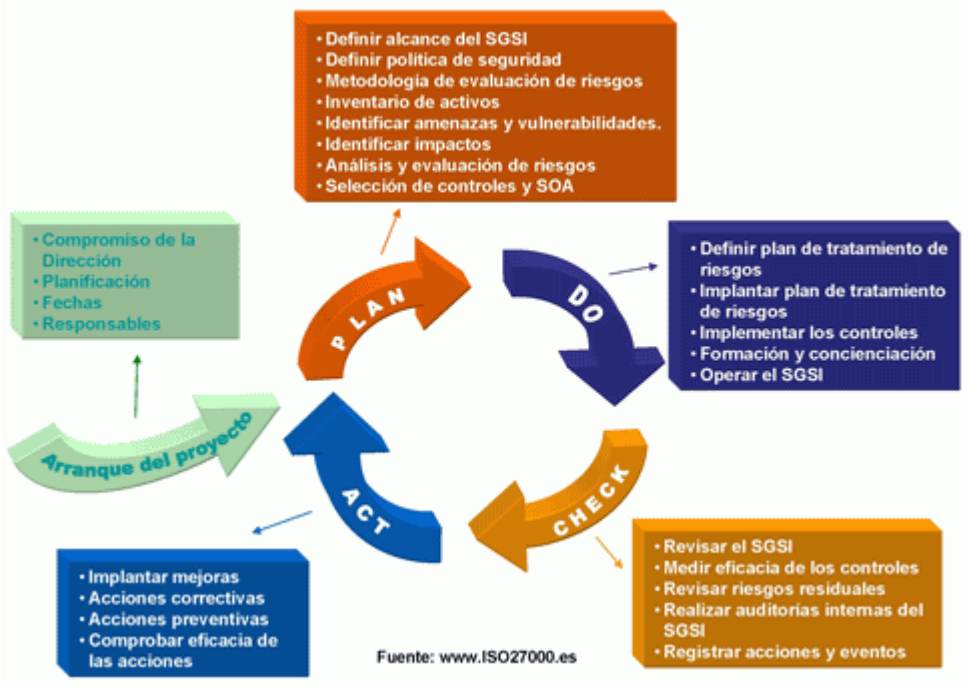
6.1.1.7 Diseño e Implementación del SGSI. En esta fase tendiente al diseño e implementación del SGSI, se debe utilizar los fundamentos teóricos del ciclo de Deming que habla sobre PHVA.

[11] Ibíd., [en línea]. disponible en: http://www.iso27000.es [citado en 25 de Abril de 2016].

Cada una de estas fases cumple un objetivo específico dentro del sistema, como se muestra a continuación:

- “Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI”[12]

Figura 2. Ciclo PDCA



Fuente. http://www.iso27000.es/sgsi_implantar.html#seccion1

[12]Sistema de Gestión de la Seguridad de la Información, p. 7. [en línea] disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf [citado en 25 de abril de 2016].

- **Plan: Establecer el SGSI**

  - ✓ “Especificar el alcance del SGSI en términos de la actividad principal, la organización de la empresa, localización, activos y conocimientos, se debe incluir referencias y justificación de las exclusiones.
  - ✓ Especificar una política de seguridad de la información que incluya el marco general y los objetivos por parte de la organización, también debe tener en cuenta los requerimientos legales, contractuales referentes a la seguridad de la información, y debe estar alineada con el entorno estratégico de gestión de riesgos de la organización en el que se constituirá y conservará el SGSI.
  - ✓ Precisar la evaluación de riesgos con una metodología apropiada para el SGSI y los requerimientos de la organización, también instituir los criterios de aceptación del riesgo y definir los niveles de riesgo aceptable. Lo importante de esta metodología es que los resultados adquiridos sean comparables y confiables para evitar puntos de vista que no sean objetivos con la valoración de los riesgos.
  - ✓ Determinar los riesgos, identificando los activos que están dentro del alcance del SGSI y a sus responsables; determinar las amenazas en relación a los activos; identificar las vulnerabilidades que puedan ser explotadas por dichas amenazas; y determinar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
  - ✓ Determinar y evaluar los riesgos, evaluando el impacto en la organización de un fallo de seguridad que conlleve la pérdida de confidencialidad, integridad o disponibilidad de un activo relacionado con la información; evaluar la posibilidad de ocurrencia de un fallo de seguridad relacionado con las amenazas, vulnerabilidades, impactos y los controles implementados; evaluar los niveles de riesgo; y establecer, de acuerdo a los criterios de aprobación de riesgo previamente determinados, si el riesgo es aceptable o debe ser tratado.
  - ✓ Determinar y evaluar las diferentes opciones de tratamiento de los riesgos, empleando controles adecuados; admitir el riesgo, con la condición de que siga cumpliendo con las políticas y criterios determinados para la aceptación de los riesgos; evitar el riesgo, mediante la interrupción de las actividades que lo causan; transferir el riesgo a terceros como por ejemplo compañías aseguradoras o proveedores de outsourcing”[13].

[13] Ibíd., p. 7.

Figura 3. Gestión de riesgos

Fuente. http://www.iso27000.es/sgsi_implantar.html#seccion1

La dirección debe ratificar los riesgos residuales, implantación y uso del SGSI: "La declaración de aplicabilidad al menos debe incluir los objetivos de control, controles seleccionados y los motivos de su elección; los objetivos de control y controles que en la actualidad están implantados; los objetivos de control y controles descartados y los motivos de su exclusión; este procedimiento permite detectar posibles omisiones involuntarias"[14].

En relación a los controles de seguridad, el estándar ISO 27002:2013 proporciona una completa guía de implantación que contiene 114 controles, según 35 objetivos de control agrupados en 14 dominios.

[14] Ibíd., p. 9.

- **Do: Implementar y utilizar el SGSI**

Figura 4. Do

Fuente. http://www.iso27000.es/sgsi_implantar.html#seccion1

- ✓ Especificar un plan de tratamiento de riesgos, cuyo objetivo sea identificar las actividades, recursos, responsabilidades y prelaciones en la gestión de los riesgos de seguridad de la información.
- ✓ Establecer el plan de tratamiento de riesgos, con la finalidad de alcanzar los objetivos de control identificados, recursos, responsabilidades y prioridades.
- ✓ Implementar los controles escogidos, para que se trasladen a los objetivos de control.
- ✓ Precisar un sistema de métricas para obtener resultados comparables que nos permita medir la efectividad de los controles.
- ✓ Gestionar programas de capacitación en relación a la seguridad de la información a todos los colaboradores de la organización.
- ✓ Legalizar las operaciones del SGSI.
- ✓ Gestionar los recursos establecidos al SGSI para el funcionamiento y mantenimiento de la seguridad de la información.
- ✓ Establecer procedimientos que admitan una rápida detección y respuesta a los incidentes de seguridad.[15]

[15] Ibíd., p. 9.

- **Check: Monitorizar y revisar el SGSI**

Figura 5. Check

Fuente. http://www.iso27000.es/sgsi_implantar.html#seccion1

La organización debe establecer procedimientos de monitorización y revisión para:

- ✓ Descubrir los errores en los resultados generados por el procesamiento de la información, a tiempo.
- ✓ Establecer incidentes de seguridad.
- ✓ Trabajar en colaboración con la dirección, para determinar si las acciones desarrolladas por los colaboradores, y unidades tecnológicas para garantizar la seguridad de la información se realizan de acuerdo a lo planeado.
- ✓ Descubrir y prevenir incidentes de seguridad utilizando los indicadores.
- ✓ Establecer si las actividades realizadas para resolver los problemas de seguridad fueron positivas.
- ✓ Inspeccionar la efectividad del SGSI de manera habitual, referente al cumplimiento de la política y objetivos, las observaciones de auditorías de seguridad, incidentes, resultados de eficiencia, propuestas y observaciones de todas las partes interesadas.
- ✓ Determinar la confianza de los controles para comprobar que se cumple con los requisitos de seguridad.
- ✓ Revisar periódicamente en intervalos determinados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que se hayan producido en la organización, la tecnología, los objetivos y procedimientos de negocio, las amenazas reconocidas, la garantía de los controles implementados y el medio ambiente exterior, requerimientos legales, obligaciones contractuales, etc.
- ✓ Realizar periódicamente auditorías internas del SGSI en intervalos de tiempo planificados.

- ✓ Inspeccionar el SGSI por parte de la dirección habitualmente, para certificar que los objetivos definidos siguen vigentes, y que las mejoras en el proceso del SGSI son incuestionables.
- ✓ Renovar los planes de seguridad de acuerdo a las conclusiones y nuevos hallazgos encontrados en las actividades de monitorización y revisión.
- ✓ Reconocer eventos que hayan impactado la efectividad del SGSI.[16]

- **Act: Mantener y mejorar el SGSI**

  - ✓ Establecer en el SGSI las mejoras referidas.
  - ✓ Ejecutar las acciones preventivas y correctivas adecuadas.
  - ✓ Notificar las acciones y mejoras a los interesados.
  - ✓ Confirmar que las mejoras establecidas alcanzan los objetivos previstos.
  - ✓ PDCA es un ciclo de vida continuo, es decir, la fase de Act lleva de nuevo a la fase de Plan para reiniciar un nuevo ciclo de las cuatro fases.[17]

Figura 6. Act

Fuente. http://www.iso27000.es/sgsi_implantar.html#seccion1

La organización regularmente deberá:

- ✓ Establecer en el SGSI las mejoras identificadas.
- ✓ Realizar las operaciones preventivas y correctivas apropiadas para prevenir no conformidades antes de que se produzcan, y corregir no conformidades detectadas y materializadas.
- ✓ Comunicar las acciones y mejoras a las partes interesadas en forma detallada y acordar, la forma de proceder.
- ✓ Confirmar que las mejoras realizadas alcanzan los objetivos previstos.

[16] Ibíd. p. 10.
[17] Ibíd. p. 11.

“El PDCA es un ciclo de vida continuo, es decir la fase de Act lleva de nuevo a la fase de Plan, para iniciar un nuevo ciclo de las cuatro fases, no necesariamente tiene que haber una secuencia estricta en el orden de las fases”[18].

6.2 MARCO CONCEPTUAL

A continuación, se definen algunos términos que serán mencionados y utilizados en el proyecto:

Amenaza. El concepto de amenaza, es todo factor que genera la posibilidad que ocurra un evento, y que puede causar o no un daño, originado por factores externos a la organización.

Vulnerabilidad. El concepto de vulnerabilidad demuestra el grado de incapacidad para anticipar, asimilar, y recuperarse de un evento natural o un acto humano, producido por factores internos a la organización.

Riesgo. El concepto de riesgo, es lo que puede llegar a suceder, cuando la vulnerabilidad y la amenaza actúan juntas, lo cual puede generar la daño en la información, en la estructura física, material o humana.

Confidencialidad. Es la capacidad del sistema para suministrar las garantías, para identificar a los usuarios que acceden al sistema de información, a través de controles adecuados.

Disponibilidad. Es la capacidad del sistema para mantener el acceso en cualquier momento, controlando los intentos de modificar archivos o eliminar registros, por intermedio de la identificación del usuario y clave de acceso.

Integridad. Es la capacidad del sistema para garantizar la modificación, borrado, manipulación y el almacenamiento de los archivos, solamente por el personal autorizado en forma controlada, suministrando las metodologías de seguridad correspondientes para salvaguardar la información.

Trazabilidad. Es la capacidad del sistema de determinar quién hizo qué y en qué momento, con el objetivo de analizar los incidentes, detectar los ataques y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Autenticidad. Es la capacidad de una entidad para determinar, para verificar y garantiza la fuente de la que proceden los datos, referente a la autenticidad de la información se puede manipular desde el origen o el contenido de los datos.

[18] Ibíd., p. 11.

6.3 MARCO LEGAL

En Colombia, a nivel de seguridad de la información, la entidad bajo estudio debe cumplir con la siguiente legislación.

Ley 1273 del 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, básicamente es la Ley general de delitos informáticos que clasifica y asigna penas para delitos y crímenes relacionado con tecnología e informática.

Ley 594 de 2000. Ley general de archivo de la nación que dispone tiempos de retención y cuidados para documentación física de tipo público.

Ley 1341 del 30 de julio de 2009. Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley 527 del 18 de agosto de 1999. Ley de comercio electrónico que establece lineamientos y protección para acceso y uso de mensajes de datos, comercio electrónico y firmas digitales.

Ley 23 de 1982. Ley de derechos de autor aplicable a propiedad intelectual.

Ley estatutaria 1266 del 31 de diciembre de 2008. La Ley Estatutaria 1266 del 31 de diciembre de 2008, por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012. Ley que establece los requerimientos para la protección de la información personal almacenada por las organizaciones y evitar la divulgación de la misma.

Ley 962 del 8 de Julio de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. (Diario Oficial nº 45.963)

Ley 1712 de 6 de marzo de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones. (Diario Oficial nº 49.084 de 6 de marzo de 2014).

6.4 MARCO CONTEXTUAL

El Instituto Nacional de Vías INVIAS inició labores el primero de enero de 1994 mediante el decreto 2171 del 30 de diciembre de 1992, el cual creó un establecimiento público del orden nacional, con personería jurídica, autonomía administrativa y patrimonio propio, adscrito al Ministerio de Transporte, cuyo objetivo general es ejecutar las políticas y proyectos relacionados con la infraestructura vial a cargo de la Nación.

Durante el fortalecimiento del sector transporte INVIAS también asumió nuevas funciones y su estructura interna cambió con los Decretos N° 2056 y 2067 del 24 de julio de 2003.

El Instituto Nacional de Vías pertenece a la Rama Ejecutiva, adscrito al Ministerio de Transporte. Los cerca de 13.000 kilómetros de extensión que tiene la infraestructura vial del país son, en síntesis, es la razón de ser, cuidando día a día las 7 troncales, que recorren el territorio colombiano de Norte a Sur, y de las 8 transversales que unen a dichas troncales en su tránsito Oriente - Occidente.[19]

Objetivo: El Instituto Nacional de Vías, Invías, tendrá como objeto la ejecución de las políticas, estrategias, planes, programas y proyectos de la infraestructura no concesionada de la Red Vial Nacional de carreteras primaria y terciaria, férrea, fluvial y de la infraestructura marítima, de acuerdo con los lineamientos dados por el Ministerio de Transporte, y entre sus actividades están:

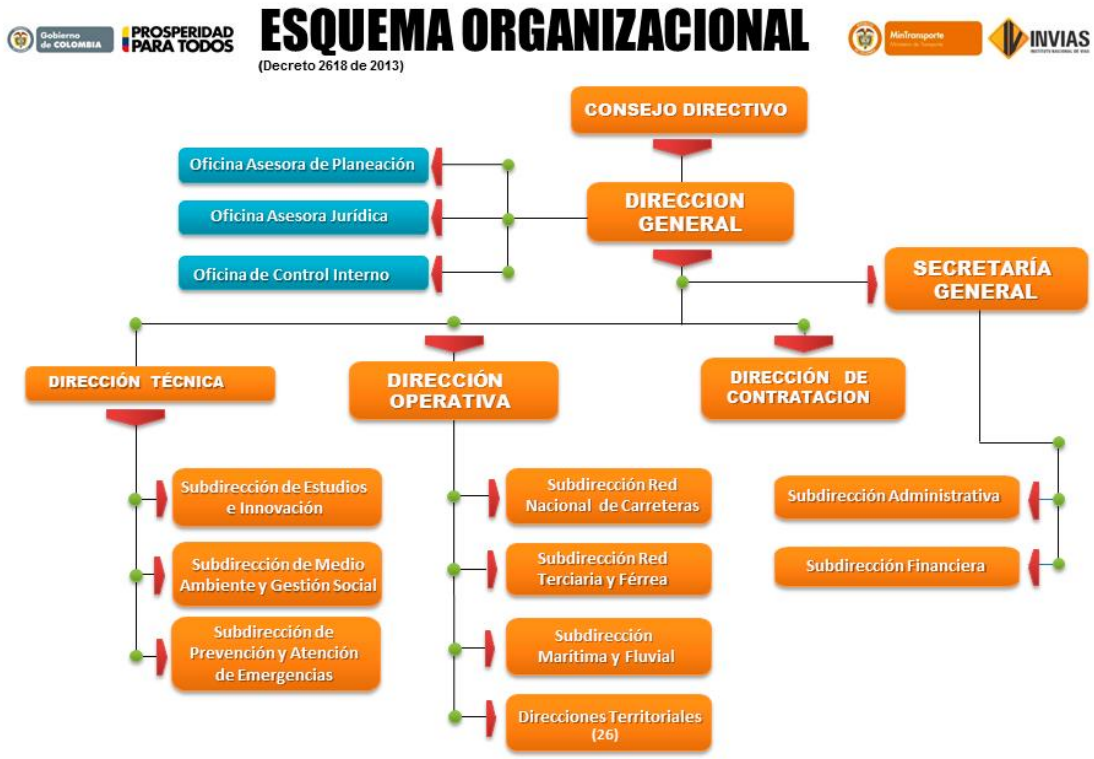
- Ejecutar la política del Gobierno Nacional en relación con la infraestructura de su competencia, de conformidad con los lineamientos establecidos por el Ministro de Transporte.
- Elaborar conjuntamente con el Ministerio de Transporte los planes, programas y proyectos tendientes a la construcción, reconstrucción, mejoramiento, rehabilitación, conservación, atención de emergencias, y demás obras que requiera la infraestructura de su competencia.
- Coordinar con el Ministerio de Transporte la ejecución de los planes y programas de su competencia.
- Adelantar investigaciones, estudios, y supervisar la ejecución de las obras de su competencia conforme a los planes y prioridades nacionales.
- Asesorar y prestar apoyo técnico a las entidades territoriales o a sus organismos descentralizados encargados de la construcción, mantenimiento y atención de emergencias en las infraestructuras a su cargo, cuando ellas lo soliciten.

[19] Objetivos y Funciones. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/objetivos-y-funciones [citado en 08 de abril de 2016].

- Recaudar los peajes y demás cobros sobre el uso de la infraestructura vial de su competencia.
- Celebrar todo tipo de negocios, contratos y convenios que se requieran para el cumplimiento de su objetivo.
- Elaborar, conforme a los planes del sector, la programación de compra de terrenos y adquirir los que se consideren prioritarios para el cumplimiento de sus objetivos.
- Adelantar, directamente o mediante contratación, los estudios pertinentes para determinar los proyectos que causen la contribución nacional por valorización en relación con la infraestructura de su competencia, revisarlos y emitir concepto para su presentación al Ministro de Transporte, de conformidad con la ley.
- Dirigir y supervisar la elaboración de los proyectos para el análisis, liquidación, distribución y cobro de la contribución nacional de valorización, causada por la construcción y mejoramiento de la infraestructura de transporte de su competencia.
- Prestar asesoría en materia de valorización, a los entes territoriales y entidades del Estado que lo requieran.
- Proponer los cambios que considere convenientes para mejorar la gestión administrativa.
- Definir las características técnicas de la demarcación y señalización de la infraestructura de transporte de su competencia, así como las normas que deberán aplicarse para su uso.
- Ejecutar los planes, programas y proyectos relacionados con el desarrollo de la infraestructura a su cargo.
- Controlar y evaluar la ejecución de las políticas, planes, programas y proyectos relacionados con el desarrollo de la infraestructura a su cargo.
- Definir la regulación técnica relacionada con la infraestructura de los modos de transporte carretero, fluvial, férreo y marítimo.
- Coordinar con la Agencia Nacional de Infraestructura, ANI, la entrega, mediante acto administrativo, de la infraestructura de transporte, en desarrollo de los contratos de concesión.
- Las demás que se le asignen.[20]

[20] Objetivos y Funciones. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/objetivos-y-funciones [citado en 08 de abril de 2016].

Figura 7. Esquema organizacional Invías



Fuente. http://www.invias.gov.co/index.php/informacion-institucional/organigrama

Misión: La misión del INVIAS, es ejecutar políticas, estrategias, planes, programas y proyectos de infraestructura de la Red Vial carretera, férrea, fluvial y marítima, de acuerdo con los lineamientos dados por el Gobierno Nacional.[21]

Visión: Para el 2030 el INVIAS será reconocido por su liderazgo en la ejecución de infraestructura vial, con procesos de innovación tecnológica y un enfoque descentralizado; que favorece la articulación del transporte intermodal, la conectividad entre centros de producción y de consumo, para la generación de redes productivas y la integración regional y Territorial en el país.[22]

[21] Misión y visión. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/objetivos-y-funciones [citado en 08 de abril de 2016].
[22] Misión y visión. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/objetivos-y-funciones [citado en 08 de abril de 2016].

Política de Calidad: Contribuir al desarrollo vial de nuestro país y a la satisfacción de clientes y usuarios manteniendo la infraestructura vial, contratando la ejecución de los programas y proyectos viales definidos por el Gobierno Nacional con eficiencia y calidad, mediante el mejoramiento continuo de sus procesos y contando para ello con un talento humano competente.

Objetivos de Calidad

- ✓ "Contribuir al desarrollo vial del País.
- ✓ Propender por la Satisfacción de clientes de INVÍAS y usuarios de la infraestructura vial.
- ✓ Mantener la infraestructura vial a cargo de INVÍAS.
- ✓ Contratar la ejecución de los programas y proyectos viales.
- ✓ Lograr eficiencia y calidad en los programas y proyectos viales.
- ✓ Mejoramiento continuo de los procesos.
- ✓ Potenciar el talento humano"[23].

[23] Objetivos de calidad. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/organigrama/mision-y-vision [citado en 08 de abril de 2016].

7. MARCO METODOLOGICO

7.1 TIPO DE INVESTIGACIÓN

El enfoque de la investigación es cuantitativo ya que se pretende hacer la medición de las vulnerabilidades, amenazas y riesgos en cuanto a la confidencialidad, integridad y disponibilidad de la información.

Es una investigación de tipo explicativa porque se trata de explicar la relación existente entre las vulnerabilidades existentes y los ataques que pueden presentarse en el sistema de información a causa de esas vulnerabilidades.

Es descriptiva porque trata de describir cómo se lleva a cabo el proceso de análisis y evaluación de los riesgos haciendo uso de la metodología MAGERIT.

7.2 METODOLOGÍA DE DESARROLLO

El proyecto está enfocado al diseño de un Sistema de Gestión de Seguridad de la Información SGSI bajo la norma ISO/IEC 27001:2013, que permita definir las políticas de seguridad orientadas a la disminución de riesgos para la información del Instituto Nacional de Vías INVIAS Territorial Nariño, y a satisfacer los requerimientos necesarios para la prestación de un buen servicio con eficiencia y calidad.

Para identificar y determinar los activos informáticos mediante la aplicación de instrumentos de recolección de información para establecer los dominios del estándar ISO 27001:2013, se deben realizar las siguientes actividades:

- Realizar visitas al Instituto Nacional de Vías Territorial Nariño, y realizar encuestas a funcionarios de los diferentes departamentos de la Territorial Nariño del Instituto Nacional de Vías, así como la observación directa de los procesos se pretende realizar una investigación analítica y descriptiva donde se identifiquen los componentes necesarios a tener en cuenta en el diseño del SGSI.

- Se analizará las necesidades en el área de informática en cuanto a seguridad física, seguridad interna, seguridad externa, seguridad lógica, seguridad perimetral, elementos de control para la seguridad del hardware y software, alcances, análisis de riesgos, amenazas, posibles ataques, plan de contingencia y políticas de seguridad.

La observación directa y la aplicación de la encuesta tienen como fin medir el grado de conocimiento sobre la importancia de seguridad en el manejo de la información, y la importancia del seguimiento y aplicación de políticas de seguridad.

Una vez analizada la información se propondrá políticas de seguridad a implementar teniendo en cuanta la Norma ISO/IEC 27001:2013 para disminuir los riesgos en cuanto a la seguridad de la información.

7.3 POBLACIÓN Y MUESTRA

7.3.1 Población. Para la encuesta de los funcionarios, la población de estudio está conformada por el personal que labora en la Territorial Nariño del Instituto Nacional de Vías.

Tabla 1. Población conformada por los funcionarios del Instituto Nacional de Vías Territorial Nariño

Población	Número de funcionarios
Instituto Nacional de Vías Territorial Nariño	**19**
Total	**19**

Fuente: Esta Investigación, 2016.

7.3.2 Muestra. Teniendo en cuenta que el personal que labora en la Territorial Nariño es un número de funcionarios relativamente pequeño, se tomó como muestra el total de funcionarios = 19.

7.4 RECOLECCIÓN DE LA INFORMACIÓN

La información que se pretende recopilar se obtendrá de la Territorial Nariño, generalidades, situación actual y en general el análisis de riesgos de seguridad en el área de informática.

7.4.1 Información primaria. Mediante encuestas aplicadas a los funcionarios de la Territorial Nariño se determinará la problemática interna de la Territorial Nariño referente al manejo de la información, los procedimientos de seguridad actuales y la implementación de políticas de seguridad necesarias para disminuir riesgos, además de la ejecución de pruebas de reconocimiento y mapeo que permitan detectar posibles riesgos a los que está expuesta la información.

7.4.2 Información secundaria. Los requerimientos externos se determinarán con la información de tipo bibliográfico, páginas de internet, los conocimientos adquiridos en el transcurso de la especialización, que nos permiten enfocarnos en el objeto de investigación.

7.4.3 Instrumentos de recolección de información. Para la recolección de la información se utilizó la técnica de observación directa, y la técnica de la encuesta.

7.4.4 Técnica de Observación. Con el objeto de observar cómo se realizan las siguientes actividades: Inicio del sistema, ubicación del servidor, ingreso de datos al sistema, elaboración de copias de seguridad, actualización de información, manejo de correos electrónicos.

7.4.5 Técnica de Encuesta. Para la realizar la encuesta a los funcionarios, se utiliza un cuestionario que contiene preguntas cerradas, preguntas categorizadas con respuesta en abanico, preguntas de estimación. Para la estructuración del documento se tomó en cuenta variables como: Tiempo, frecuencia, calidad, problemas, estados, reportes y nivel de satisfacción.

7.5 MUESTRA

7.5.1 Muestra funcionarios. Para la estructuración del documento de encuesta se tomó en cuenta aspectos tales como: Incidentes presentados respecto a la confidencialidad, integridad y disponibilidad de la información, manejo de contraseñas, medidas y políticas de seguridad, fallos, robos, virus etc.

7.5.2 Características de la encuesta para funcionarios de la Territorial Nariño. El instrumento consta de: 10 ítems, la forma de contestar es escrita en un tiempo de 15 a 20 minutos.

7.6 DESCRIPCIÓN DEL INSTRUMENTO

7.6.1 Presentación. Los instrumentos están diseñados con base en el siguiente criterio: El cumplimiento de los Objetivos.

7.6.2 Normas de Administración. Los instrumentos fueron aplicados en forma individual a los funcionarios de la Territorial Nariño. El diseño de ítems consta de preguntas cerradas, preguntas categorizadas con respuesta en abanico, preguntas de estimación y de opción múltiple las cuales el sujeto puede elegir la respuesta con la que mayor se identifique.

7.6.3 Áreas que explora. La elaboración de los instrumentos permite indagar si existen falencias y dificultades en los procesos de manejo y seguridad de la información.

7.7 PROCESAMIENTO DE LA INFORMACIÓN

La información disponible para el diseño de un Sistema de Gestión de Seguridad de la Información SGSI para el área de Informática del Instituto Nacional de Vías Territorial Nariño, se clasifica y analiza cuidadosamente para determinar riesgos, debilidades, amenazas y políticas de seguridad a implementarse a través del SGSI.

7.7.1 Metodología para el análisis y diseño. En el diseño de un Sistema de Gestión de Seguridad de la Información SGSI se debe seguir un orden de los procesos que permitan organizar las actividades para construir el sistema, de acuerdo a un conjunto de métodos y técnicas que permitan desarrollar un SGSI de calidad.

Para el desarrollo del presente proyecto se toma como guía el método denominado Ciclo PHVA, Planificar, Hacer, Verificar y Actuar. El ciclo PHVA como modelo para “implantación de SGSI, permanece en una constante revaluación, por cuanto funciona, bajo la filosofía del mejoramiento continuo; en seguridad sería la revaluación de las medidas de prevención, corrección y evaluación, manteniendo un constante ciclo que por sus características no podría terminar. A continuación, se detalla cada uno de los pasos del modelo Deming como metodología apropiada los SGSI”[24].

[24] Sistemas de Gestión de Seguridad de la Información. [en línea] disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html [citado en 10 de abril de 2016].

Planear. En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la entidad respecto a los mecanismos de seguridad implementados y la normativa ISO/IEC 27001:2013, la cual se pretende implantar para evaluación y certificación. Así mismo en la etapa de planeación se organizan fases relevantes como son:

- Establecer el compromiso con los directivos de la oficina de Planeación Organizacional de la entidad para el inicio, proceso y ejecución.
- Fase de análisis de información de la organización, en esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la entidad para el cumplimiento de su misión u objeto social.
- Fase de evaluación del riesgo, en esta fase se evalúan los riesgos, se presentan y se seleccionan los controles a implementar.

Hacer. En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de organización. También se formula y se implementa un plan de riesgo.

Verificar. Consiste en efectuar el control de todos los procedimientos implementados en el SGSI, realizando controles periódicos para asegurar la eficacia del SGSI implementado, se revisan los niveles de riesgos.

Actuar. Desarrollar mejoras a los hallazgos identificadas al SGSI y validarlas, realizar las acciones correctivas y preventivas, mantener comunicación con el personal de la organización relevante.[25]

7.8 Análisis de la encuesta realizada a los funcionarios del Instituto Nacional de Vías Territorial Nariño. Se analiza la información obtenida de la encuesta a los funcionarios de la Territorial Nariño a través de 10 preguntas que están enfocadas a evaluar los siguientes aspectos como incidentes presentados, manejo y cambio de contraseñas, medidas y políticas de seguridad adoptadas actualmente por la empresa, se puede obtener las siguientes conclusiones:

- El manejo y cambio de contraseñas no es el más adecuado, toda vez que no se cambian regularmente, y cuando se lo realiza, se lo hace de forma inadecuada.

[25] Ibíd., Sistemas de Gestión de Seguridad de la Información. [en línea] disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html [citado en 10 de abril de 2016].

- Los funcionarios manifiestan que han tenido inconvenientes al utilizar su computador como instrumento de trabajo, por varios aspectos, tales como la obsolescencia de los mismos, por lentitud, por bloqueo, por mensajes de error, inconvenientes de acceso a red, y también manifiestan no conocer políticas de seguridad concretas que se deben tener en cuenta para proteger la información.

De acuerdo a lo anterior, es necesario diseñar un Sistema de Gestión de Seguridad de la Información SGSI y con su posterior implementación que permita clasificar la información, conocer que activos son los más importantes para la entidad, realizar un análisis de riesgos, definir salvaguardas, definir responsabilidades en el manejo de la información y adoptar políticas y controles de seguridad para proteger el área de informática del Instituto Nacional de Vías Territorial Nariño.

8. SGSI PARA EL INSTITUTO NACIONAL DE VIAS TERRITORIAL NARIÑO

Teniendo en cuenta el ciclo PHVA que permite realizar una serie de pasos y procesos para la construcción de un Sistema de Gestión de Seguridad de la Información SGSI, a continuación, se procede a realizar cada una de estas fases:

8.1 ESTABLECER EL SGSI

8.1.1 Alcance. Con el fin de mejorar la calidad en la prestación de los diferentes servicios que presta el Instituto Nacional de Vías Territorial Nariño se aplica el SGSI a los procesos, recursos informáticos y tecnológicos que hacen parte del área de informática de la Territorial Nariño con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información y debe ser aplicada y cumplida por todos los funcionarios de la entidad.

8.1.2 Inventario de Activos. Las empresas deben proteger la confidencialidad, integridad y disponibilidad de la información para velar por la continuidad del negocio independientemente de su actividad social. Para proteger dicha información de riesgos y amenazas el Instituto Nacional de Vías Territorial Nariño realiza un inventario de sus activos teniendo en cuenta la metodología MAGERIT que los clasifica en los siguientes grupos.

- Activos esenciales.
- Datos o información (catalogados como fundamentales).
- Servicios.
- Las aplicaciones de software.
- Equipos informáticos.
- Personal.
- Redes de Comunicación.
- Soportes de Información.
- Equipamiento Auxiliar.
- Instalaciones.

8.1.2.1 Activos Esenciales.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[vr]	Datos vitales	[I_Juridicos]	Información de Procesos Jurídicos (base de datos y registro de procesos jurídicos)

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
		[I_Permiso]	Permiso Estación de Servicio
		[I_Normativa]	Información de Normativa (Derecho de vía)
		[I_Historia_Laboral]	Información sobre historia labora de los extrabajadores del extinto Ministerio de Obras Publicas MOPT Distrito 14.
[per]	Datos de Carácter Personal	[I_Financiera]	Obligación de cuentas
[classified]	Datos clasificados	[D_Históricos]	Datos Históricos de proyectos terminados
		[D_Proyectos]	Documentació n de proyectos en ejecución.

Fuente: El Autor

8.1.2.2 Datos/Información.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[files]	Archivos	[A_proyectos]	Archivos de proyectos
		[A_Administrador Vial]	Archivos de Administrador Vial
		[A_Microempresa]	Archivo de Microempresa
		[A_Interventor]	Archivos de Interventorías
		[A_Contratista]	Archivos de Contratistas
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos en ejecución
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de funcionarios

Fuente: El Autor

8.1.2.3 Claves criptográficas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[encrypt]	Claves de cifra	[CC_Aplicaciones_financiera]	Claves de cifra de aplicaciones financieras

Fuente: El Autor

8.1.2.4 Inventario de servicios.

Código grupo de activo MAGERITT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[ext]	A usuarios externos	[S_U_Externo]	Servicios prestados a usuarios externos
[int]	Interno (a usuarios de la propia entidad)	[S_U_Interno]	Servicios prestados a funcionarios tanto al interior como haciendo uso de internet.
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los funcionarios.
[email]	Correo electrónico	[S_correo]	Manejo de correos electrónicos

Código grupo de activo MAGERITT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[file]	Almacenamiento de archivos	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la entidad.

Fuente: El Autor

8.1.2.5 Software.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos
[Oficce]	Ofimática	[Oficce]	Office 365
[av]	Antivirus	[Antivirus]	Windows Defender original con actualizaciones automáticas.
[os]	Sistema operativo	[OS_Win7_Win8]	Sistema operativo Windows 7 y 8, en su versión professional con actualizaciones

Fuente: El Autor

8.1.2.6 Equipos Informáticos.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[PC_trabajadores]	Equipos de escritorio
[pc]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portatiles
[print]	Equipos de impresión	[E_Impresoras]	Impresoras
[router]	Enrutadores	[R_enrutadores]	Enrutadores

Fuente: El Autor

8.1.2.7 Redes de comunicaciones.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica
[LAN]	Red local	[R_Local]	Red local
[Internet]	Internet	[Internet]	Internet
[Intranet]	Intranet	[intranet]	Intranet

Fuente: El Autor

8.1.2.8 Soportes de Información _almacenamiento electrónico.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[cd]	Discos	[A_CD]	Almacenamientos en Disco
[cd]	Cederrón (CD_ROM)	[A_CD]	Almacenamiento
[USB]	Memorias	[A_Memorias]	Almacenamiento en Memorias USB
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD

Fuente: El Autor

8.1.2.9 Soportes de Información _almacenamiento no electrónico.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[printed]	Material impreso	C_Documentación_proyecto	Carpetas con la documentación de cada proyecto en ejecución

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
		C_Documentacion_juridica	Carpetas con la documentación de los procesos jurídicos
		C_Reportes_informes	Carpetas de reportes e informes
		C_Soportes-financieros	Carpetas de obligación de cuentas.
		C_varios	Carpetas varios

Fuente: El Autor

8.1.2.10 Equipamiento auxiliar.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[printed]	Sistemas de Alimentación ininterrumpida	U_Computadores	UPS computadores
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.
[Furniture]	Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.

Fuente: El Autor

8.1.2.11 Instalaciones.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[building]	Edificio	[E_entidad]	Instalacion física de la entidad

Fuente: El Autor

8.1.2.12 Personal.

Código grupo de activo MAGERI	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad
[ui]	Usuarios internos	[E_funcionario]	Funcionarios de recepción, área técnica, administrativa y archivo
[adm]	Administradores de sistemas	[A_sistemas]	Administrador de sistemas

Fuente: El Autor

8.1.3 Metodología de Evaluación del Riesgo. Se elige la metodología MAGERIT para el análisis y gestión de los de riesgos.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos normalizados, los cuales son:

"**Paso 1.** Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

Paso 2. Determinar a qué amenazas están expuestos aquellos activos.

Paso 3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

Paso 4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

Paso 5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza"[26].

8.1.4 Valoración cualitativa de los activos. Teniendo en cuenta que todos los activos no tienen la misma relevancia e importancia para la entidad, y que cada uno de estos en caso de ser atacado o sufrir un incidente genera un impacto diferente en la entidad, se procede a realizar una valoración cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo a la siguiente Tabla.

[26] Ibíd., p. 22.

Tabla 2. Criterios de Valoración

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: MAGERIT V3 libro 2 Catalogo de elementos

8.1.4.1 Valoración Cualitativa de Activos esenciales.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[vr]	Datos vitales	[I_Juridicos]	Información de Procesos Jurídicos (base de datos y registro de procesos jurídicos)	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	8
		[I_Permiso]	Permiso Estación de Servicio	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	4
				Trazabilidad	5
		[I_Normativa]	Información de Normativa (Derecho de vía)	Confiabilidad	5
				Integridad	5
				Autenticidad	5
				Disponibilidad	4
				Trazabilidad	4
		[I_Historia_Laboral]	Información sobre historia labora de los extrabajadores del extinto Ministerio de Obras Publicas	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
			MOPT Distrito 14.	Trazabilidad	8
[per]	Datos de Carácter Personal	[I_Financiera]	Obligación de cuentas	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	6
				Trazabilidad	6
[classified]	Datos clasificados	[D_Históricos]	Datos Históricos de proyectos terminados	Confiabilidad	6
				Integridad	6
				Autenticidad	7
				Disponibilidad	5
				Trazabilidad	6
		[D_Proyectos]	Documentación de proyectos en ejecución.	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	6
				Trazabilidad	6

Fuente: El Autor

8.1.4.2 Valoración Cualitativa de Datos/Información.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[files]	Archivos	[A_proyectos]	Archivos de proyectos	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	5

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
				Trazabilidad	5
		[A_Administrador Vial]	Archivos de Administrador Vial	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	5
				Trazabilidad	5
		[A_Microempresa]	Archivos de Microempresa	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5
		[A_Interventor]	Archivos de Interventorías	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	5
				Trazabilidad	5
		[A_Contratista]	Archivos de Contratistas	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	5
				Trazabilidad	5
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información	Confiabilidad	6
				Integridad	7
				Autenticidad	6

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
				Disponibilidad	4
				Trazabilidad	4
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos	Confiabilidad	6
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos en ejecución	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	6
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de funcionarios	Confiabilidad	7
				Integridad	6
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6

Fuente: El Autor

8.1.4.3 Valoración Cualitativa de Claves Criptográficas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[encrypt]	Claves de cifra	[CC_Aplicaciones_financiera]	Claves de cifra de aplicaciones	Confiabilidad	7
				Integridad	7

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
			financieras	Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6

Fuente: El Autor

8.1.4.4 Valoración cualitativa de servicios.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[ext]	A usuarios externos	[S_U_Externo]	Servicios prestados a usuarios externos	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6
[int]	Interno (a usuarios de la propia entidad)	[S_U_Interno]	Servicios prestados a funcionarios tanto al interior como haciendo uso de internet.	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los funcionarios.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6
[email]	Correo electrónico	[S_correo]	Manejo de correos electrónic os	Confiabilidad	7
				Integridad	7
				Autenticidad	7

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
				Disponibilidad	6
				Trazabilidad	6
[file]	Almacenamiento de archivos	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la entidad.	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7

Fuente: El Autor

8.1.4.5 Valoración Cualitativa de Software – Aplicaciones Informáticas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el	Confiabilidad	6
				Integridad	6
				Autenticidad	6

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
			proceso de gestión de las bases de datos manejadas al	Disponibilidad	6
				Trazabilidad	6
[Oficce]	Ofimática	[Oficce]	Office 365	Confiabilidad	5
				Integridad	5
				Autenticidad	5
				Disponibilidad	4
				Trazabilidad	5
[av]	Antivirus	[Antivirus]	Windows Defender original con actualizaciones automáticas.	Confiabilidad	7
				Integridad	5
				Autenticidad	5
				Disponibilidad	7
				Trazabilidad	5
[os]	Sistema operativo	[OS_Win7_ Win8]	Sistema operativo Windows 7 y 8, en su versión professional con actualizaciones automáticas activadas.	Confiabilidad	7
				Integridad	5
				Autenticidad	5
				Disponibilidad	5
				Trazabilidad	5

Fuente: El Autor

8.1.4.6 Valoración Cualitativa de Equipos Informáticos.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[PC_trabajadores]	Equipos de escritorio	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[pc]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portatiles	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	6
				Trazabilidad	6
[print]	Equipos de impresión	[E_Impresoras]	Impresoras	Confiabilidad	5
				Integridad	5
				Autenticidad	5
				Disponibilidad	5
				Trazabilidad	5
[router]	Enrutadores	[R_enrutadores]	Enrutadores	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	8

Fuente: El Autor

8.1.4.7 Valoración Cualitativa de Redes de comunicaciones.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	8
[LAN]	Red local	[R_Local]	Red local	Confiabilidad	8
				Integridad	8
				Autenticidad	6
				Disponibilidad	8
				Trazabilidad	6
[Internet]	Internet	[Internet]	Internet	Confiabilidad	5
				Integridad	5
				Autenticidad	5
				Disponibilidad	5
				Trazabilidad	5
[Intranet]	Intranet	[intranet]	Intranet	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	8
				Trazabilidad	7

Fuente: El Autor

8.1.4.8 Valoración Cualitativa de Soportes de Información - almacenamiento electrónico.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6
[usb]	Cederom (CD_ROM)	[A_CD]	Almacenamiento en CD	Confiabilidad	5
				Integridad	6
				Autenticidad	5
				Disponibilidad	6
				Trazabilidad	5
	Memorias	[A_Memorias]	Almacenamiento en Memorias USB	Confiabilidad	7
				Integridad	6
				Autenticidad	5
				Disponibilidad	6
				Trazabilidad	5
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD	Confiabilidad	5
				Integridad	6
				Autenticidad	5
				Disponibilidad	6
				Trazabilidad	5

Fuente: El Autor

8.1.4.9 Valoración Cualitativa de Soportes de Información _almacenamiento no electrónico.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[printed]	Material impreso	C_Documentación_proyecto	Carpetas con la documentación de cada proyecto en ejecución	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
				Trazabilidad	7
		C_Documentacion_juridica	Carpetas con la documentación de los procesos jurídicos	Confiabilidad	8
				Integridad	8
				Autenticidad	8
				Disponibilidad	8
				Trazabilidad	
		C_Reportes_informes	Carpetas de reportes e informes impresos	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	7
		C_Soportes-financieros	Carpetas de obligación de cuentas.	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	7
		C_varios	Carpetas varias	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	7

Fuente: El Autor

8.1.4.10 Valoración Cualitativa de Equipamiento auxiliar.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[ups]	Sistemas de Alimentación	U_Computadores	UPS computadores	Confiabilidad	7
				Integridad	5
				Autenticidad	5

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
	ininterrumpida			Disponibilidad	5
				Trazabilidad	5
[supply]	Suministros Esenciales	Esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.	Confiabilidad	5
				Integridad	5
				Autenticidad	5
				Disponibilidad	3
				Trazabilidad	5
[Furniture]	Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.	Confiabilidad	5
				Integridad	5
				Autenticidad	5
				Disponibilidad	3
				Trazabilidad	5

Fuente: El Autor

8.1.4.11 Valoración Cualitativa de Instalaciones.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[building]	Edificio	[E_entidad]	Instalación física de la entidad	Confiabilidad	3
				Integridad	3
				Autenticidad	3
				Disponibilidad	5
				Trazabilidad	3

Fuente: El Autor

8.1.4.12 Valoración Cualitativa de Personal.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[ui]	Usua	[E_funcionario	Funcionarios de	Confiabilidad	7

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
	rios intern os	]	recepción, área técnica, administrativa y archivo	Integridad	8
				Autenticidad	8
				Disponibilidad	6
				Trazabilidad	5
[adm]	Administrador es de sistemas	[A_sistemas]	Administrad or de sistemas	Confiabilidad	7
				Integridad	6
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6

Fuente: El Autor

8.1.5 Identificación de amenazas. Se realiza una evaluación de amenazas basado en la frecuencia de materialización de la amenaza, las dimensiones de seguridad según MAGERIT y la escala de rango porcentual de impactos en los activos.

Tabla 3: Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: Módulo de Sistemas de Gestión de Seguridad Informática, UNAD.

Tabla 4: Dimensiones de seguridad según MAGERIT

Dimensiones de Seguridad	Identificación
Autenticidad	A
Confiabilidad	C
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente: El Autor

Tabla 5*:* Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Impacto	Valor cuantitativo
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Módulo de Sistemas de Gestión de la Seguridad Informática, UNAD.

De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad.

Tabla 6. Amenazas MAGERIT

[N]	Desastres naturales	
N1	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
N2	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
N.*	Desastres naturales	Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto.
[I]	**De origen industrial**	
I1	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
I2	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
I.*	Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, etc.
I3	Contaminación mecánica	Vibraciones, polvo, suciedad,
I4	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta,

I5	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
I6	Corte del suministro eléctrico	Cese de la alimentación de potencia
I7	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,
I8	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
I9	Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante,
I10	Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo
I11	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.
		Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
[E]	**Errores y fallos no intencionados**	
E1	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
E2	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación
E3	Errores de monitorización (logs)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos,

Continuación tabla 23.

E4	Errores de configuración	Introducción de datos de configuración erróneos.
E7	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.
E8	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
E9	Errores de [re]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
E10	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.
E14	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
E15	Alteración de la información	Alteración accidental de la información.
		Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E18	Destrucción de información	Pérdida accidental de información.
		Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E19	Divulgación de información	Revelación por indiscreción.
		Incontinencia verbal, medios electrónicos, soporte papel, etc.
[E]	**Errores y fallos no intencionados**	
E20	Vulnerabilidades de los programas	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

E21	Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
E23	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
E24	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
E25	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
E28	Indisponibilidad del personal	ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica
[A]	**Ataques intencionados**	
A3	Manipulación de los registros de actividad	Registros de actividad [D.log]
A4	Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
A5	Suplantación de identidad de usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
A6	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
A7	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos

		personales, etc.
A8	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
A9	Encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
A10	Alteración de secuencia (de mensajes)	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
A11	Acceso no autorizado (aprovechando una debilidad)	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
A12	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.
A13	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.
		Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.
		Repudio de recepción: negación de haber recibido un mensaje o comunicación.
A14	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
A15	Modificación de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
A18	Destrucción la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
A19	Divulgación de información	Revelación de información.

A22	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A23	Manipulación de equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A24	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A25	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
		El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
A26	Ataque destructivo	vandalismo, terrorismo, acción militar,
A27	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
A28	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos
A29	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
A30	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero

8.1.6 Inspección visual de los activos de información. En la visita a las instalaciones físicas de la entidad, captando en fotografías las vulnerabilidades encontradas.

- **Inspección visual a la sala de comunicaciones.** En las siguientes imágenes se puede apreciar los equipos en la sala de comunicaciones.

Figura 8. Rack de comunicaciones, UPS y tablero de control

Fuente. El Autor

La entrada a la sala de comunicaciones carece de una cámara de seguridad dirigida a esta, el control de acceso de personal es brindado por una chapa común con llave, siendo el único con acceso autorizado a esta zona por el Director Territorial, le empresa de seguridad contratada por el Instituto posee la llave para acceder a la sala de comunicaciones, pero esta es fácilmente transferibles a otras personas, a pesar de que se cuenta con control de acceso adecuado, no se cuenta con una sistema o un control que verifique que esas las personas que acceden a esta zona son las autorizadas, como lo es un sistema de cerradura biométrico.

En las anteriores imágenes se evidencia que existe orden en la parte de cableado sobre todo en el rack de comunicaciones donde la mayoría de cables se encuentran etiquetados al igual que los switch ahí presentes, también se rescata que el cableado eléctrico va por separado del cableado de datos evitando interferencia electromagnética en esta.

El panel eléctrico cuenta con su puerta de seguridad y un mensaje pequeño de alerta alto voltaje. En la sala de comunicaciones no se evidencia la existencia de un extintor especializado para equipos de cómputo en caso de incendio.

La sala de servidores carece de dispositivos de control de ambiente, no posee alarmas de humo, ni aire acondicionado, ni vaporizador, impidiendo el control de las variables ambientales de temperatura, gases y humedad.

- **Inspección visual a la oficina del Departamento Técnico.** En las siguientes imágenes se observa el estado y distribución del Departamento Técnico.

Figura 9. Puestos de trabajo Departamento Técnico

Fuente. El Autor

Figura 10. Puestos de trabajo Departamento Técnico

Fuente. El Autor

En las anteriores imágenes se puede apreciar algunos puestos de trabajo de los funcionarios que trabajan en el área técnica. Se observa que cuentan con un limitado espacio libre.

Los Ingenieros cuentan con computadores de escritorio que trabajan como estaciones, algunos de ellos son equipos antiguos repotenciados, también se observa la disposición desordenada de cableado de alimentación eléctrica, y de comunicaciones. En estas áreas se cuenta con cableado estructurado y alimentación eléctrica regulada. Cada uno de los ingenieros posee llave de la oficina en donde existen varios puestos de trabajo, a esta zona de trabajo también tiene acceso el personal de la empresa de aseo, una llave la maneja la empresa de vigilancia privada, pero realmente no se tiene un control del acceso del personal que ingresa a estas oficinas.

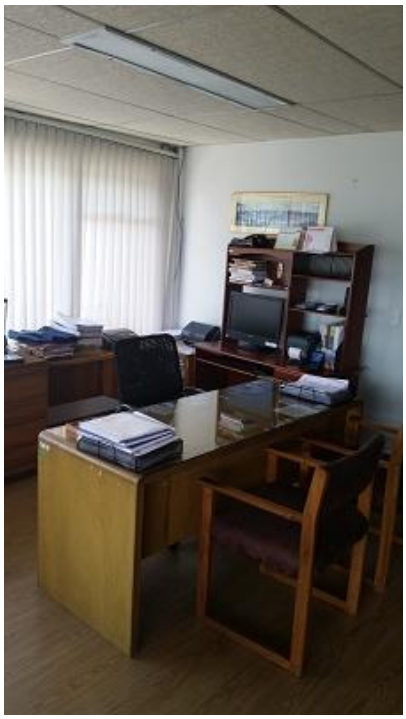
- **Inspección visual a la oficina del Director Territorial.** En las siguientes imágenes se observa el estado y distribución de la oficina de la dirección territorial.

Figura 11. Puesto de trabajo oficina del Director Territorial

Fuente. El Autor

La estación de trabajo del Director Territorial es un computador todo en uno nuevo, es importante aclarar que la configuración de todas las estaciones de trabajo de la territorial es la misma, y básicamente se compone del sistema operativo Windows 10 u 8, Office 365, aplicativos en red tales como SICOR (sistema de correspondencia), SICO (sistema de gestión de contratación), KACTUS (recursos humanos y nómina), SIPLAN (siatema de planeación), y utilidades como compresor, lector archivos pdf, entre otros, la estación de trabajo del director cuenta con una UPS, red electrica regulada, telefonía IP.

Figura 12. Puesto de trabajo oficina secretaria ejecutiva del Director Territorial



Fuente. El Autor

La estación de trabajo de la secretaria ejecutiva es un computador todo en uno nuevo, con la configuración básicamente se compone del sistema operativo Windows 10 u 8, Office 365, aplicativos en red tales como SICOR (sistema de correspondencia), KACTUS (recursos humanos y nómina), y utilidades como compresor, lector archivos pdf, entre otros, este puesto de trabajp cuenta con una UPS, red electrica regulada, telefonía IP, escaner, impresora para radicación de correspondencia.

- **Inspección visual a la oficina jurídica.** En las siguientes imágenes se observa el estado y distribución de la oficina jurídica.

Figura 13. Puestos de trabajo Oficina Jurídica

Fuente. El Autor

Las estaciones de trabajo de la oficina jurídica la componenen computadores de más de cinco años de antigüedad, los cuales han sido repotenciados, tienen instalado la configuración básica, no tiene UPS, si estabilizadores de voltaje conectados a la red electrica regulada, a esta ofina tiene acceso el personal de aseo y el de vigilancia.

Figura 14. Impresoras y Escaners en red

Fuente. El Autor

Las impresoras y escaners estan en red con todas las estaciones de trabajo de la territorial, el mantenimiento preventivo es mínimo y se depende mucho de los insumos para su correcto funcionamiento los cuales son enviados desde Planta Central del Instituto en Bogotá, tienen su correspondiente estabilizador de voltaje, al sitio donde se ubican estos elementos tiene acceso el personal de aseo y el público en general toda vez que se ubican en las sala de recepción adjunto al puesto de trabajo de la secretaria ejecutiva.

- **Inspección visual de los archivos documentales.** En las siguientes imágenes se observa el estado y distribución de los archivos documentales en las diferentes oficinas..

Figura 15. Archivo documental de la oficina jurídica

Fuente. El Autor

En la oficina jurídica se encuentra el archivo temporal de los proceso en curso, estos se encuentran organizados y foliados, pero presentan vulnerabilidad toda vez que a esta oficina tiene acceso el personal de aseo, el de vigilancia y sobre todo que no se lleva un control de acceso de las personas que ingresan a esta oficina en horas no hábiles. Es de aclarar que en la edificación adjunta a la sede lse encuentra el archivo de la territorial, la cual tiene un nivel de control alto, toda vez que la llave de ingreso solamente la manejan la funcionaria encargada del archivo y el personal de vigilancia, en este archivo se aplican todos los procedimientos y normas de la gestión documental, mientras los archivos permanecen en la territorial antes de ser remitidos al archivo central del institito en

Bogotá. La gestión documental de los archivos historicos si se llevan de acuerdo a la legislación documental de acuerdo a las tablas de retención documental TRD.

Figura 16. Archivo documental oficina de la dirección

Fuente. El Autor

En la oficina del director territorial se encuentra el archivo temporal de los informes de los últimos tres meses de los proyectos en ejecución que estan bajo su supervisión, presentan vulnerabilidad toda vez que a esta oficina tiene acceso el personal de aseo, el de vigilancia y sobre todo que no se lleva un control de acceso de las personas que ingresan a esta oficina en horas no hábiles. Los archivos temporales una vez que no se necesitan en la oficina del director territorial se trasladan a la oficina de archivo en donde se realizad la gestión documental aplicando la legislación vigente.

Figura 17. Archivo documental oficinas departamento técnico

Fuente. El Autor

En la oficina técnica que ocupan los ingenieros supervisores se encuentra el archivo temporal de los informes de los últimos tres meses de los proyectos en ejecución que estan bajo su supervisión, presentan vulnerabilidad toda vez que a esta oficina tiene acceso el personal de aseo, el de vigilancia y sobre todo que no se lleva un control de acceso de las personas que ingresan a esta oficina en horas no hábiles. Los archivos temporales una vez que no se necesitan en la oficina de los ingenieros se trasladan a la oficina de archivo en donde se realizad la gestión documental aplicando la legislación vigente.

Figura 18. Extintor contra incendios primer piso

Fuente. El Autor

En el primer piso se encuentra el extintor contra incendios, y la camilla de primeros auxilios con la señaletica correspondiente, el extintor se recarga permanentemente de acuerdo a las recomendaciones del Comité Paritario de Seguridad y Salud en el Trabajo COPASST.

Figura 19. Extintor contra incendios segundo piso

Fuente. El Autor

En el segundo piso se encuentra el extintor contra incendios con la señaletica correspondiente, el cual se recarga permanentemente, de acuerdo a las recomendaciones del Comité Paritario de Seguridad y Salud en el Trabajo COPASST.

Figura 20. Tablero eléctrico primer piso

Fuente. El Autor

Los tableros eléctricos cuentan con la señaletica correspondiente, en el año 2015 en la territorial se ejecutó un contrato para la reposición de las redes electricas a la Norma RETIE, toda vez que estas instalaciones datan de 1984, además, la plataforma informática dispone de una red regulada con su respectiva malla a tierra.

8.1.7 Ethical hacking y análisis de vulnerabilidades. Se realizó un proceso denominado ethical hacking con el fin de encontrar vulnerabilidades en cuanto a configuración y administración de los activos de información relacionadas a la parte lógica como lo es el software y las aplicaciones web, este proceso se realizó con el aplicativo Kali Linux, la cual fue creado con el fin de integrar herramientas que permitan realizar auditorías informáticas. Es importante aclarar que la entidad no permite la realización del test de penetración o pentesting, tales como el escaneo de vulnerabilidades, la explotación y la post-explotación.

Para realizar el proceso de ethical hacking se utilizaron las herramientas dimitry, para recolección de información del servicio DNS, zenmap, la interfaz gráfica de nmap, la herramienta por preferencia para realizar escaneo de vulnerabilidades a servidores, y subgraph vega, una de las mejores herramientas para escaneo de vulnerabilidades en las aplicaciones web.

8.1.7.1 Recolección de información con dmitry. Para obtener todos los subdominios relacionados al dominio invias.gov.co se realizó una exploración minuciosa de la página institucional y se utilizó herramienta dmitry, esta es una herramienta que permite obtener toda la información posible sobre un host, esta incluye lo relacionado con los servidores DNS incluyendo nombre de la empresa a la que está registrado el dominio, el nombre las personas encargadas de este host, los correos electrónicos de las mismas y los subdominios asociados y sus respectivas direcciones IP.

Es importante aclarar que no se procedió a efectuar pruebas a cada uno del host con el fin de identificar vulnerabilidades que pueden ser explotadas para alterar la información de alguna manera, toda vez que la entidad no permite este tipo de pruebas.

8.1.7.2 Pruebas a los portales web con la herramienta Subgrap Vega

Subgraph Vega es una herramienta utilizada para escaneo de vulnerabilidades de aplicaciones web, la cual hace un barrido completo de todos los directorios que integran a una aplicación web específica, Subgraph Vega es una herramienta utilizada para escaneo de vulnerabilidades de aplicaciones web, la cual hace un barrido completo de todos los directorios que integran a una aplicación web específica, arrojando un reporte donde las vulnerabilidades son agrupadas en distintos niveles según la gravedad de las mismas, esta clasificación puede ser alta, media, baja e información, para efectos de este trabajo, por políticas internas de la entidad no se publican los resultados.

El portal web www.invias.gov.co es el portal institucional donde se encuentra información relacionada a la entidad y sirve como plataforma de re direccionamiento hacia los otros portales y aplicaciones web que utiliza la institución. Este portal puede apreciarse en la siguiente imagen.

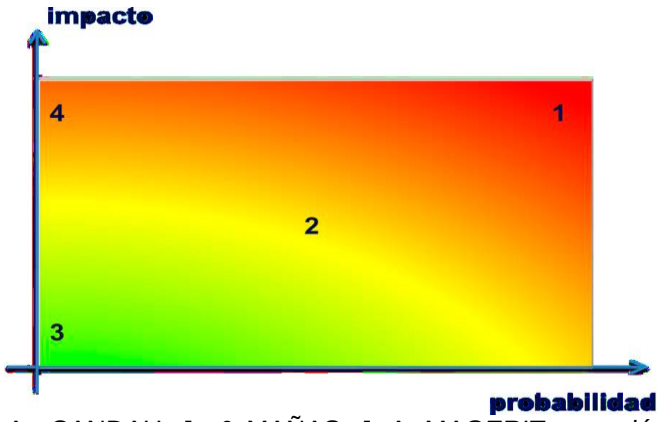
Figura 21. Página Web del Invías

Fuente. www.invias.gov.co

Este portal fue sometido a las pruebas con la herramienta Subgraph Vega, para efectos de este trabajo, por políticas internas de la entidad no se publican los resultados, pero se pudo observar que en general que es un sitio web muy estable.

8.1.8 Identificación de riesgos. El riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. El riesgo crece con el impacto y con la probabilidad como se muestra en la siguiente ilustración:

Figura 22. Zonas de riesgos



Fuente. AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 30.

Donde las zonas identifican lo siguiente:[27]

Zona 1: Riesgos muy probables y de muy alto impacto (MA: Críticos).

Zona 2: Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables, pero de impacto bajo o muy bajo (M: Apreciables).

Zona 3: Riesgos improbables y de bajo impacto (MB, B: Despreciables o Bajos).

Zona 4: Riesgos improbables, pero de muy alto impacto (A: Importantes).

Por otra parte, se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas:

[27] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 30.

Tabla 7. Estimación cualitativa del riesgo

escala		
impacto	**probabilidad**	**riesgo**
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 7.

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

Tabla 8: Tabla combinada para la estimación cualitativa del riesgo.

riesgo		**probabilidad**				
		MB	**B**	**M**	**A**	**MA**
impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 7.

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[HW] equipos informáticos.											
[N.1] Fuego	B				MA					MA	
[N.2] Daños por agua	MB				A					M	
[N.7] Desastres naturales. Fenómeno sísmico.	MB				A					M	
[N.8] Desastres naturales. Fenómeno de origen volcánico.	B				MA					MA	
[I.2] Daños por agua	B				A					A	
[I.3] Contaminación mecánica.	B				A					A	
[I.4] Contaminación electromagnética.	M				A					A	
[I.5] Avería de origen físico o lógico.	M				MA					MA	
[I.6] Corte del suministro eléctrico.	M				MA					MA	
[I.7] Condiciones inadecuadas de temperatura o humedad.	M				MA					MA	
[E.23] Errores de mantenimiento / actualización de equipos (hardware).	B				A					A	
[E.24] Caída del sistema por agotamiento de recursos.	B				MA					MA	
[E.25] Pérdida de equipos-Robo.	MB		A		MA			M		A	
[A.6] Abuso de privilegios de acceso.	M		A	A	A			A	A	A	
[A.7] Uso no previsto.	M		A	A	A			A	A	A	
[A.11] Acceso no autorizado.	B		A	B				A	B		
[A.23] Manipulación de los equipos.	M		A		MA			A		MA	
A.24] Denegación de servicio.	MB				A					M	
[A.25] Robo.	MB		A		MA			M		A	

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	Probabilidad	IMPACTO para cada dimensión					RIESGO para cada dimensión				
		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[A.26] Ataque destructivo.	MB				MA					A	
[Media] soportes de información. CD-DVD-HD											
[N.1] Fuego	B				MA					MA	
[N.2] Daños por agua	MB				A					M	
[N.7] Desastres naturales. Fenómeno sísmico.	MB				A					M	
[N.8] Desastres naturales. Fenómeno de origen volcánico.	B				MA					MA	
[I.2] Daños por agua	B				A					A	
[I.3] Contaminación mecánica.	B				A					A	
[I.5] Avería de origen físico o lógico.	M				MA					MA	
[I.6] Corte del suministro eléctrico.	M				MA					MA	
[I.10] Degradación de los soportes de almacenamiento de la información.	MB				MB					MB	
[E.1] Errores de los usuarios.	B		M	M	M			M	M	M	
[E.18] Destrucción de información.	MB				B					MB	
[E.19] Fugas de información.	B		A					A			
[E.25] Pérdida de equipos-Robo.	MB		M		MA			B		A	
[A.7] Uso no previsto.	MB		M	M	M			B	B	B	
[A.11] Acceso no autorizado.	MB		B	B				MB	MB		
[A.18] Destrucción de información.	MB				A					M	
[A.19] Revelación de información.	MB		M					B			
[A.23] Manipulación de los equipos.	MB		B		B			MB		MB	
[A.25] Robo.	MB		A		B			M		MB	

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[A.26] Ataque destructivo.	MB				M					B	
[AUX] equipamiento auxiliar.											
[N.1] Fuego	MB				M					B	
[N.2] Daños por agua	MB				M					B	
[N.7] Desastres naturales. Fenómeno sísmico.	MB				M					B	
[N.8] Desastres naturales. Fenómeno de origen volcánico.	MB				M					B	
[I.2] Daños por agua	MB				M					B	
[I.3] Contaminación mecánica.	MB				B					MB	
[I.5] Avería de origen físico o lógico.	MB				B					MB	
[I.6] Corte del suministro eléctrico.	MB				MB					MB	
[I.9] Interrupción de otros servicios y suministros esenciales.	MB				MB					MB	
[E.23] Errores de mantenimiento / actualización de equipos (hardware).	B				A					A	
[E.25] Pérdida de equipos-Robo.	MB		M		MA			B		A	
[A.7] Uso no previsto.	MB		M	M	M			B	B	B	
[A.11] Acceso no autorizado.	MB		MB	MB				MB	MB		
[A.23] Manipulación de los equipos.	MB		MB		MB			MB		MB	
[A.25] Robo.	MB		A		B			M		MB	
[A.26] Ataque destructivo.	MB				M					B	
[L] instalaciones											
[N.1] Fuego	MB				M					B	
[N.2] Daños por agua	MB				M					B	
[N.7] Desastres naturales. Fenómeno sísmico.	B				MA					MA	
[N.8] Desastres naturales. Fenómeno de origen	B				MA					MA	

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
volcánico.											
[I.2] Daños por agua	MB				M					B	
[A.7] Uso no previsto.	MB		M	B	B			B	MB	MB	
[A.11] Acceso no autorizado.	MB		MB	MB				MB	MB		
[A.26] Ataque destructivo.	MB				A					M	
[SW] aplicaciones. Software.											
[I.5] Avería de origen físico o lógico.	M				M					M	
[E.2] Errores del administrador.	MB		M	M	M			B	B	B	
[E.8] Difusión de software dañino.	MB		M	M	A			B	B	M	
[E.9] Errores de reencaminamiento.	MB		B					MB			
[E.18] Destrucción de información.	MB				M					B	
[E.19] Fugas de información.	B		M					M			
[A.5] Suplantación de la identidad del usuario.	B	M	M	M			M	M	M		
[A.6] Abuso de privilegios de acceso.	B		M	M	M			M	M	M	
[A.7] Uso no previsto.	B		A	A	A			A	A	A	
[A.8] Difusión de software dañino.	MB		B	B	B			MB	MB	MB	
[A.11] Acceso no autorizado.	B		A	M				A	M		
[A.15] Modificación deliberada de la información.	MB			A					M		
[A.18] Destrucción de información.	MB				M					B	
[A.22] Manipulación.	MB		M	M	M			B	B	B	
[SW] aplicaciones. Servidor de aplicaciones.											
[E.1] Errores de los usuarios.	MB		B	B	B			MB	MB	MB	

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	Probabilidad	IMPACTO para cada dimensión					RIESGO para cada dimensión				
		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[E.20] Vulnerabilidades de los programas (software).	MB		M	M	B			B	B	MB	
[E.21] Errores de mantenimiento / actualización de programas (software).	MB			B	M				MB	B	
[SW] aplicaciones. Sistema Operativo.											
[E.1] Errores de los usuarios.	B		M	B	M			M	B	M	
[E.20] Vulnerabilidades de los programas (software)	B		M	B	M			M	B	M	
[E.21] Errores de mantenimiento / actualización de programas (software).	B			M	M				M	M	
[SW] aplicaciones. Antivirus.											
[E.1] Errores de los usuarios.	MB		M	B	M			B	MB	B	
[E.20] Vulnerabilidades de los programas (software).	MB		M	B	M			B	MB	B	
[E.21] Errores de mantenimiento / actualización de programas (software).	B			MB	B				MB	B	
[SW] aplicaciones. Sistema de Gestión de Bases de Datos.											
[E.1] Errores de los usuarios.	MB		B	B	B			MB	MB	MB	
[E.20] Vulnerabilidades de los programas (software).	B		M	B	M			M	B	M	
[E.21] Errores de mantenimiento / actualización de programas (software).	B			B	M				B	M	
[SW] aplicaciones. Ofimática.											
[E.1] Errores de los usuarios.	MB		B	B	B			MB	MB	MB	

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[E.20] Vulnerabilidades de los programas (software).	MB		MB	MB	MB			MB	MB	MB	
[E.21] Errores de mantenimiento / actualización de programas (software).	B			MB	B				MB	B	
[COM] redes de comunicaciones.											
[I.8] Fallo de servicios de comunicaciones.	M				MA					MA	
[E.2] Errores del administrador.	B		MA	A	A			MA	A	A	
[E.9] Errores de reencaminamiento.	MB		B					MB			
[E.24] Caída del sistema por agotamiento de recursos.	MB				MA					A	
[A.5] Suplantación de la identidad del usuario.	B	M	M	M			M	M	M		
[A.6] Abuso de privilegios de acceso.	B		A	A	A			A	A	A	
[A.7] Uso no previsto.	B		A	A	A			A	A	A	
[A.11] Acceso no autorizado.	B		A	B				A	B		
[A.14] Interceptación de información (escucha).	MB		A					M			
A.24] Denegación de servicio.	MB				A					M	
[S] servicios. E-mail, internet											
[E.1] Errores de los usuarios.	B		A	M	M			A	M	M	
[E.2] Errores del administrador.	MB		A	M	A			M	B	M	
[E.9] Errores de reencaminamiento.	MB		B					MB			
[E.19] Fugas de información.	B		A					A			
[E.24] Caída del sistema por agotamiento de	MB				MA					A	

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
recursos.											
[A.5] Suplantación de la identidad del usuario.	B	A	A	A			A	A	A		
[A.6] Abuso de privilegios de acceso.	MB		M	M	A			B	B	M	
[A.7] Uso no previsto.	MB		A	A	A			M	M	M	
[A.11] Acceso no autorizado.	MB		A	M				B	M		
[A.13] Repudio.	MB			M		A			B		M
[A.15] Modificación deliberada de la información.	MB			A					M		
[A.18] Destrucción de información.	MB				MA					A	
[A.19] Revelación de información.	MB		M					B			
[A.24] Denegación de servicio¨.	MB				A					M	
[D] datos / información. Archivos de Contratistas.											
[E.1] Errores de los usuarios.	B		M	MA	M			M	MA	M	
[D] datos / información. Archivos de Informes Jurídicos.											
[E.1] Errores de los usuarios.	B		MA	MA	M			MA	MA	M	
[D] datos / información. Archivo de Copias de seguridad de la información.											
[E.1] Errores de los usuarios.	MB		MA	MA	M			A	A	B	
[D] datos / información. Archivos de viabilidad Estaciones de servicio											
[E.1] Errores de los usuarios.	MB		MA	MA	M			A	A	B	
[D] datos / información.											

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Contraseñas de acceso de funcionarios.											
[E.1] Errores de los usuarios.	MB		M	M	M			B	B	B	
[D] datos / información.											
[E.2] Errores del administrador.	M		MA	A	M			MA	A	M	
[E.15] Alteración accidental de la información.	B			MA					MA		
[E.18] Destrucción de información.	B				M					M	
[E.19] Fugas de información.	B		A					A			
[A.5] Suplantación de la identidad del usuario.	B	MA	MA	MA			MA	MA	MA		
[A.6] Abuso de privilegios de acceso.	MB		A	MA	MA			M	A	A	
[A.11] Acceso no autorizado.	B		MA	A				MA	A		
[A.15] Modificación deliberada de la información.	MB			A					M		
[A.18] Destrucción de información.	MB			MA					A		
[A.19] Revelación de información.	B		MA					MA			
[keys] claves criptográficas.											
[E.1] Errores de los usuarios.	B		MA	MA	MA			MA	MA	MA	
[E.2] Errores del administrador.	M		MA	A	M			MA	A	M	
[E.19] Fugas de información.	MB		A					A			
[A.5] Suplantación de la identidad del usuario.	B	MA	A	A			MA	A	A		
[A.6] Abuso de privilegios de acceso.	MB		A	M	MB			M	B	MB	
[A.11] Acceso no	MB		M	A				B	M		

Relación de amenazas por activo identificando su probabilidad, impacto y riesgo											
Activo/Amenaza	**Probabilidad**	**IMPACTO para cada dimensión**					**RIESGO para cada dimensión**				
		[A]	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
autorizado.											
[A.15] Modificación deliberada de la información.	MB			A					M		
[A.18] Destrucción de información.	MB				A					M	
[A.19] Revelación de información.	MB		MA					A			
[Media] soportes electrónicos.											
[E.23] Errores de mantenimiento / actualización de equipos (hardware).	B				A					A	
[Media] soportes de información. Almacenamiento no electrónico.											
[E.1] Errores de los usuarios.	B		M	M	M			M	M	M	
[P] personal interno.											
[E.7] Deficiencias en la organización.	M				A					A	
[E.19] Fugas de información.	B		A					A			
[E.28] Indisponibilidad del personal No intencionado.	B				A					A	
[A.28] Indisponibilidad Intencionada.	B				A					A	
[A.29] Extorsión.	MB		A	A	A			M	M	M	
[A.30] Ingeniería	MB		A	A	A			M	M	M	
[D.log] registros de actividad.											
[E.3] Errores de monitorización (log).	MB			MA					A		
[D.conf] datos de configuración.											
[E.4] Errores de configuración.	MB			MA					A		

8.1.9 Salvaguardas. "Los Controles de Seguridad o Salvaguardas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, donde se deben establecer los controles para cada amenaza de cada activo"[28].

Las salvaguardas son medidas, rutinas o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se solucionan simplemente organizándose, otras en cambio demandan elementos técnicos, otras, seguridad física y finalmente otras solicitan políticas orientada a las personas. Es importante identificar las salvaguardas existentes que tengan los activos y sistemas de información, para establecer su nivel de eficacia y de esta manera plantear nuevas salvaguardas, eliminarlas o mantener las que están cumpliendo con los respectivos criterios de seguridad.
"Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definen las salvaguardas que son procedimiento tecnológico que reduce el riesgo, de acuerdo a los activos que se van proteger, en este caso se tiene en cuenta las salvaguardas definidas en MAGERIT"[29].

Tipo de protección. Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] prevención. Una salvaguarda es preventiva, cuando reduce las oportunidades de que un incidente ocurra, si el incidente llega a suceder, los daños son los mismos.[30]

[DR] disuasión. Una salvaguarda es disuasoria, cuando los atacantes no se atreven o lo piensan muy bien antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; no tienen influencia sobre los daños causados cuando estos suceden.[31]

[EL] eliminación. Una salvaguarda elimina un incidente cuando impide que éste suceda, actúan antes de que el incidente se haya producido. No reducen los daños en caso de que la salvaguarda no sea perfecta y el incidente llegue a suceder.[32]

---

[28] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 53-57.
[29] Ibíd., p. 59.
[30] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 32
[31] Ibíd., p. 32.
[32] Ibíd., p. 32.

[IM] minimización del impacto / limitación del impacto. Una salvaguarda minimiza o limita el impacto cuando delimita las consecuencias de un incidente.[33]

[CR] corrección. Una salvaguarda es correctiva, cuando repara el daño una vez producido, actúan después de que el incidente se haya producido y por tanto minimizan los daños.[34]

[RC] recuperación. Una salvaguarda ofrece recuperación, cuando regresa al incidente al estado anterior, no reducen las probabilidades del incidente, pero limitan los daños a un periodo de tiempo.[35]

[MN] monitorización. Son salvaguardas que monitorizan lo que está sucediendo o lo que ha sucedido. Si se detectan eventos en tiempo real, podemos reaccionar deteniendo el incidente para limitar el impacto; si se detectan eventos posteriormente, se puede aprender del incidente y optimizar el sistema de salvaguardas.[36]

[DC] detección. Una salvaguarda funciona detectando un ataque, informando que el evento está sucediendo. Aunque no lo frena, sí permite que entren en operación otras medidas que detengan el ataque, minimizando los daños.[37]

[AW] concienciación. Son las actividades de formación de los usuarios del sistema que influyen sobre él. La formación reduce las omisiones de los usuarios, lo cual tiene un efecto preventivo. Mejora las salvaguardas de todo tipo, toda vez que los usuarios las operan lo hacen con eficacia y rapidez, fortaleciendo su efecto.[38]

[AD] administración. "Son las salvaguardas relacionadas con la seguridad del sistema. Una administración adecuada, evita la impericia, e impide que haya accesos al sistema por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo"[39]

La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

[33] Ibíd., p. 33.
[34] Ibíd., p. 33.
[35] Ibíd., p. 33.
[36] Ibíd., p. 33.
[37] Ibíd., p. 33.
[38] Ibíd., p. 33.
[39] Ibíd., p. 33.

Tabla 9. Tipos de salvaguardas según MAGERIT.

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas
	[DR] disuasorias
	[EL] eliminatorias
Acotan la degradación	[IM] minimizadoras
	[CR] correctivas
	[RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

Fuente: MAGERIT. V 3.0 Libro 1

8.1.9.1 Salvaguardas de Activos esenciales.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[vr]	Datos vitales	[I_Juridicos]	Información de Procesos Jurídicos (base de datos y registro de procesos jurídicos)	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
		[I_Permiso]	Permiso Estación de Servicio	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
		[I_Normativa]	Información de Normativa (Derecho de vía)	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
		[I_Historia_Laboral]	Información sobre historia labora de los extrabajadore	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
			s del extinto Ministerio de Obras Publicas MOPT Distrito 14.	Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[per]	Datos de Carácter Personal	[I_Financiera]	Obligación de cuentas	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
[classified]	Datos clasificados	[D_Históricos]	Datos Históricos de proyectos terminados	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
		[D_Proyectos]	Documentación de proyectos en ejecución.	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información

Fuente: El Autor

8.1.9.2 Salvaguardas de Datos/Información.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[files]	Archivos	[A_proyectos]	Archivos de proyectos	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Eliminación (EL)	Gestión de contraseñas
		[A_Administrador Vial]	Archivos de Administrador Vial	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
		[A_Microempresa]	Archivos de Microempresa de mantenimioento rutinario de vías	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
		[A_Interventor]	Archivos de Interventorías	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
		[A_Contratista]	Archivos de Contratistas	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Eliminación (EL)	Gestión de contraseñas
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
[int]	Datos de gestión interna	[D_Gestion Proyectos]	Datos de Gestión de proyectos en ejecución	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad
				Concienciación	Capacitación al personal,
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de funcionarios	Preventivas(PR)	Políticas de seguridad, personal que tiene acceso información
				Recuperación (RC)	Copias de Seguridad

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas

Fuente: El Autor

8.1.9.3 Salvaguardas de Claves Criptográficas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[encrypt]	Claves de cifra	[CC_Aplicaciones_financiera]	Claves de cifra de aplicaciones financieras	Preventivas(PR)	Clasificación y Encriptación de la información.
				Minimización (IM)	Detención del servicio en caso de
				Correctivas(CR)	Gestión de incidentes
				Monitorización (MN)	Registro de descarga
				Detección (DC)	IDS y Firewall activos, escaneo, manejo de antivirus

Fuente: El Autor

8.1.9.4 Salvaguardas de Servicios.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[ext]	A usuarios externos	[S_U_Externo]	Servicios prestados a usuarios externos	Preventivas (PR)	Clasificación Información confidencial. Políticas
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[int]	Interno (a usuarios de la propia entidad)	[S_U_Interno]	Servicios prestados a funcionarios tanto al interior como haciendo uso de internet.	Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los funcionarios.	Monitorización (MN)	Registro de descarga
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Recuperación (RC)	Copias de Seguridad

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[email]	Correo electrónico	[S_correo]	Manejo de correos electrónicos	Monitorización (MN)	Registro de descarga
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[file]	Almacenamiento de archivos	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	Monitorización (MN)	Registro de descarga
				Preventivas (PR)	Clasificación Información confidencial.
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al	Preventivas (PR)	Clasificación Información confidencial.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
			rol dentro de la entidad.	Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Eliminación (EL)	Gestión de contraseñas

Fuente: El Autor

8.1.9.5 Salvaguardas de Software – Aplicaciones Informáticas

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones	Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal, en manejo información.
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al	Detección (DC)	IDS y Firewall activos, escaneo, manejo de antivirus
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
			interior de la empresa.	Concienciación (AW)	Capacitación al personal, en manejo información.
				Monitorización (MN)	Registro de descarga
				Eliminación (EL)	Gestión de contraseñas
[Oficce]	Ofimática	[Oficce]	Office 365	Concienciación (AW)	Capacitación al personal, en manejo información.
				Monitorización (MN)	Registro de descarga
				Eliminación (EL)	Gestión de contraseñas
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
[av]	Antivirus	[Antivirus]	Windows Defender original con actualizaciones automática	Concienciación (AW)	Capacitación al personal, en manejo información.
				Monitorización (MN)	Registro de descarga
				Eliminación (EL)	Gestión de contraseñas
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
[os]	Sistema operativo	[OS_Win7_Win8]	Sistema operativo Windows 7 y 8, en su	Concienciación (AW)	Capacitación al personal, en manejo información.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
			versión professional con actualizaciones automáticas activadas.	Monitorización (MN)	Registro de descarga
				Eliminación (EL)	Gestión de contraseñas
				Preventivas (PR)	Clasificación Información confidencial.

Fuente: El Autor

8.1.9.6 Salvaguardas de Equipos Informáticos.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[PC_trabajadores]	Equipos de escritorio	Detección (DC)	IDS y Firewall activos, escaneo, manejo de antivirus
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Recuperación (RC)	Copias de Seguridad
				Eliminación (EL)	Gestión de contraseñas
				Correctivas (CR)	Gestión de incidentes
[pc]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portatiles	Detección (DC)	IDS y Firewall activos, escaneo, manejo de antivirus

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Preventivas (PR)	Clasificación Información confidencial.
				Concienciación (AW)	Capacitación al personal, en manejo información.
				Recuperación (RC)	Copias de Seguridad
				Eliminación (EL)	Gestión de contraseñas
				Correctivas (CR)	Gestión de incidentes
[print]	Equipos de impresió n	[E_Impreso ras]	Impresoras	Preventivas(PR)	Políticas de seguridad.
				Correctivas(CR)	Gestión de incidentes
[router]	Enrutad ores	[R_enrutad ores]	Enrutadores	Monitorización (MN)	Registro de descarga
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Detección (DC)	IDS y Firewall activos, escaneo, manejo de antivirus

Fuente: El Autor

8.1.9.7 Salvaguardas de comunicaciones.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
[LAN]	Red local	[R_Local]	Red local	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
[Internet]	Internet	[Internet]	Internet	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
[Intranet]	Intranet	[intranet]	Intranet	Disuasión (DR)	Guardias de seguridad

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Preventivas (PR)	Clasificación Información confidencial.
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes

8.1.9.8 Salvaguardas de Soportes de Información _almacenamiento electrónico

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
[usb]	Cederrom (CD_ROM)	[A_CD]	Almacenamiento en CD	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
	Memorias	[A_Memorias]	Almacenamiento en Memorias USB	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes

Fuente: El Autor

8.1.9.9 Salvaguardas de Soportes de Información _almacenamiento no electrónico

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[printed]	Material impreso	C_Documentación_proyecto	Carpetas con la documentación de cada proyecto en ejecución	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
		C_Documentacion_juridica	Carpetas con la documentación de los procesos jurídicos	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
		C_Reportes_informes	Carpetas de reportes e informes impresos	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
		C_Soportes-financieros	Carpetas de obligación de cuentas.	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
		C_varios	Carpetas varias	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes

Fuente: El Autor

8.1.9.10 Salvaguardas de Equipamiento auxiliar.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[ups]	Sistemas de Aliment	U_Computadores	UPS computadores	Disuasión (DR)	Guardias de seguridad

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
	ación ininterrumpida			Preventivas (PR)	Clasificación Información confidencial. Políticas de seguridad.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes
[supply]	Suministros Esenciales	Esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial.
				Administrativas (AD)	Políticas y Normas de Seguridad
				Correctivas(CR)	Gestión de incidentes
[Furniture]	Mobiliario	M_Mobiliario	Mobiliario Estantes, armarios, escritorios, archivadores, etc.	Disuasión (DR)	Guardias de seguridad
				Preventivas (PR)	Clasificación Información confidencial.
				Administrativas (AD)	Políticas y Normas de Seguridad Información
				Correctivas(CR)	Gestión de incidentes

Fuente: El Autor

8.1.9.11 Salvaguardas de Instalaciones.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda

[building]	Edificio	[E_entidad]	Instalacion física de la entidad	Disuasión (DR)	Guardias de seguridad
				Detección (DC)	Detección de Incendios

8.1.9.12 Salvaguardas – Personal.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Tipo de Protección	Desarrollo Salvaguarda
[ui]	Usuarios internos	[E_funcionario]	Funcionarios de recepción, área técnica, administrativa y archivo	Administrativas (AD)	Políticas y Normas de Seguridad Información
				Concienciación (AW)	Capacitación al personal, en manejo información.
[adm]	Administradores de sistemas	[A_sistemas]	Administrador de sistemas	Administrativas (AD)	Políticas y Normas de Seguridad Información
				Concienciación (AW)	Capacitación al personal, en manejo información.

Fuente: El Autor

8.1.10 Informe de Calificación del Riesgos. Se procede a realizar una valoración de los riesgos teniendo en cuenta las dimensiones de seguridad como confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad en relación a la frecuencia con que pueden ocurrir las amenazas definidas para cada activo.

De acuerdo al análisis de riesgos, se puede determinar que existen activos del Instituto Nacional de Vías Territorial Nariño, que presentan riesgos clasificados como críticos y con una probabilidad de frecuencia alta, tales como, equipos informáticos (hardware), debido a la avería de los mismos por manipulación inadecuada por parte de los funcionarios, por variación del voltaje de la energía eléctrica, también de la infraestructura de comunicaciones debido a la exposición y poca seguridad de los equipos que componen esta infraestructura.

Igualmente se presentan activos con riesgos clasificados como críticos y con una probabilidad de frecuencia baja, tales como, equipos informáticos (hardware), debido a eventos sísmicos, fuego, y volcánicos, debido a que la sede del Instituto Nacional de Vías Territorial Nariño se encuentra ubicada en una zona de Amenaza Volcánica Alta ZAVA por sus cercanía a las faldas de volcán Galeras hacia el occidente de la ciudad de Pasto, con respecto a la parte sísmica es importante recalcar que la sede de la Territorial Nariño corresponde a las antiguas instalaciones del Ministerio de Obras Públicas y Transporte Distrito 14, las cuales fueron construidas durante los primeros años de la década de los 80 y por lo tanto, su estructura no cumple con la Norma Sismoresistente 2010, y no está entre los planes realizar un estudio de vulnerabilidad sísmica y el refuerzo correspondiente.

También se pueden presentar riesgos en los activos clasificados como críticos y con una probabilidad de frecuencia baja, tales como, equipos informáticos (hardware) por las condiciones inadecuadas de humedad y temperatura, por fuego y agua por causas no naturales, manejo inadecuado de los archivos por los funcionarios, este riesgo puede conllevar a la perdida de la integridad de la información, difundir la información confidencial, avería en equipos, difusión de virus y el interrupción de actividades de la entidad.

Referente a los activos de redes de comunicaciones, el riesgo es clasificado como crítico con una probabilidad de frecuencia baja, el cual puede ser generado por errores de usuarios; por lo que es importante implementar políticas de seguridad orientadas a proteger los activos de la entidad y minimizar los riesgos, y cuando estos se presenten el impacto sea mínimo.

Dentro de los Riesgos clasificados como importantes y con una probabilidad de frecuencia baja se encuentra la organización deficiente por parte de los funcionarios de la oficina jurídica, área técnica, área administrativa y archivo, privilegios de acceso no controlados, suplantación de la identidad del usuario, fugas de información, modificación de la información, uso inadecuado del servicio de internet y correo electrónico, manipulación no autorizada y falta de mantenimiento de los equipos informáticos, robo de los equipos informáticos, y una muy importante que es la indisponibilidad de los funcionarios. Todas las anteriores son riesgos a tener en cuenta, y los cuales pueden originar daños a la entidad.
La ocurrencia de eventos tales como incendio, sismo, erupción volcánica son críticos en caso de que ocurra, aunque la probabilidad de que se presente es muy baja, a pesar de que la sede está ubicada en una zona de amenaza volcánica alta y en una zona de riesgo sísmico alto, se deben tener en cuenta y establecer políticas y medidas de seguridad enfocadas a minimizar cada riesgo.

De acuerdo a lo anterior, los activos con mayor prioridad de ser protegidos son: equipos informáticos, datos e información, redes de comunicación, software y aplicaciones, toda vez que son vulnerables a los ataques.

Se los debe proteger del uso no advertido, del abuso de privilegios, errores de usuarios, entornos inadecuados de seguridad, etc. La protección se la consigue diseñando e implementando políticas de seguridad que capaciten al funcionario en el adecuado manejo de la información, gestión de contraseñas, control de acceso, administración de equipos y software que permitan mejorar la seguridad física y lógica, ejecución permanente de copias de seguridad, etc.

Después de realizar el análisis de riesgos para los activos del Instituto Nacional de Vías Territorial Nariño, y de acuerdo a los resultados obtenidos, se especifican las políticas de la seguridad informática, teniendo como guía la norma ISO/IEC 27001:2013

Se diseñan las políticas que se pretende implementar en cada dependencia de la territorial con el fin de minimizar los riesgos encontrados. El documento de la política de seguridad de la información debe enunciar el compromiso de la dirección y establecer el enfoque de la entidad para manejar la seguridad de la información. El documento de la política debe contener enunciados relacionados con políticas y medidas de seguridad enfocadas a minimizar cada riesgo.

Se debe proteger del uso no previsto, del abuso de privilegios, fallos en los servicios de comunicaciones, errores de usuarios, condiciones inadecuadas de seguridad, etc., esto se logra diseñando e implementando políticas de seguridad que permitan capacitar al usuario en el manejo y clasificación de la información, gestión de contraseñas, control de acceso, seguridad física y lógica, actualizaciones permanentes del software, elaboración permanente de copias de seguridad. etc.

Las políticas y los estándares constituidos, son referentes marco para la administración y conservación de los activos informáticos, los documentos y los archivos de la Instituto Nacional de Vías - Territorial Nariño.

Con el diseño de las políticas de seguridad de la información, se establece al interior de la entidad una cultura de calidad, trabajando de forma confiable y controlada, constituyendo referentes de organización y administración de las tecnologías de la información y las comunicaciones TIC, involucrando a todos los funcionarios comprometidos en la seguridad y el uso de los recursos informáticos.

En la Instituto Nacional de Vías - Territorial Nariño los documentos, los archivos y la información son de carácter público y por lo tanto cumple con los objetivos esenciales de organización, clasificación, conservación y consulta en las diferentes fases del ciclo vital de los documentos.

8.1.11 Diseño de un modelo general de seguridad de la información SGSI. Con el análisis de los controles del anexo A de la norma ISO 27001: 2013, los pilares de seguridad de la información y los activos de información se recomiendan mejoras, implementar y nuevas medidas de seguridad sobre los activos, los procesos y los sistemas que brindan servicios en el Instituto Nacional de Vías Territorial Nariño.

La versión 2013 de la norma ISO 27001: 2013 incluye los siguientes catorce controles principales:

- ✓ Dominio A5. Políticas de la seguridad de la información.
- ✓ Dominio A6. Organización de la seguridad de la información.
- ✓ Dominio A7. Seguridad de los recursos humanos.
- ✓ Dominio A8. Gestión de activos.
- ✓ Dominio A9. Control de acceso.
- ✓ Dominio A10. Criptografía.
- ✓ Dominio A11. Seguridad física y del entorno.
- ✓ Dominio A12. Seguridad de las operaciones.
- ✓ Dominio A13. Seguridad de las comunicaciones.
- ✓ Dominio A14. Adquisición, desarrollo y mantenimiento de sistemas.
- ✓ Dominio A15. Relaciones con los proveedores.
- ✓ Dominio A16. Gestión de incidentes de seguridad de la información.
- ✓ Dominio A17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- ✓ Dominio A18. Cumplimiento.

8.1.12 Análisis detallado del Anexo A ISO 27001:2013. La Norma ISO/IEC 27001:2013 requiere el cumplimiento de ciertos criterios para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información SGSI en la entidad.

Para comprobar el estado actual del cumplimiento del estándar ISO/IEC 27001:2013 del Instituto Nacional de Vías Territorial Nariño, a continuación, se realiza el análisis, el cual permite comparar las condiciones existentes actualmente con el fin de encontrar las deficiencias existentes y el nivel de cumplimiento en base al estándar y desarrollar el diseño del Sistema de Gestión de Seguridad de la Información SGSI de acuerdo a los objetivos de seguridad deseados.

Se realiza un Análisis referente al Anexo A del estándar ISO/IEC 27001:2013 con el fin de determinar el nivel de cumplimiento de los Dominios, Objetivos de Control y Controles de Seguridad conformes al estándar ISO/IEC 27001:2013. Estos corresponden a los numerales 5 al 18.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
A.5.	POLITICAS DE SEGURIDAD			
A.5.1	Directrices de la Dirección en seguridad de la información			
A.5.1.1	Conjunto de políticas para la seguridad de la información.	La dirección debe aprobar un documento de política, este se debe publicar y comunicar a todos los funcionarios y entidades externas relevantes.	NO	Se redactan y documentan las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables. Este documento se pone a disposición de los funcionarios y público en general.
A.5.1.2	Revisión de las políticas para la seguridad de la información.	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.	NO	Las políticas de seguridad de la información se revisan y evalúan periódicamente y/o cuando sea necesario. Se documentan los cambios y las justificaciones de los mismos.
A.6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION			
A.6.1	Organización interna.			
A.6.1.1	Asignación de responsabilidades	La dirección debe apoyar	NO	Los roles y responsabilidades de la

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	para la seguridad de la información.	activamente la seguridad dentro de la entidad a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.		seguridad de la información están definidas, y son vitales para la protección de los activos informáticos individuales, así como los procesos específicos para la seguridad de la información.
A.6.1.2	Segregación de tareas	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la entidad con las funciones y roles laborales relevantes.	SI	El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades.	Se deben mantener los contactos apropiados con las autoridades relevantes.	NO	Implementar procedimientos para contactar a las autoridades pertinentes y reportar las incidencias relativas a la seguridad de la información.
A.6.1.4	Contacto con grupos de interés especial.	Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de	NO	Contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		seguridad especializada y asociaciones profesionales.		
A.6.1.5	Seguridad de la información en la gestión de proyectos.	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	NO	Una metodología de análisis de riesgos debería ser parte del proceso de implementación de un proyecto de TI con el fin de direccionarlos y controlarlos.
A.6.2	Dispositivos para movilidad y teletrabajo			
A.6.2.1	Política de uso de dispositivos para movilidad.	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	NO	Se documenta una política de seguridad apropiada para los móviles. Los dispositivos móviles son configurados bajo las condiciones de seguridad aplicables antes de realizar cualquier conexión a la red institucional.
A.6.2.2	Teletrabajo.	Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza	NO	No Aplica para la Territorial.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		teletrabajo.		
A.7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.			
A.7.1	Antes de la contratación			
A.7.1.1	Investigación de antecedentes.	Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a funcionarios, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso.	NO	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
A.7.1.2	Términos y condiciones de contratación.	Como parte de su obligación contractual; los funcionarios, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer	NO	Los acuerdos contractuales deben incluir las responsabilidades asignadas relativas a la seguridad de la información.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		sus responsabilidades y las de la organización para la seguridad de la información.		
A.7.2	Durante la contratación.			
A.7.2.1	Responsabilidades de gestión.	La dirección debe exigir a todos los funcionarios y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la entidad.	NO	La dirección asegura que los roles y responsabilidades están claramente definidas antes de brindar acceso confidencial, así como los funcionarios están comprometidos con las políticas de seguridad de la información.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información.	La dirección debe requerir que los funcionarios, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos en la entidad.	NO	Realizar campañas y talleres de formación y educación en la seguridad de la información.
A.7.2.3	Proceso disciplinario.	Debe existir un proceso disciplinario formal para los funcionarios que han cometido	SI	Los funcionarios son sometidos a procesos disciplinarios en caso de incumplimiento con las políticas de seguridad de la

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		una violación en la seguridad.		información de forma deliberada.
A.7.3	Cese o cambio de puesto de trabajo.			
A.7.3.1	Cese o cambio de puesto de trabajo.	Los derechos de acceso de todos los funcionarios, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.	NO	Los acuerdos contractuales deben plasmar el compromiso relativo a la confidencialidad de la información aún después de la terminación o cambio de empleo
A.8.	GESTION DE ACTIVOS			
A.8.1	Responsabilidad sobre los activos.			
A.8.1.1	Inventario de activos	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.	NO	Realizar el inventario de activos y su documentación con su clasificación y responsable, lo que permite identificar la importancia de cada uno de ellos y su impacto en la entidad.
A.8.1.2	Propiedad de los activos	Toda la información y los activos asociados con los medios de procesamiento de la	SI	Los activos inventariados tienen asignados los funcionarios responsables.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		información deben ser 'propiedad' de una parte designada de la entidad.		
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.	NO	Los funcionarios se comprometen a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de información generales.
A.8.1.4	Devolución de activos	Todos los funcionarios y usuarios de las partes externas deben devolver todos los activos de la entidad que se encuentren a su cargo, al terminar su empleo, o contrato.	SI	Se mantienen registros de la devolución de los activos entregados a los funcionarios. Necesarios para firmar paz y salvo con la entidad.
A.8.2	Clasificación de la información			
A.8.2.1	Directrices de clasificación.	La información debe ser clasificada en términos de su valor, requerimientos legales,	NO	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo a los niveles de seguridad establecidos

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		confidencialidad y grado crítico para la entidad.		
A.8.2.2	Etiquetado y manipulado de la información.	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la entidad.	NO	Cada uno de los activos inventariados está etiquetado con la clasificación de la información asociada.
A.8.2.3	Manipulación de activos.	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la entidad.	NO	Realizar y documentar los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
A.8.3	Manejo de los soportes de almacenamiento.			
A.8.3.1	Gestión de soportes extraíbles.	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación de la entidad.	NO	Implementar una política para la gestión de los medios removibles y se clasifican y protegen de acuerdo a su tipo.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
A.8.3.2	Eliminación de soportes.	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NO	Los medios removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
A.8.3.3	Soportes físicos en tránsito.	Los medios que contienen información se deben proteger contra acceso no autorizados, uso indebido o corrupción durante el transporte.	NO	Implementar las medidas de seguridad, para los medios transportados, los cuales podrían tener información sensitiva.
A.9	CONTROL DE ACCESOS			
A.9.1	Requisitos de negocio para el control de accesos.			
A.9.1.1	Política de control de accesos	Se debe establecer, documentar y revisar la política de control de acceso con base a los requisitos del negocio y de la seguridad para el acceso.	NO	Documentar la política de control de acceso en las Políticas de la Seguridad de Información.
A.9.1.2	Control de acceso a las redes y servicios asociados.	Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados	SI	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los funcionarios contienen una VLAN separada y que permite el acceso a

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		específicamente.		ella sólo a aquellos que son debidamente autenticados.
A.9.2	Gestión de acceso de usuario.			
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	NO	Implementar los identificadores únicos de los funcionarios, para mantener un registro de las acciones realizadas.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	NO	Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso formal.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	SI	A los funcionarios se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo. Estos privilegios son documentados y los funcionarios son agrupados bajo Perfiles de Usuario.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	SI	La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	NO	Verificar que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación se realiza de forma periódica y cualquier anormalidad es debidamente documentada.
A.9.2.6	Retirada o adaptación de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, o contrato, o se deben ajustar cuando se hagan cambios.	NO	Se debe implementar y soportar todo proceso que se haga cuando un funcionario se retire de la entidad o cualquier cambio.
A.9.3	Responsabilidades del usuario.			
A.9.3.1	Uso de información confidencial para la autenticación.	Se debe exigir a los usuarios que cumplan con las prácticas de la organización	SI	La información de autenticación del empleado en los sistemas y acceso a información es

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		para el uso de información de autenticación secreta.		confidencial.
A.9.4	Control de acceso a sistemas y aplicaciones.			
A.9.4.1	Restricción del acceso a la información.	Se debe restringir el acceso a la información y las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida en el control de acceso.	SI	Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del funcionario en la entidad.
A.9.4.2	Procedimientos seguros de inicio de sesión.	El acceso a los sistemas de información se debe controlar mediante un procedimiento de registro de inicio seguro.	NO	Implementar la protección de los sistemas mediante un mecanismo de inicio de sesión seguro. Se emplean mecanismos seguros de cifrado de información.
A.9.4.3	Gestión de contraseñas de usuario.	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.	SI	Se implementan mecanismos de recuperación de contraseñas de forma automática y se garantiza que la nueva contraseña del funcionario cumpla con los requisitos de seguridad expuestos en la Política de Seguridad de contraseñas.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
A.9.4.4	Uso de herramientas de administración de sistemas.	Se asigna a cada usuario claves de acceso a cada módulo de los programas que se manejan.	SI	Verificar que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados.
A.9.4.5	Control de acceso al código fuente de los programas.	Se debe restringir el acceso a los códigos fuentes de los programas.	SI	El código fuente sólo es accedido por las personas autorizadas.
A.10	CIFRADO			
A.10.1	Controles criptográficos.			
A.10.1.1	Política de uso de los controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO	Política de seguridad que documente el uso de los controles criptográficos, la escogencia y justificación de los algoritmos de cifrado y su aplicación en los servicios que la requieran.
A.10.1.2	Gestión de claves.	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	NO	Política de seguridad que documente el proceso y ciclo de vida de las llaves criptográficas.
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.			
A.11.1	Áreas seguras.			
A.11.1.1	Perímetro de seguridad física.	Se deben definir y usar	NO	El perímetro de seguridad física impide

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.		el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.
A.11.1.2	Controles físicos de entrada.	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	NO	Se desarrolla un control al acceso a las instalaciones e información vital de los sistemas de Información de la entidad.
A.11.1.3	Seguridad de oficinas, despachos y recursos.	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	NO	Las oficinas y lugares de trabajo claves deberían estar protegidas impidiendo el acceso físico a personas no autorizadas, así como no ser públicamente visibles.
A.11.1.4	Protección contra las amenazas externas y ambientales.	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas	NO	Desarrollar un plan de contingencia para controlar causas ambientales que podrían alterar el buen funcionamiento de la infraestructura Informática que contiene la información de la entidad.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		de desastre natural o creado por el hombre.		
A.11.1.5	El trabajo en áreas seguras.	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	NO	Las áreas seguras deben estar físicamente aseguradas y revisadas periódicamente.
A.11.1.6	Áreas de acceso público, carga y descarga.	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	NO	Los lugares de entrega de equipos y otros dispositivos están controlados y se restringe el acceso a áreas externas de la entidad.
A.11.2	Seguridad de los equipos.			
A.11.2.1	Emplazamiento y protección de equipos.	Los equipos de deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.	SI	Los equipos están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. y existen políticas de seguridad de la información documentadas para su uso.
A.11.2.2	Instalaciones de	Los equipos	SI	Los servicios de

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	suministro.	deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas en los servicios de suministro.		suministros de energía eléctrica, están acordes a al tipo de los equipos informáticos.
A.11.2.3	Seguridad del cableado.	El cableado de energía eléctrica y telecomunicaciones que trasporta datos o presta soporte a los servicios de información deben estar protegidos contra interrupciones o daños	SI	El cableado eléctrico está separado del cableado de datos previniendo de esta manera las interferencias.
A.11.2.4	Mantenimiento de los equipos.	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad	NO	Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	Formato de autorización para retirar equipos, informáticos y su registro, al devolverlo identificar quienes están autorizados a recibirlo.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Se debe aplicar seguridad al equipo fuera de la entidad tomando en	NO	Los equipos y/o dispositivos que pertenecen a la organización deberían ser gestionados sólo

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la entidad.		por el personal autorizado, así como tampoco ser utilizado en lugares públicos.
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Todos los ítems de equipo que contengan medios de almacenamiento deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier dato confidencial y software con licencia antes de su eliminación.	SI	Realizar un procedimiento seguro y documentado para la disposición o reutilización de equipos. Establecer política y procedimiento borrar información y software.
A.11.2.8	Equipo informático de usuario desatendido.	Los usuarios deben asegurarse de que los equipos desatendidos se les de la protección apropiada.	SI	Los usuarios deberían cerrar sesiones y proteger el equipo con contraseñas fuertes cuando no lo estén utilizando ya que podría estar expuesto a acceso no autorizado.
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia	NO	Implementar que toda documentación no debe estar expuesta hay que tenerla guardada en gabinetes, cerrar sesión, puntos de escritorio, correo, uso no autorizado de fotocopiadora-scanner,

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		en las instalaciones de procesamiento de información.		cámaras.
A.12	SEGURIDAD EN LA OPERATIVA.			
A.12.1	Responsabilidades y procedimientos de operación.			
A.12.1.1	Documentación de procedimientos de operación.	Documentar los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.	SI	Procedimientos de copias, mantenimiento, manejo de información, informes especiales, manejo de medios, mantenimiento, de recuperación y reinicio, eliminación segura.
A.12.1.2	Gestión de cambios.	Verificar que los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.	SI	Controlar cambios en equipos, software y procedimiento.
A.12.1.3	Gestión de capacidades.	Realizar un monitoreo continuo a los recursos y la adquisición de los nuevos, y se proyecta de acuerdo a las necesidades críticas de la entidad.	NO	Los recursos deberían ser monitoreados con el fin de gestionar su capacidad y rendimiento, así como proyectar que responda a las necesidades de la organización a largo plazo.
A.12.1.4	Separación de entornos de	Se deben separar los	NO	La separación de ambientes de desarrollo

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	desarrollo, prueba y producción.	ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.		y pruebas reduce el riesgo de operaciones no autorizadas.
A.12.2	Protección contra código malicioso.			
A.12.2.1	Controles contra el código malicioso.	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	NO	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos, especialmente sobre el software de código malicioso.
A.12.3	Copias de seguridad.			
A.12.3.1	Copias de seguridad de la información.	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	NO	Realizar por parte de los funcionarios las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A.12.4	Registro de			

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	actividad y supervisión.			
A.12.4.1	Registro y gestión de eventos de actividad.	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NO	Se mantienen los registros de los eventos ocurridos en los sistemas.
A.12.4.2	Protección de los registros de información.	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI	Implementar controles de seguridad que garanticen la protección de la información de los registros.
A.12.4.3	Registros de actividad del administrador y operador del sistema.	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	NO	Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de relojes.	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la entidad o ámbito de seguridad se deben	SI	Asegurar que todos los sistemas están acordes y ajustados en una referencia de tiempo única y sincronizada.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		sincronizar con una única fuente de referencia de tiempo.		
A.12.5	Control del software en explotación.			
A.12.5.1	Instalación del software en sistemas en producción.	Procedimientos de instalación en sistemas operativos con autorización.	SI	Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y software, que cumpla con las políticas de seguridad de la información.
A.12.6	Gestión de la vulnerabilidad técnica.			
A.12.6.1	Gestión de las vulnerabilidades técnicas.	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la entidad a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	NO	Implementar una metodología de análisis y evaluación de riesgos sistemática y documentada.
A.12.6.2	Restricciones en la instalación de software.	Se debe establecer e implementar las reglas para la	SI	La instalación de software es realizada sólo por el personal autorizado y con

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		instalación de software por parte de los usuarios.		software probado y licenciado, además de otorgar el principio del menor privilegio.
A.12.7	Consideraciones de las auditorías de los sistemas de información.			
A.12.7.1	Controles de auditoría de los sistemas de información.	Los requisitos y actividades que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos propios de la entidad.	NO	Determinar fechas de auditorías internas para los sistemas de información. El procedimiento es documentado.
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.			
A.13.1	Gestión de la seguridad en las redes.			
A.13.1.1	Controles de red	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	NO	Las redes deberían proteger la transmisión de la información garantizando su confidencialidad e integridad y en algunos casos su disponibilidad.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	Se deben identificar los mecanismos de seguridad, los	SI	El acceso a la red de los proveedores de servicios de red debe ser controlado y

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o contraten externamente.		monitoreado.
A.13.1.3	Segregación de redes.	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los funcionarios contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.13.2	Intercambio de información con partes externas.			
A.13.2.1	Políticas y procedimientos de intercambio de información.	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	SI	Las políticas y procedimientos para la transferencia de la información están debidamente documentados y se aplican los mecanismos de seguridad necesarios para garantizar la confidencialidad e integridad de la información.
A.13.2.2	Acuerdos de	Se deben	NO	Existen documentos y

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	intercambio.	establecer acuerdos para el intercambio de la información y el software entre la entidad y partes externas.		acuerdos sobre los algoritmos de cifrado a utilizar para la transferencia de información que garanticen su confidencialidad e integridad.
A.13.2.3	Mensajería electrónica.	La información contenida en la mensajería electrónica debe tener la protección adecuada.	NO	Implementar controles criptográficos que garanticen la seguridad en la transmisión de la información.
A.13.2.4	Acuerdos de confidencialidad y secreto.	Se tiene el mecanismo de encriptación, la información es solo accesible por aquellos a los cuales se ha autorizado a tener acceso.	NO	En los documentos y acuerdos contractuales de los funcionarios se estipula el compromiso con la confidencialidad de la información.
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.			
A.14.1	Requisitos de seguridad de los sistemas de información.			
A.14.1.1	Análisis y especificación de los requisitos de seguridad.	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos	NO	Existe una política documentada que establece los requisitos relativos a la seguridad de la información para la adquisición de los nuevos equipos.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		para nuevos sistemas de información o para mejoras a los sistemas de información existentes.		
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NO	Garantizar la comunicación de los servicios y aplicaciones bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.
A.14.1.3	Protección de las transacciones por redes telemáticas.	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de	NO	Garantizar la comunicación de los servicios y aplicaciones bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		mensajes no autorizada.		
A.14.2	Seguridad en los procesos de desarrollo y soporte.			
A.14.2.1	Política de desarrollo seguro de software.	Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	NO	No se desarrolla software.
A.14.2.2	Procedimientos de control de cambios en los sistemas.	Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	NO	El procedimiento formal de los cambios en el desarrollo de software debe ser documentado para garantizar la integridad del sistema o aplicación.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones de seguridad de la	SI	Los cambios en las aplicaciones deben ser revisados y probados antes de implementarlas de manera que se garantice que no comprometa la seguridad.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		entidad.		
A.14.2.4	Restricciones a los cambios en los paquetes de software.	Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO	Las actualizaciones y modificaciones de software son desarrolladas por el respectivo proveedor.
A.14.2.5	Uso de principios de ingeniería en protección de sistemas.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	NO	No se desarrolla software.
A.14.2.6	Seguridad en entornos de desarrollo.	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan	NO	No se desarrolla software.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		todo el ciclo de vida de desarrollo de sistemas.		
A.14.2.7	Externalización del desarrollo de software.	La entidad debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	El software desarrollado externamente debe tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros.
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.	NO	Los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	Pruebas de aceptación.	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	NO	Los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.3	Datos de prueba.			
A.14.3.1	Protección de los datos utilizados en pruebas.	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente .	SI	Los funcionarios pertinentes verifican que los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
				confidencialidad de la información.
A.15	RELACIONES CON PROVEEDORES.			
A.15.1	Seguridad de la información en las relaciones con proveedores.			
A.15.1.1	Política de seguridad de la información para proveedores.	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad se deben acordar y se deben documentar.	NO	Existe una política de seguridad de la información relacionada con los proveedores.
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de proveedores.	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la entidad.	NO	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.1.3	Cadena de	Los acuerdos	NO	Existen los acuerdos

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	suministro en tecnologías de la información y comunicaciones.	con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.		documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2	Gestión de la prestación del servicio por suministradores.			
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.	NO	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de	NO	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos.		
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
A.16.1	Gestión de incidentes de seguridad de la información y mejoras.			
A.16.1.1	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	NO	Los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.2	Notificación de los eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar	SI	Los funcionarios están alertados de los eventos e incidentes correspondientes

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		a través de los canales de gestión apropiados, tan pronto como sea posible.		relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados. Se establecen los procedimientos a seguir.
A.16.1.3	Notificación de los eventos de seguridad de la información.	Se debe exigir a todos los funcionarios y contratistas que usan los servicios y sistemas de información de la entidad, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	NO	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información.
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	NO	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información.
A.16.1.5	Respuesta a los incidentes de seguridad.	Se debe dar respuesta a los incidentes de seguridad de la información de	NO	Los funcionarios pertinentes tienen documentado los procesos y procedimientos para los

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		acuerdo con procedimientos documentados.		incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto sobre incidentes futuros.	NO	Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A.16.1.7	Recopilación de evidencias.	La entidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI	Existen formatos y documentos para recolectar la evidencia y emitirlos a las autoridades competentes.
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.			
A.17.1	Continuidad de la			

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	seguridad de la información.			
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	La entidad debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	NO	Los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	La entidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	NO	Los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La entidad debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e	NO	Los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.		de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.2	Redundancias.			
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	NO	La información debe ser redundante con el fin de mantener la disponibilidad de los servicios y ser probadas en intervalos regulares.
A.18	CUMPLIMIENTO.			
A.18.1	Cumplimiento de los requisitos legales y contractuales.			
A.18.1.1	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada Sistema de	SI	Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley. Aplicar la legislación Colombiana.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		Información y para la organización.		
A.18.1.2	Derechos de propiedad intelectual (DPI).	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.	NO	Definir las políticas y procedimientos para controlar la propiedad intelectual.
A.18.1.3	Protección de los registros de la organización.	Los registros importantes se deben proteger contra perdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	NO	Los registros están protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados.
A.18.1.4	Protección de datos y privacidad de la información personal.	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos	SI	Los datos personales son almacenados y protegidos de acuerdo a las conformidades de la ley y regulaciones.

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
		pertinentes, si se aplica, con las cláusulas del contrato.		
A.18.1.5	Regulación de los controles criptográficos.	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	SI	Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información.
A.18.2	Revisiones de la seguridad de la información.			
A.18.2.1	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	NO	No se realizan auditorías con entidades externas.
A.18.2.2	Cumplimiento de las políticas y normas de	Se debe garantizar que todos los	NO	Existe la documentación para la realización de la

Dominio	Control ISO 27001:2013	Descripción del Control	Se cumple actualmente	Implementación
	seguridad.	procedimientos de seguridad dentro de las áreas de responsabilidad se llevan a cabo correctamente para lograr los cumplimientos con las políticas y las normas de seguridad.		auditoría interna del Sistema de Gestión de la Seguridad de la Información con el fin de verificar el nivel de cumplimiento, controles y políticas de seguridad de la información.
A.18.2.3	Comprobación del cumplimiento.	Los Sistemas de Información se deben verificar periódicamente para verificar el cumplimiento con las normas de implementación de la seguridad.	NO	Exista la documentación para la realización periódica de los test de penetración y verificación de resultados e informes.

Fuente: El Autor

El nivel de cumplimiento para los Dominios, Objetivos de Control y Controles de Seguridad del Anexo A de la norma ISO/IEC 27001:2013 es el siguiente:

Tabla 10. Nivel de Cumplimiento de los Dominios de Control de la Norma ISO/IEC 27001:2013.

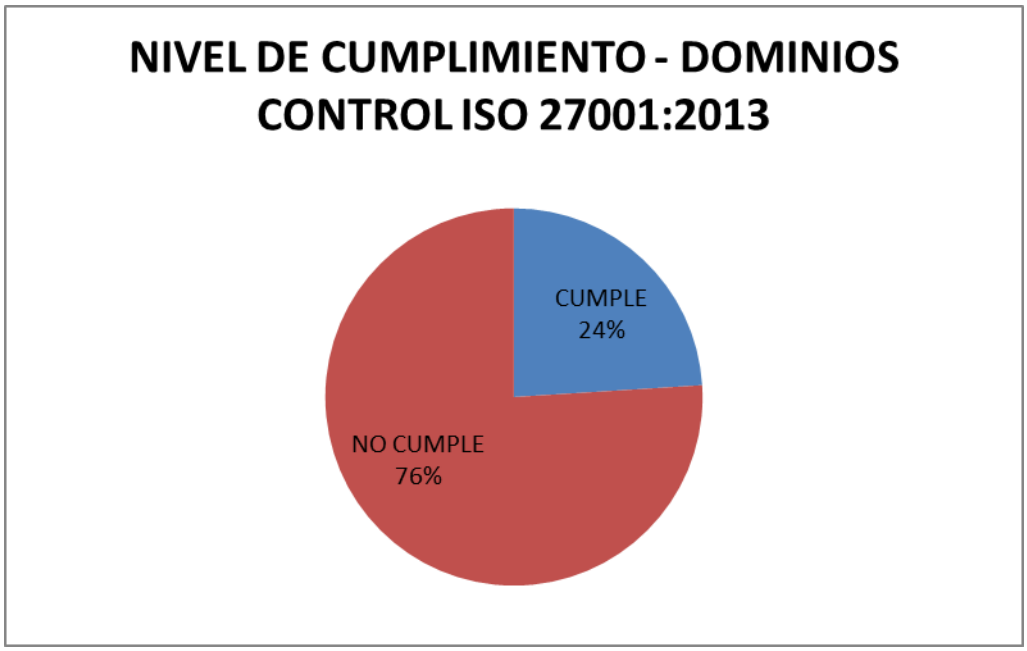
DOMINIO	CUMPLE (%)	NO CUMPLE (%)
Dominio A5. Políticas de la seguridad de la información.	0	100
Dominio A6. Organización de la seguridad de la información.	15	85
Dominio A7. Seguridad de los recursos humanos.	17	83

DOMINIO	CUMPLE (%)	NO CUMPLE (%)
Dominio A8. Gestión de activos.	20	80
Dominio A9. Control de acceso.	57	43
Dominio A10. Criptografía.	0	100
Dominio A11. Seguridad física y del entorno.	40	60
Dominio A12. Seguridad de las operaciones.	50	50
Dominio A13. Seguridad de las comunicaciones.	43	57
Dominio A14. Adquisición, desarrollo y mantenimiento de sistemas.	23	77
Dominio A15. Relaciones con los proveedores.	0	100
Dominio A16. Gestión de incidentes de seguridad de la información.	29	71
Dominio A17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.	0	100
Dominio A18. Cumplimiento.	38	62

Fuente: El Autor

De acuerdo a la anterior tabla, el nivel de cumplimiento referente a los Dominios de Control relacionados es el siguiente:

Figura 23: Nivel de Cumplimiento de los Dominios de Control de la Norma ISO/IEC 27001:2013.



Fuente. El Autor

De acuerdo al análisis anterior, se determina que el Instituto Nacional de Vías Territorial Nariño no cumple con la mayoría de los Dominios, Objetivos de Control y Controles de Seguridad de la norma ISO/IEC 27002:2013, esto se determina debido a que no se tiene la documentación correspondiente al estándar ISO/IEC 27001:2013, de igual manera no se poseen mecanismos de seguridad en la transmisión de la información.

Igualmente, aunque las instalaciones físicas estén protegidas con algunos controles de acceso y vigilancia, los funcionarios y algunos activos informáticos no están protegidos adecuadamente ante un gran evento, y no existen los procedimientos de contingencia para garantizar la continuidad de las actividades propias de la entidad.

9. DISEÑO DEL PLAN DE IMPLEMENTACIÓN DEL SGSI

9.1 Políticas y Normas de Seguridad de la Información. Con el propósito de establecer las políticas de seguridad de información requeridas por el Instituto Nacional de Vías Territorial Nariño y a fin de asegurar y garantizar la confidencialidad, integridad y disponibilidad de sus sistemas de Información interna. Se hace necesario el establecer las Políticas de Seguridad y Privacidad de la Información; con base a lo anterior se dará a conocer los lineamientos de actuación para funcionarios y contratistas, en relación con los recursos y servicios de información.

A partir de estas políticas se espera que el Instituto Nacional de Vías Territorial Nariño proteja sus activos de información a través de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), el cual contendrá las políticas específicas, normas, procedimientos, controles y asignación de responsabilidades, generando información confiable, integra y disponible a todos los usuarios.

Para asegurar la dirección estratégica en el Instituto Nacional de Vías – Territorial Nariño se establecen los siguientes objetivos de seguridad de la información:

- Minimizar el riesgo de seguridad de la información.
- Cumplir con los principios de seguridad de la información.
- Implementar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Proteger los activos de información.
- Establecer las políticas específicas, normas, procedimientos, controles y asignación de responsabilidades en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y terceros.
- Garantizar la continuidad de las actividades propias de la entidad frente a incidentes.

9.2 POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

9.2.1 Política de responsabilidad por los activos. Esta política tiene como propósito que el Instituto Nacional de Vías Territorial Nariño, asegure la información que genera, procesa, almacena y transmite a través de sus sistemas internos de información, con el fin de dar cumplimiento a una prestación del servicio oportuno, eficiente y de calidad.

9.2.1.1 Normas de responsabilidad por los activos

- Ejercer control sobre la aprobación o revocación de acceso a la información.
- Avalar la recolección y reajuste del inventario de activos de información tecnológicos.
- Facultar la restructuración de componentes de su plataforma tecnológica.
- Implantar una distribución adecuada para los recursos tecnológicos, con el propósito de garantizar la seguridad de la información.
- Establecer un plan de revisión periódica de la plataforma tecnológica y sus sistemas de información.
- A nivel del personal se tendrá como exigencia la utilización de los recursos tecnológicos en forma ética y responsable. Los funcionarios deberán guardar responsabilidad y cuidado a fin de evitar daños o pérdidas que afecten las actividades del instituto, de no ser así se actuara conforme a los mecanismos disciplinarios que la ley establece.
- Cada una de las ayudas o recursos tecnológicos suministrados a los funcionarios de planta y contratistas son de uso exclusivo para las labores de la entidad. En ningún caso estos deberán ser utilizados para fines personales o ajenos a su labor.
- Los funcionarios y contratistas pueden utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar sus actividades laborales al interior del instituto siempre y cuando se autorice su utilización.
- No se permite utilizar software de propiedad de funcionarios y contratistas en la plataforma tecnológica del instituto en la territorial Nariño.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Director Territorial o a quien este delegue, junto con copia de la información crítica que maneja; así mismo, debe entregar todos los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

9.2.2 Política de clasificación y manejo de la información. El Instituto Nacional de Vías Territorial Nariño definirá los mecanismos más idóneos para clasificar su información conforme a la importancia que tenga esta. Posteriormente generará guías de codificación de la información y generar los controles específicos para su protección. La información que genera el instituto está clasificada como pública, excepto aquella que por ley tenga reserva.

9.2.2.1 Normas para la clasificación y manejo de la información

- Socializar las guías de clasificación de la información a los funcionarios y contratistas del instituto, con una copia simple de estos documentos.

- Suministrar los componentes relacionados con el cifrado de la información, y su software.

- A partir de que un equipo es dado de baja se debe garantizar la eliminación segura de la información.

- Diseñar un sistema de control que permita generar confidencialidad, integridad y disponibilidad de la información.

- Determinar la adopción de un sistema dirigido al acceso, divulgación, almacenamiento, copia, transmisión, y eliminación de la información, para funcionarios y personal contratista.

- Establecer los periodos de almacenamiento conforme a las tablas de retención documental TRD.

9.2.3 Política de uso de periféricos y medios de almacenamiento. Se autorizará el uso de periféricos y medios que permitan el almacenamiento en los recursos de la plataforma tecnológica de la territorial Nariño, considerando las labores realizadas por los funcionarios y su necesidad de uso.

9.2.3.1 Normas uso de periféricos y medios de almacenamiento.

- Establecer los lineamientos y condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la territorial, así como la implementación de los controles que regulen su uso.

- Los funcionarios y contratistas no podrán modificar la configuración de periféricos y medios de almacenamiento establecidos.

9.2.4 Políticas de uso de dispositivos móviles. El Instituto Nacional de Vías Territorial Nariño establecerá los requerimientos de manejo de los dispositivos móviles institucionales y la responsabilidad es exclusiva de los funcionarios en cuanto su buen uso.

9.2.4.1 Normas de uso de dispositivos móviles

- Generar un cifrado de la memoria de almacenamiento de estos dispositivos a fin de garantizar la imposibilidad de generación de copias o extracción de datos.

- Configuración de un software antivirus que prevenga pérdidas y corrupción de información.

- Los usuarios no están autorizados para modificar las configuraciones de seguridad de los dispositivos móviles.

- Los usuarios deben garantizar el buen uso de estos equipos y evitar instalación de programas desde fuentes desconocidas.

- Los usuarios deben aceptar y aplicar nuevas versiones que sugiera el administrador.

- Los usuarios deben evitar conectar estos equipos a computadores de uso público.

- Los usuarios no podrán almacenar información diferente a la institucional.

9.3 POLÍTICAS DE CONTROL DE ACCESO LÓGICO

9.3.1 Política de acceso a redes y recursos de red. El Instituto Nacional de Vías Territorial Nariño suministrará los mecanismos necesarios para proteger las redes y recursos de red, a través de mecanismos de control de acceso lógico.

9.3.1.1 Normas de acceso a redes y recursos de red

- El Instituto Nacional de Vías Territorial Nariño establecerá los procesos de autorización y control que permitan proteger el acceso a redes de datos y recursos de red del instituto.

- El Instituto deberá asegurar las redes del instituto y que estas cuenten con métodos de autenticación para el acceso.

- Establecer mecanismos de control que permitan la identificación y autenticación de usuarios provistos por terceras partes.

- Verificar en forma periódica los accesos y que estos sean solo los permitidos.

- Los funcionarios y personal deberán firmar un acuerdo de confidencialidad con las condiciones de responsabilidad y seguridad de la información.

- Los equipos de cómputo deben cumplir con todos los requisitos o controles para autenticarse y solo podrán realizar tareas para las que fueron autorizados.

9.3.2 Política de administración de acceso de usuarios. La entidad avalará la incorporación de lineamientos para el control del acceso lógico de cada usuario o grupo de usuarios a las redes, los recursos tecnológicos y los sistemas de información de la territorial.

9.3.2.1 Normas de administración de acceso de usuarios

- Generar un proceso que permita la administración de seguridad del acceso de usuarios a los recursos tecnológicos de la territorial.

- Administrar, verificar y confirmar (crear, modificar, bloquear o eliminar cuentas de usuarios, perfiles, y políticas de contraseñas) el acceso a las redes de datos, recursos tecnológicos y sistemas de información.

- Constituir el procedimiento adecuado para la eliminación o bloqueo del acceso sobre los recursos tecnológicos y los sistemas de información de la territorial, cuando los funcionarios se desvinculan, toman vacaciones, o cambian de cargo.

- Especificar las políticas adecuadas de contraseñas de acceso a la plataforma tecnológica y los sistemas de información del instituto, tales como longitud, cambio periódico entre otros.

9.3.3 Política de responsabilidades de acceso de los usuarios. Los usuarios de los recursos tecnológicos deberán garantizar su uso adecuado y responsable, para la protección de la información.

9.3.3.1 Normas de responsabilidades de acceso de los usuarios

- Los usuarios son responsables directos de las posibles acciones realizadas en los sistemas de información, así como del usuario y contraseña asignados para el acceso a estos.

- Los usuarios no deben compartir sus cuentas y contraseñas, a fin de garantizar la gestión y administración adecuada, así como la protección de la información.

9.3.4 Política de uso de privilegios y utilitarios de administración. Los recursos de la plataforma tecnológica del instituto serán operados y administrados en condiciones controladas, éticas y de seguridad.

9.3.4.1 Normas de uso de privilegios y utilitarios de administración

- Otorgar los privilegios de seguridad sólo a aquellos funcionarios designados para dichas funciones.

- Limitar las conexiones remotas.

- Cambiar los usuarios o perfiles que traen por defecto los sistemas operativos y las bases de datos, así como sus contraseñas.

- No pasar por alto la seguridad de los sistemas de información del instituto, haciendo uso de utilidades que permiten el acceso directo al sistema operativo o a las bases de datos.
- Inhabilitar las funciones no utilizadas de los sistemas operativos, para optimizar recursos de procesamiento.

- Inspeccionar en forma periódica la actividad de los usuarios con privilegios de administración.

9.3.5 Política de control de acceso a sistemas de información. Garantizar que los sistemas de información sean apropiadamente resguardados contra ingresos no autorizados a través de componentes de control de acceso lógico, así mismo se espera acoger buenas prácticas de desarrollo en los productos para controlar el acceso lógico y evitar accesos no autorizados.

9.3.5.1 Normas de control de acceso a sistemas de información

- Establecer privilegios y restricciones de acceso a los sistemas y aplicativos del Instituto.

- Asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como la deshabilitación del campo de recordación de contraseñas.

- Garantizar que las cuentas se deshabilitan después de tres intentos inválidos de ingreso a los sistemas desarrollados.

- Asegurar la reautenticación de usuarios antes de la realización de operaciones críticas en los sistemas de información.

- Limitar el número de sesiones sobre el mismo sistema de información en un cierto período de tiempo.

9.4 POLÍTICAS DE CONTROL DE ACCESO FÍSICO

9.4.1 Política de seguridad física. Garantizar la efectividad de los mecanismos de seguridad física y control de acceso de sus instalaciones, así como el control de las amenazas externas e internas que puedan afectar las instalaciones**.**

9.4.1.1 Normas de seguridad física

- Garantizar la seguridad física y control de equipos de cómputo, centros de cableado y otras áreas de procesamiento de la información.

- Las solicitudes de acceso deben ser aprobadas por el Director Territorial, además, los visitantes siempre deberán estar acompañados de un funcionario designado por el Director Territorial durante su visita a estos equipos de cómputo o centros de cableado.

- Anotar el ingreso a los centros de cómputo, en un registro o bitácora ubicada en la portería de la entidad.

- Controlar los privilegios de acceso físico a los centros de cómputo y de cableado en eventos de retiro, traslado o cambio de personal autorizado.

- Proporcionar las condiciones físicas y medioambientales adecuadas, para garantizar la protección de los recursos ubicados en los centros de cómputo.

- Certificar que el cableado se encuentra protegido con el fin de reducir las intercepciones o daños.

- Garantizar que los recursos de la plataforma tecnológica estén protegidos contra fallas o interrupciones eléctricas.

- Programar labores de mantenimiento preventivo de redes eléctricas, voz y datos, con personal capacitado, autorizado e identificado.

- Programar los recursos para asegurar el perfecto estado de los controles físicos implantados.

- Las entradas y salidas de funcionarios y personal a las instalaciones del instituto deben ser registrados en el sistema de control de acceso (todo el personal debe contar con autorización previa).

9.4.2 Política de seguridad para los equipos institucionales. El Instituto proveerá las inspecciones que permitan la disminución de riesgos sobre los recursos de la plataforma tecnológica en cuanto a pérdida, robo o exposición al peligro dentro o fuera de sus instalaciones.

9.4.2.1 Normas de seguridad para los equipos institucionales

- Proveer los mecanismos de confidencialidad, integridad y disponibilidad de los recursos, dentro y fuera de las instalaciones del instituto.

- La entrada y salida de equipos y recursos tecnológicos de las instalaciones de la territorial, debe estar previamente autorizado por el Director Territorial.

- Adelantar periódicamente los mantenimientos preventivos y correctivos de los recursos tecnológicos del instituto.

- Garantizar la adquisición de pólizas de seguro para la plataforma tecnológica de la territorial.

- Instituir un bloqueo automático de los equipos de cómputo institucionales por inactividad, transcurrido un periodo de tiempo establecido.

- Los recursos tecnológicos que se encuentren por fuera de las instalaciones de la territorial, deben contar con medidas de protección de la información.

- Los recursos tecnológicos asignados a los funcionarios y contratistas, deben atender las instrucciones técnicas proporcionadas por el instituto.

- Cuando se presente una falla o problema de hardware o software, se debe informar al Director Territorial. El usuario no debe intentar solucionar el problema.

- Los usuarios deben bloquear sus equipos de cómputo en el momento de ausentarse de su puesto de trabajo.

- Los funcionarios de la territorial deben apagar los equipos de cómputo u otros recursos tecnológicos en horas no laborables.

9.5 POLÍTICAS DE NO REPUDIO Y AUTENTICIDAD DE LA INFORMACIÓN

9.5.1 Política de intercambio de información. El Instituto garantizará la seguridad de la información en el momento de ser transferida o intercambiada con otras entidades, aplicando los procedimientos de transferencia de información de acuerdo con su nivel de clasificación; de igual manera, se instituirán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio.

9.5.1.1 Normas de intercambio de información. Se definirá previamente los procedimientos de intercambio de información electrónica y física, que contemplen el uso de medios de transferencia confidenciales y la protección de los controles establecidos, con el fin de resguardar la confidencialidad e integridad de la misma.

9.5.2 Políticas para uso de conexiones remotas. El Instituto instituirá las condiciones para el establecimiento de conexiones remotas, y proveerá las herramientas y controles necesarios para que se realice de manera segura.

9.5.2.1 Normas para uso de conexiones remotas

- Establecer métodos y controles de seguridad a conexiones remotas hacia la plataforma tecnológica del instituto.

- Inspeccionar las conexiones remotas a los recursos. Las credenciales serán temporales y al culminar el periodo de autorización serán bloqueadas.

- Examinar y certificar los métodos de conexión remota a la plataforma tecnológica del Instituto.

9.5.3 Políticas para revisión independiente y auditoría. El Instituto gestionará la realización de revisiones independientes y auditorías al Sistema de Gestión de Seguridad de la Información (SGSI) y sus diferentes componentes.

9.5.3.1 Normas para revisión independiente y auditoría. Realizar auditorías al Sistema de Gestión de Seguridad de la Información (SGSI) del instituto con un espacio de tiempo programado de manea previa, finalmente efectuar recomendaciones si están fuese necesarias.

9.6 POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

9.6.1 Política de confidencialidad de la información. El Instituto garantizara la confidencialidad de la información.

9.6.1.1 Normas de confidencialidad de la información

- Firmar un acuerdo de Confidencialidad y Aceptación de las Políticas de Seguridad de la Información, por parte de los funcionarios de la territorial, con copia a su hoja de vida.

- Concretar Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y terceras partes incluyendo las obligaciones adquiridas y las responsabilidades civiles o penales por el incumplimiento de dichos acuerdos.

9.6.2 Política de privacidad y protección de datos personales. El Instituto actuara conforme a los requerimientos legales en cuanto a la protección de datos personales de funcionarios, contratistas, proveedores y demás terceros de los cuales reciba y administre información.

9.6.2.1 Normas de privacidad y protección de datos personales

- Las áreas de la territorial que procesan datos de funcionarios, contratistas y proveedores deben solicitar su autorización para el manejo de estos datos en el desarrollo de las actividades del instituto.

- Asegurar que solo aquellas personas que tengan una necesidad legítima y autorizada puedan tener acceso a datos de funcionarios, contratistas y proveedores.

- Las áreas de la territorial que procesan datos personales de funcionarios, contratistas y proveedores, deben atender las directrices técnicas y procedimientos establecidos para el intercambio de estos datos.
- Establecer mecanismos de control para proteger la información personal y evitar su divulgación, alteración o eliminación sin autorización previa.

- Guardar la reserva absoluta con respecto a la información del instituto o de sus funcionarios en el ejercicio de los Acuerdos de Confidencialidad.

- Es deber verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, personalmente, por correo electrónico, correo certificado, entre otros.

9.7 POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN

9.7.1 Política de controles criptográficos. El Instituto vigilará porque la información sensible o no pública, será cifrada al momento de almacenarse y/o transmitirse para preservar su integridad.

9.7.1.1 Normas de controles criptográficos

- Garantizar que la información electrónica no pública sea almacenada y/o transmitida con técnicas de cifrado a fin de proteger su confidencialidad e integridad.

- Verificar que el sistema de información que requiera realizar la transmisión de información no pública, cuente con mecanismos y procedimientos para el manejo y administración de cifrado de datos.

9.8 POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN

9.8.1 Política de copias de respaldo de la información. Garantizar la reproducción de copias de respaldo y almacenamiento a través de los recursos necesarios que permitan la efectividad de estas actividades.

9.8.1.1 Normas de copias de respaldo de la información.

- Crear y adoptar los procedimientos de responsabilidad para la generación, restauración, almacenamiento, recuperación de copias y tratamiento de estas que den respaldo de la información, garantizando su integridad, disponibilidad y seguridad.

- Es responsabilidad de los funcionarios identificar la información crítica almacenada en sus estaciones de trabajo o dispositivos móviles, que debe ser respaldada y almacenada de manera segura.

9.8.2 Política de inclusión de consideraciones de seguridad de la información en la continuidad, contingencia, recuperación y retorno a la normalidad. Proporcionar los recursos para proveer una respuesta efectiva a las necesidades del sistema en caso de contingencia o eventos catastróficos que afecten a los procesos de la entidad.

9.8.2.1 Normas de inclusión de consideraciones de seguridad de la información en la continuidad, contingencia, recuperación y retorno a la normalidad

- Ejecutar análisis de riesgos con las consideraciones de seguridad de la información a que haya lugar.

- Autorizar procedimientos de contingencia, recuperación y retorno a la normalidad.

- Designar responsables de emergencia, así como velar por su capacitación en caso de un evento catastrófico.

- Establecer el plan de recuperación de equipos de cómputo ante contingencias.

- Documentar los procedimientos de continuidad ante contingencias, teniendo en cuenta la seguridad de la información.

9.8.3 Política de redundancia. El Instituto garantizará la existencia de una plataforma tecnológica que satisfaga los requerimientos de disponibilidad de información para el instituto**.**

9.8.3.1 Normas de redundancia

- Examinar y constituir los requerimientos de redundancia para los sistemas de información críticos para el instituto y la plataforma tecnológica que los apoya.

- Gestionar las soluciones de redundancia tecnológica y realizar las respectivas pruebas periódicas, para garantizar el cumplimiento de los requerimientos de disponibilidad del instituto.

9.9 POLÍTICAS DE REGISTRO Y AUDITORÍA

9.9.1 Política de registro de eventos y monitoreo de lo recurso tecnológico y los sistemas de información. Realizar monitoreo permanente del uso de los sistemas de información del Instituto por parte de los funcionarios, además, velar por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.9.9.1.1 Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

- Garantizar la integridad y disponibilidad de los registros de auditoria, generados por la plataforma tecnológica y sistemas de información.

- Facultar sistemas de monitoreo que permitan detectar inconsistencias a la Política de Control de Acceso.

- Establecer los periodos de retención de archivos con base en las tablas de retención documental TRD.

- Examinar habitualmente los archivos de auditoria e identificar brechas de seguridad y otras actividades del monitoreo.

- Registrar los logs de auditoría, tales como: transacciones sobre los datos, fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, fallas en los módulos criptográficos, entre otros.

9.10 POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

9.10.1 Política que rige la organización interna. Establecer un esquema de seguridad de la información con roles y responsabilidades de administración, operación y gestión de la seguridad de la información.

9.10.1.1 Normas que rigen la organización interna

- Establecer los roles y responsabilidades dirigidos a la seguridad de la información en todos los niveles, las cuales deben estar documentadas.

- Garantizar la asignación de los recursos para la gestión de seguridad de la información del instituto.

- Promover la gestión de seguridad de la información del instituto y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad de la información.

- Autorizar y monitorear de manera periódica la organización de los controles de seguridad requeridos por el sistema.

9.11 POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.11.1 Política relacionada con la vinculación de personal. El Instituto reconociendo la importancia que tiene el factor humano, garantizará que la vinculación de nuevos funcionarios y contratistas se realizará siguiendo un proceso formal de selección, acorde a la legislación vigente.

9.11.1.1 Normas relacionadas con la vinculación de personal

- Realizar el análisis de antecedentes de los candidatos.

- Circunscribir aspectos relacionados con seguridad de la información en el proceso de inducción a funcionarios y contratistas.

- Los funcionarios, contratistas deben comprometerse con la suscripción y el cumplimiento de las Políticas de Seguridad de la Información, y el Acuerdo de Confidencialidad del instituto.

9.11.2 Política aplicable durante la vinculación de funcionarios y contratistas. Promover que los funcionarios y contratistas cuenten con el nivel deseado de conocimiento en seguridad de la información para la correcta gestión de los activos de información.

9.11.2.1 Normas aplicables durante la vinculación de funcionarios y contratistas

- Definir la aprobación de políticas, normas y demás lineamientos referentes a la seguridad de la información.
- Promover la importancia de la seguridad de la información entre los funcionarios y contratistas.

- Trazar y ejecutar un programa de auto apropiación del sistema de seguridad de la información, a fin de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

- Convocar a los funcionarios y contratistas a las capacitaciones de Concienciación en Seguridad de la Información.

- Informar a su jefe inmediato cuando se tenga conocimiento del incumplimiento de las políticas de seguridad de la información.

- El instituto deberá aplicar sanciones que por ley afecten o vulneren la seguridad de la información, de acuerdo con la normatividad vigente.

9.12 POLÍTICA DE DESVINCULACIÓN DE CONTRATISTAS; LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS.

El Instituto garantizará que sus funcionarios y contratistas serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada, segura y conforme a los lineamientos dados en la ley.

9.12.1 Normas para la desvinculación de contratistas; licencias, vacaciones o cambios de labores de los funcionarios

- Realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios del instituto aplicando los procedimientos y establecidos para tal fin.

- La territorial es responsable del proceso de desvinculación de los contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

- Informar de manera inmediata al administrador del cambio de labores de los funcionarios y desvinculación de contratistas, para la remoción o reasignación de privilegios en los recursos tecnológicos y/o sistemas de información.

9.13 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

9.13.1 Política de asignación de responsabilidades operativas. Determinar funciones específicas a funcionarios y contratistas, quienes deben garantizar la adecuada operación, administración y efectividad de los recursos tecnológicos, manteniendo y actualizando de la documentación de procesos operativos para la ejecución de dichas actividades.

9.13.1.1 Normas de asignación de responsabilidades operativas. Garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica.

9.14 POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

El Instituto suministrará los componentes necesarios que certifiquen la protección de la información y los recursos, adoptando los controles para evitar la divulgación, modificación o daño permanente causados por el contagio de software malicioso. Además, suministrará los dispositivos para generar cultura de seguridad entre sus funcionarios frente a los ataques de software malicioso.

9.14.1 Normas de protección frente a software malicioso

- Proporcionar herramientas tales como antivirus, antimalware, antispam, antispyware.

- Garantizar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso, garantizando así su autenticidad y su posibilidad de actualización.

- Garantizar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, antimalware, antispam y antispyware.

- Garantizar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- Garantizar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad.

- Los usuarios deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos ejecutados por primera vez, esencialmente los que se localizan en medios de almacenamiento externo o que provienen del correo electrónico.

- Los usuarios deben garantizar que los archivos descargados provienen de fuentes conocidas y seguras para evitar la contaminación de virus informáticos y/o instalación de software maliciosos en los recursos tecnológicos.

9.15 POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO

El Instituto designará los responsables y establecerá operaciones para vigilar la instalación del sistema operativo, con la garantía de soporte de los proveedores asegurando la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el sistema operativo es actualizado.

9.15.1 Normas de control al software operativo

- Implantar responsabilidades y procedimientos para vigilar la instalación de software en los sistemas operativos.

- Garantizar que el software instalado en la plataforma tecnológica del instituto cuente con soporte de proveedores confiables.

- Conferir accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, deberá monitorear dichas actualizaciones.

- Certificar los riesgos que genera la migración hacia nuevas versiones de los sistemas operativos.

- Implementar los controles para evitar la instalación de software en los equipos de cómputo del instituto.

9.16 POLÍTICA DE GESTIÓN DE VULNERABILIDADES

El Instituto revisará habitualmente las vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica a través de pruebas, con el objetivo de efectuar la corrección sobre los hallazgos encontrados por dichas pruebas.

9.16.1 Normas para la gestión de vulnerabilidades

- Examinar habitualmente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma, con el fin de advertir la exposición al riesgo de estos.

- Crear lineamientos y estándares para la operación segura de la plataforma tecnológica.
- Instituir restricciones y limitaciones para instalación de software en los equipos de cómputo.

- Formular, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

9.17 POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

9.17.1 Política de gestión de seguridad en las redes de datos. El Instituto garantizara la disponibilidad de redes de datos y de servicios con mecanismos de seguridad que protejan la integridad y la confidencialidad de la información.

9.17.1.1 Normas de gestión de seguridad en las redes de datos

- Adoptar medidas para garantizar la disponibilidad de los recursos y servicios de red del instituto.

- Establecer controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

9.18 POLÍTICA DE ASEGURAMIENTO DE LAS REDES DE DATOS

El Instituto propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información sensible del instituto ante posibles eventos de acceso o divulgación no autorizados.

9.18.1 Normas para el aseguramiento de las redes de datos

- Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del instituto.
- Realizar periódicamente las revisiones de los métodos de configuración de los dispositivos de seguridad y de red.
- Implementar la protección entre las redes internas del instituto y cualquier red externa, que este fuera de la capacidad de control por parte del instituto.
- Configurar los dispositivos de seguridad y de red de forma que limiten el tráfico entrante y saliente de las redes de datos del instituto.
- Vigilar la confidencialidad de la información transportada por las redes de datos.

9.19 POLÍTICA DE USO DEL CORREO ELECTRÓNICO

El Instituto proporcionará y garantizará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

9.19.1 Normas de uso del correo electrónico

- Suministrar un ambiente seguro y controlado para la plataforma de correo electrónico.

- Implantar controles que permitan proteger la plataforma de correo electrónico.
- Ejecutar control sobre el uso de cuentas de correo específicas.

- La cuenta de correo electrónico asignada es de carácter individual.

- Queda prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios y contratistas del instituto.

- Solo se aprueba la información relacionada con las labores y funciones de cada usuario en apoyo al objetivo misional del instituto.

9.20 POLÍTICA DE USO ADECUADO DE INTERNET

El Instituto suministrará los recursos necesarios para garantizar su disponibilidad a los usuarios, que así lo requieran para el desarrollo de sus actividades diarias en el instituto.

9.20.1 Normas de uso adecuado de internet

- Suministrar los recursos necesarios para la implementación, administración y mantenimiento para la prestación del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

- Diseñar e implementar componentes que permitan la continuidad o restablecimiento del servicio de internet en caso de eventualidad interna.

- Monitorear los canales del servicio de Internet.

- Implementar controles para evitar la descarga de software no autorizado.

- Crear registros correspondientes con la navegación y accesos de los usuarios a Internet.

- Instaurar canales para servicios o sistemas de información, de manera que optimicen su rendimiento.

- Evitar la descarga de información ajena al desempeño institucional.

9.21 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

9.21.1 Política para el establecimiento de requisitos de seguridad. El Instituto asegurará que el software adquirido y desarrollado por proveedores externos, cumplirá con los requisitos de seguridad y calidad establecidos.

9.21.1.1 Normas para el establecimiento de requisitos de seguridad. Los proveedores externos de sistemas de información deben instituir el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

9.22 POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

9.22.1 Política para el reporte y tratamiento de incidentes de seguridad. El Instituto promoverá el reporte de incidentes relacionados con la seguridad de la información.

9.22.1.1 Normas para el reporte y tratamiento de incidentes de seguridad

- Se debe informar los incidentes de seguridad que hayan sido identificados.
- Crear responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva.
- Evaluar los incidentes de seguridad de acuerdo a situaciones particulares y analizar en detalle aquellos en los que se considere pertinente.
- Destinar personal calificado, para investigar adecuadamente los incidentes.

9.23 POLÍTICAS DE CUMPLIMIENTO

9.23.1 Política de cumplimiento con requisitos legales, reglamentarios y contractuales. El Instituto velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, tales como los derechos de autor y propiedad intelectual, por lo tanto, garantizará porque el software instalado cumpla con los requerimientos legales y de licenciamiento.

9.23.1.1 Normas de cumplimiento con requisitos legales, reglamentarios y contractuales

- Identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables al Invías relacionados con seguridad y privacidad de la información.
- Garantizar que todo el software que se ejecuta en el instituto esté protegido por derechos de autor y requiera licencia de uso.
- Establecer una lista del software y sistemas de información que se encuentran permitidos, así como verificar que el software instalado en dichas estaciones de trabajo o equipos móviles sea el permitido.

- Efectuar los controles necesarios para proteger la información personal almacenada en la plataforma tecnológica.

- Cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.

CONCLUSIONES

Se pudo clasificar los activos de información y determinar el nivel de riesgo potencial de cada uno de ellos aplicando una metodología de riesgos de Tecnologías de Información como MAGERIT, el cual permite documentar paso a paso el Inventario de activos, la valoración cualitativa de los mismos, la identificación de amenazas, identificación de salvaguardas para los activos, valoración y evaluación del riesgo, la calificación del riesgo que nos indica los activos que se encuentran en riesgo y que deben ser tratados de inmediato.

Mediante el análisis de riesgos elaborado, se obtiene como insumo los problemas de seguridad del Instituto Nacional de Vías Territorial Nariño, que permite encontrar todos los elementos críticos dentro de la entidad, valorar dichos riesgos, determinar las amenazas, el impacto para cada dimensión de seguridad, la probabilidad, valorar los riesgos y las respectivas salvaguardas.

El desarrollo del proyecto permitió conocer los beneficios que genera un Sistema de Gestión de Seguridad de la Información SGSI en el Instituto Nacional de Vías Territorial Nariño mediante la aplicación de la norma ISO/IEC 27002:2013, que permitió conocer el estado actual de los dominios, objetivos y controles de seguridad, con un análisis detallado y el nivel de cumplimiento en referencia al Anexo A del estándar, que sugiere 14 dominios, 35 objetivos de control y 114 controles en materia de seguridad que abarcan todos los aspectos a proteger en la entidad.

De acuerdo al estado actual de los dominios, objetivos y controles de seguridad permitió elaborar las Políticas de Seguridad de la Información generales, las cuales deben ser comunicadas a todos los funcionarios de la territorial con el fin de establecer un compromiso en mantener de los niveles de riesgos aceptables

RECOMENDACIONES

- Realizar la revisión de los controles de seguridad, con cierta regularidad en periodos de tiempo determinados para verificar su efectividad.

- Se recomienda la implementación de las Normas y Políticas de seguridad definidas en el presente proyecto de grado.

- Se recomienda agregar en los procesos de la entidad, el análisis y gestión de riesgos informáticos como una medida para mejorar la seguridad de la información.

- Se recomienda capacitar al personal seleccionado de la entidad, para que lidere los procesos de seguridad de la información de la entidad.

DIVULGACIÓN

Como medios de divulgación se tiene previsto la socialización, y sensibilización de las Políticas y Normas de Seguridad de la Información a los funcionarios de la entidad, por medio de talleres prácticos, con el propósito que los funcionarios adopten, interioricen y acaten las Políticas y Normas de Seguridad de la Información, los procedimientos y prácticas de seguridad definidas en la entidad y comprendan las implicaciones, peligros y riesgos de sus acciones, con el objeto de garantizar su desempeño, eficacia y cumplimiento.

BIBLIOGRAFIA

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.

AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012.

BUITRAGO Estrada J. C., BONILLA Pineda D.H., MURILLO Varón C. E. Diseño de una Metodología para la Implementación del Sistema de Gestión de Seguridad de la Información - SGSI, en el sector de Laboratorios de Análisis Microbiológicos, basado en ISO 27001. Bogotá, 2012, 142 p. Trabajo de Grado. Universidad EAN.

COLOMBIA. Presidencia de la república. Decreto 2618 de 2013 por el cual se modifica la estructura del Instituto Nacional de Vías (Invías) y se determinan las funciones de sus dependencias. ART. 1 [En línea]. Disponible en: https://www.mintransporte.gov.co/descargar.php?idFile=13029 [citado en 20 de abril de 2016].

CONSTAIN Gustavo Eduardo, RAMÍREZ Gabriel Mauricio. Módulo Modelos y Estándares de Seguridad Informática, 2013. Universidad Nacional Abierta y a Distancia.

DORIA CORCHO, Andrés Felipe. Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la Universidad de Córdoba. Montería, 2015, 267 p. Trabajo de Grado. Universidad Nacional Abierta y a Distancia.

GUZMAN GARCIA Alexander, TABORDA BEDOYA Carlos Alberto. Diseño de un Sistema de Gestión de la Seguridad Informática SGSI para empresas del área textil, en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la Auditoría. Bogotá, 2015, 311 p. Trabajo de Grado. Universidad Nacional Abierta y a Distancia.

ISO 27001. (2005). ¿Qué es un SGSI? El portal de ISO 27001 en español. [en línea]. disponible en: http://www.iso27000.es [citado en 25 de abril de 2016].

Misión y visión. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/objetivos-y-funciones [citado en 08 de abril de 2016].

Objetivos y Funciones. [en línea] disponible en: http://www.invias.gov.co/index.php/informacion-institucional/objetivos-y-funciones [citado en 08 de abril de 2016].

RAMIREZ CASTRO, A. Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013. 2014. Trabajo Final de Máster. UOC.

SARRIA CUELLAR, Mercedes. Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. Florencia, 2015, 175 p. Trabajo de Grado. Universidad Nacional Abierta y a Distancia.

Sistema de Gestión de la Seguridad de la Información, p. 7. [en línea] disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf [citado en 25 de abril de 2016].

Anexo A

Resumen analítico RAE.

Título de Documento.	DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA EL INSTITUTO NACIONAL DE VIAS TERRITORIAL NARIÑO.
Autor	CÉSAR ENRIQUE MORÁN FERNÁNDEZ
Palabras Claves	SGSI, ISO/IEC 27001, análisis de riesgos, MAGERIT.
Descripción El documento es un proyecto aplicado que tiene como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información SGSI aplicado al Instituto Nacional de Vías Territorial Nariño.	
Fuentes Bibliográficas	• Amutio, M. A., Candau, J., Mañas, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. 2012. Madrid: Ministerio de Hacienda y Administraciones Públicas. • Constain, Gustavo Eduardo, Ramírez, Gabriel Mauricio, "Módulo Modelos y Estándares de Seguridad Informática", 2013. UNAD. • López Neira Agustín, Ruiz Sphor Javier. El Portal del ISO 27001 en español. Disponible en Internet: http://www.iso27000.es/iso27000.html • Ramírez Castro, A. Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013. 2014. Trabajo Final de Máster. UOC.

Contenido:

a) **Descripción del problema:** En la actualidad dado el incremento de la utilización del Internet, las redes sociales, la evolución de la tecnología en general, y la falta de conocimiento para prevenir riesgos, ha generado múltiples amenazas que aprovechan vulnerabilidades de las organizaciones para generar un impacto negativo en las mismas, ocasionando que se pierdan alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Los problemas presentados y las fallas de seguridad registradas en Instituto Nacional de Vías Territorial Nariño, muchas veces se deben al poco conocimiento que tienen las entidades del concepto de seguridad informática, ya que la mayoría de las veces los funcionarios ignoran que existe un procedimiento para realizar una actividad. En ocasiones, si este procedimiento existe, lo omiten y operan de la manera que ellos mejor consideran creyendo que así es la forma correcta, siendo esto un aspecto negativo para la entidad. La Territorial Nariño maneja mucha información ya sea administrativa, contractual, etc., la cual en muchas ocasiones se ve expuesta a terceros, de ahí la importancia de realizar un análisis detallado de errores que se pueden cometer ya sea por la parte humana o por parte del manejo de la seguridad que se lleva a cabo en esta institución y también fallas que son producto de la planta física.

a) **Objetivo General.** Diseñar un Sistema de Gestión de Seguridad Informática SGSI basado en la norma ISO/IEC 27001:2013 en el Instituto Nacional de Vías – Territorial Nariño, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque.

b) Objetivos Específicos.

- Identificar los activos informáticos para establecer los dominios del estándar ISO/IEC 27001:2013.
- Determinar las vulnerabilidades, amenazas y riesgos de seguridad existentes para hacer la valoración de los mismos aplicando la metodología MAGERIT.
- Verificar la existencia de controles de acuerdo a la norma ISO 27001:2013 que ayude a definir la existencia de políticas y procedimientos de seguridad.
- Diseñar el SGSI para la empresa de acuerdo a los resultados de la evaluación realizada anteriormente, que permita obtener confidencialidad, integridad y disponibilidad de la información.

c) **Resumen de lo desarrollado en el proyecto**. El proyecto de grado se desarrolla a lo largo de nueve capítulos. Desde el primer capítulo hasta el capítulo quinto corresponde a la presentación del proyecto y contiene el título, planteamiento del problema, justificación, objetivos,

alcance y delimitación respectivamente. En el capítulo sexto se desarrolla el Marco Referencial, en el cual se desarrolla el Marco Teórico en donde se realiza una recopilación de la teoría sobre la cual se desarrolla el proyecto, el Marco Conceptual en el que se estudian los conceptos relacionados, el Marco Legal, toda vez que es importante delimitar el proyecto a la legislación correspondiente y el Marco Contextual en donde se hace una descripción del Instituto Nacional de Vías. En el capítulo siete se desarrolla el Marco Metodológico del proyecto. En el capítulo ocho se comienza propiamente el desarrollo del Sistema de Gestión de la información SGSI, para ello se realiza un análisis completo de los riesgos a los que están sometidos los medios relativos a la información, para ello utilizamos la Metodología MAGERIT, en este mismo capítulo, con el análisis de los controles del anexo A de la norma ISO 27001: 2013, se realiza un estudio completo de los 14 dominios, 35 objetivos de control y 114 controles, este análisis nos presenta el panorama en el que se encuentra el Instituto Nacional de Vías Territorial Nariño con respecto a la norma , y con este insumo en el capítulo nueve se realiza el Diseño del Plan de implementación del SGSI por intermedio de las Políticas y Normas de Seguridad de la Información, por último se realizan las conclusiones y recomendaciones.

Metodología

El enfoque de la investigación es cuantitativo ya que se pretende hacer la medición de las vulnerabilidades, amenazas y riesgos en cuanto a la confidencialidad, integridad y disponibilidad de la información.
Es una investigación de tipo explicativa porque se trata de explicar la relación existente entre las vulnerabilidades existentes y los ataques que pueden presentarse en el sistema de información a causa de esas vulnerabilidades.
Es descriptiva porque trata de describir cómo se lleva a cabo el proceso de análisis y evaluación de los riesgos haciendo uso de la metodología MAGERIT.

Conclusiones.

- Se pudo clasificar los activos de información y determinar el nivel de riesgo potencial de cada uno de ellos aplicando una metodología de riesgos de Tecnologías de Información como MAGERIT, el cual permite documentar paso a paso el Inventario de activos, la valoración cualitativa de los mismos, la identificación de amenazas, identificación de salvaguardas para los activos, valoración y evaluación del riesgo, la calificación del riesgo que nos indica los activos que se encuentran en riesgo y que deben ser tratados de inmediato.
- Mediante el análisis de riesgos elaborado, que se obtiene como insumo todos los problemas de seguridad del Instituto Nacional de Vías Territorial Nariño y que permite encontrar todos los elementos críticos dentro de la entidad, valorar dichos riesgos, determinar las amenazas, el impacto para

cada dimensión de seguridad, la frecuencia, valorar los riesgos y las respectivas salvaguardas.

- El desarrollo del proyecto permitió conocer los beneficios que genera un Sistema de Gestión de Seguridad de la Información SGSI en el Instituto Nacional de Vías Territorial Nariño mediante la aplicación de la norma ISO/IEC 27001:2013, que permitió conocer el estado actual de los dominios, objetivos y controles de seguridad, con un análisis detallado y el nivel de cumplimiento en referencia al Anexo A del estándar, que sugiere 14 dominios, 35 objetivos de control y 114 controles en materia de seguridad que abarcan todos los aspectos a proteger en la entidad.
- De acuerdo al estado actual de los dominios, objetivos y controles de seguridad permitió elaborar las Políticas de Seguridad de la Información generales, las cuales deben ser comunicadas a todos los funcionarios de la territorial con el fin de establecer un compromiso en mantener de los niveles de riesgos aceptables.

Recomendaciones.

- Realizar revisión de los controles de seguridad, con cierta regularidad en periodos de tiempo determinados para verificar su efectividad.
- Implementar en la entidad de las Normas y Políticas de seguridad definidas en el presente proyecto de grado.
- Agregar en los procesos de la entidad, el análisis y gestión de riesgos informáticos como una medida para mejorar la seguridad de la información.
- Capacitar al personal seleccionado de la entidad, para que lidere los procesos de seguridad de la información de la entidad.

Anexo B

ENCUESTA PARA LOS FUNCIONARIOS DEL INSTITUTO NACIONAL DE VIAS – TERRITORIAL NARIÑO

Duración de la encuesta 15 minutos:

Basándose en su propia experiencia:

Marque con una X su respuesta

¿Frecuencia del cambio de las contraseñas del computador asignado?

_____a) Entre 1 y tres meses
_____b) Entre 3 y 6 meses
_____c) Entre 6 meses y 12 meses
_____d) más de 12 meses

¿Frecuencia del uso del Internet?

_____a) 1 hora al día
_____b) Dos horas al día
_____c) más de dos horas al día
_____a) Nunca

Problemas frecuentes que se presentan en el computador a su cargo son: Siendo 1= Siempre, 2= Algunas veces, 3= nunca

Afirmaciones:	1	2	3
a) El computador se bloquea	_____	_____	_____
b) El computador presenta mensajes error	_____	_____	_____
c) El computador no se conecta a la red	_____	_____	_____
d) El computador es lento	_____	_____	_____
	_____	_____	_____

Valore las siguientes afirmaciones: Siendo 1= Inaceptable, 2= Aceptable, 3= Bueno, 4= Excelente

Afirmaciones:	1	2	3	4
a) Cambio de Contraseñas periódicamente	_____	_____	_____	_____
b) Almacenamiento y manejo de copias de seguridad de la información		_____	_____	_____
c) Información sobre la responsabilidad en cuanto al manejo de la información		_____	_____	_____
		_____	_____	_____

Preguntas generales

¿Últimamente usted ha tenido algún problema en el momento de utilizar el computador? SI:_____NO:_____

¿Si ha encontrado dificultades, estas influyen en la calidad de atención al

cliente? SI:__NO:_____

¿Las dificultades encontradas en su computador son determinantes en el tiempo utilizado y en la calidad de su trabajo?

SI:_____NO:_____

¿Usted cree que las medidas de seguridad informática utilizadas son suficientes para proteger la información y prevenir incidentes?

SI:_____NO:_____

¿Usted cree que es necesario adoptar políticas de seguridad informáticas?

SI:_____NO:_____