DISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA Y DE INFORMACIÓN UTILIZANDO LA NORMA ISO 27001/2013 Y MAGERIT VERSIÓN 3.0 PARA LA GOBERNACIÓN DE NARIÑO

ARGENIS YERALDIN FAJARDO GUERRERO

ANGELA MARÍA TIMARAN JIMÉNEZ

UNIVERSIDAD DE NARIÑO

FACULTAD DE INGENIERÍA PROGRAMA

DE INGENIERÍA DE SISTEMAS SAN JUAN

DE PASTO

2018

DISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA Y DE INFORMACIÓN UTILIZANDO LA NORMA ISO 27001/2013 Y MAGERIT VERSIÓN 3.0 PARA LA GOBERNACIÓN DE NARIÑO

ARGENIS YERALDIN FAJARDO GUERRERO

ANGELA MARÍA TIMARAN JIMÉNEZ

Trabajo de Grado presentado como requisito para optar el título de Ingeniera de Sistemas

Director

FRANCISCO NICOLÁS SOLARTE SOLARTE

INGENIERO DE SISTEMAS

UNIVERSIDAD DE NARIÑO

FACULTAD DE INGENIERÍA PROGRAMA

DE INGENIERÍA DE SISTEMAS SAN JUAN

DE PASTO

2018

NOTA DE RESPONSABILIDAD

“La universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor**”.**

Artículo 13, Acuerdo No. 005 del 26 de enero de 2010, emanado por el Honorable Consejo Académico de la Universidad de Nariño.

“Las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de los autores.”

Artículo 1ro del Acuerdo No. 324 de octubre 11 de 1966 emanado del Honorable Consejo Directivo de la Universidad de Nariño.

NOTA DE EXCLUSIÓN

El pensamiento que se expresa en esta obra es de exclusiva responsabilidad de sus autoras y no comprometen la ideología de la Universidad de Nariño.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____
Firma del jurado

_____
Firma del jurado

_____
Firma del asesor

_____
Firma del co-asesor

San Juan de Pasto, Octubre 2018

AGRADECIMIENTOS

Agradezco primero a Dios por haberme permitido llegar hasta esta etapa profesional de mi vida, a mis padres y hermanos por todo su apoyo, comprensión y sobretodo la paciencia de esperar todo este tiempo hasta llegar este momento.

Al asesor Francisco Solarte por su guía e incondicional disposición para el desarrollo del proyecto.

A la Gobernación de Nariño, en especial a la Secretaría de TIC, Innovación y Gobierno Abierto y al Ingeniero Daniel Álvarez por su constante asesoría en la realización y consecución de resultados a lo largo del proyecto.

Ángela María Timaran Jiménez

AGRADECIMIENTOS

Doy gracias a Dios por darme la vida y las ganas de luchar cada día por mis sueños y aspiraciones.

A mis padres a quienes, jamás me cansaré de agradecerles por todo lo que estando a su alcance me han brindado siempre.

A mis hermanos por su apoyo incondicional y de quienes jamás he escuchado un no para conmigo.

A mi abuela Rosa Enríquez quien es mi segunda madre y a quien le debo tanto.

A mi familia y amigos quienes de alguna u otra manera contribuyeron para lograr este sueño.

Al asesor Francisco Nicolás Solarte por compartir sus conocimientos, brindarme su apoyo, colaboración incondicional y su permanente asesoría para la culminación de este proyecto.

Al Ingeniero Daniel Álvarez por brindarme su colaboración y asesoría en el desarrollo del proyecto.

A la Universidad de Nariño y sus docentes por enriquecer mis conocimientos y experiencias que contribuyeron a mi crecimiento y desarrollo como persona y profesional.

Por ultimo a la Gobernación de Nariño y a los funcionarios de la Secretaria de TIC por su predisposición para el desarrollo del proyecto de grado.

Argenis Yeraldin Fajardo Guerrero.

DEDICATORIA

Dedico mi proyecto de grado primero a Dios por haberme dado la sabiduría, perseverancia y por guiarme para poder alcanzar cada una de mis metas.

A mis padres por su apoyo incondicional y por su esfuerzo que a pesar de los momentos difíciles nunca me abandonaron y cumplieron conmigo este gran logro.

A mis hermanos por siempre estar ahí para mí, quienes son el motor de mi vida, a quienes amo y respeto.

A mis familiares que contribuyeron de manera muy positiva para culminar esta etapa.

Argenis Yeraldin Fajardo Guerrero.

DEDICATORIA

El proyecto de grado lo dedico a Dios por darme la fuerza y fe para terminar este proyecto y a mi familia por su incondicional apoyo para culminar mi carrera universitaria.

Ángela María Timarán Jiménez.

RESUMEN

El presente proyecto tuvo como finalidad el diseño de políticas y procedimientos de seguridad informática y de información para la Gobernación de Nariño, mediante un Sistema de Gestión de Seguridad de la información (SGSI), este diseño se elaboró basado en la Norma ISO/IEC 27001:2013 y la Metodología MAGERIT V. 3.0, los cuales especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI, estableciendo un conjunto de procesos y controles encaminados a garantizar la confidencialidad, disponibilidad e integridad de los activos informáticos y de información con los que cuenta la entidad.

Asimismo, se pudo salvaguardar la información el cual es el activo más importante de la Gobernación, donde el diseño de un sistema de Gestión de Seguridad de la Información podrá proporcionar una metodología muy sencilla y completa para contrarrestar los riesgos asociados o en su caso reducirlos al máximo, implantando medidas preventivas y correctivas las cuales garantizaron que los servicios informáticos y de información ofrecidos por la entidad fueran preservados, seguros y confiables.

Palabras clave:

Gobernación de Nariño, Sistema de Gestión de la Seguridad Informática, ISO 27001/2013, Magerit versión 3.0, Políticas.

ABSTRACT

The purpose of this project was to design information and security policies and procedures for the Government of Nariño, through an Information Security Management System (ISMS), this design was based on ISO / IEC 27001 : 2013 and the MAGERIT V. 3.0 Methodology, which specify the necessary requirements to establish, implement, maintain and improve an ISMS, establishing a set of processes and controls aimed at guaranteeing the confidentiality, availability and integrity of information and information assets with which the entity counts.

Likewise, it was possible to safeguard the information, which is the most important asset of the Government, where the design of an Information Security Management system will be able to provide a very simple and complete methodology to counteract the associated risks or, where appropriate, reduce them to maximum, implementing preventive and corrective measures which guarantee that the information and computer services offered by the entity are preserved, safe and reliable

Keywords:

Nariño Governorate, Computer Security Management System, ISO 27001/2013, Magerit version 3.0, Policies.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

Glosario

Amenazas: Vulnerabilidades que se pueden presentar en un sistema de información, donde una mala configuración y un mal funcionamiento del sistema de control pueden denegar o no detectar las causas potenciales que pueden afectar la infraestructura.

Confidencialidad: Medidas y herramientas que permiten a los sistemas de información, evitar el acceso de personas no autorizadas, con el fin de custodiar la información.

Disponibilidad: Es la técnica para que los sistemas de información se puedan recuperar de fallos tecnológicos, con el propósito de mantener el acceso a las funcionalidades en la gran mayoría del tiempo.

Integridad: Medidas y herramientas que permiten asegurar la procedencia de la información o datos, los cuales se identifican como datos seguros porque no se ha producido ninguna modificación o cambio desde su emisión y es exactamente igual al dato o información original.

Procedimientos: “Según la definición de la Real Académica Española, el significado de esta palabra refiere a la acción y efecto de proceder. Este concepto se define como un método o sistema estructurado para ejecutar algunas cosas”.

Riesgos: Termino que proviene del italiano, adoptado de una palabra árabe, la cual representa el potencial de perjuicios que se pueden presentar en una organización, por la falta de una estrategia de seguridad, asociándose al peligro o daño de un acontecimiento, a través de la probabilidad de ocurrencia dentro de un instante de tiempo.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Vulnerabilidades: Debilidad de un sistema, el cual permite a un hacker ingresar a un computador violentado la confidencialidad, integridad, disponibilidad de los datos y aplicaciones.

Activo: Relacionado con la seguridad de la información, es cualquier elemento informático o elemento relacionado con el tratamiento de la misma, es decir, sistemas, soportes, edificios, personas, que tengan un valor para la organización. Un activo es aquello que represente ganancias para la entidad, y que a su vez si son mal administrados representan perdidas y a su vez dependiendo del nivel de gravedad será el grado de complejidad los controles para aplicar para la búsqueda de una solución.

Control: Es también utilizado como sinónimo de salvaguarda o contramedida. Permite a las políticas, procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos por debajo del nivel asumido. En toda organización se necesita tener controles para evitar los riesgos y amenazas que no permitan que se cumpla el objetivo del negocio y colocando de este modo a la entidad en riesgo; los controles permiten si son bien aplicados un equilibrio en toda la organización.

Política de seguridad: Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

Autenticidad: El procedimiento de verificar la identidad que reclama un sujeto mediante una validación en un sistema de control de acceso.

Código malicioso: En seguridad informática, código malicioso es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso.

Copia de seguridad (backup): Archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.

Firewall (cortafuegos): Es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

Valoración del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

Trazabilidad: Consiste en un conjunto de medidas, acciones y procedimientos que permiten registrar e identificar cada producto desde su origen hasta su destino final.

INTRODUCCIÓN

Con la aparición de la computación digital, inició el periodo de más desarrollo tecnológico jamás visto por la humanidad, donde la información se ha convertido en un activo de gran valor para las organizaciones, es primordial garantizar que este activo este siempre bien custodiado, preservando su integridad, confidencialidad y disponibilidad en todo momento y lo más resguardado posible de todas las amenazas que hay alrededor, por lo anterior fue importante la seguridad informática, pues trató de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implicó la necesidad de gestión, fundamentalmente gestión del riesgo, donde se implantaron medidas preventivas y correctivas que ayudaron a eliminar los riesgos asociados o en su caso reducirlos al máximo garantizando así que los servicios informáticos ofrecidos por las empresas e instituciones fueran preservados, seguros y confiables.

La Gobernación de Nariño, sufrió algunos incidentes de seguridad informática, es por eso que se pretendió realizar estudios para determinar amenazas, vulnerabilidades y riesgos presentes en los activos informáticos, los cuales afectaban los recursos y el prestigio de la entidad, para mitigar estos riesgos se realizó una propuesta de diseño de políticas claras de seguridad informática acorde a las actividades de la empresa, que fueron aprobadas, difundidas y aplicadas en la misma.

El objetivo de este proyecto fue diseñar las políticas y procedimientos de seguridad informática para la Gobernación de Nariño, donde existía una infraestructura tecnológica bastante compleja de datos y redes, usando la norma ISO/IEC 27001 y la metodología MAGERIT para la gestión del riesgo en los activos de información presentes en la Gobernación, con el propósito de eliminar o mitigar el riesgo informático y salvaguardar activos de información para la mejora continua de la entidad.

Línea de investigación

Gestión Seguridad y control. Esta línea tuvo como objetivo, planificar, analizar, diseñar, implantar sistemas de control de información, con el propósito de brindar seguridad de la información en las organizaciones.

Alcance y delimitación

Para este proyecto solo se aplicaron los dominios definidos a continuación debido a que en estos las amenazas, vulnerabilidades y riesgos encontrados afectaron de manera crítica a la organización.

Tabla 1 Dominios y Objetivos de Control

DOMINIOS	OBJETIVOS DE CONTROL
A.5 Políticas de la seguridad de la información.	Directrices de la Dirección en seguridad de la información
A.6 Organización de la seguridad de la información.	Dispositivos de la Dirección en seguridad de la información
A.7Seguridad de los Recursos Humanos	Antes de la Contratación
	Durante la Contratación
	Cese o Cambio de Puesto de Trabajo
A.8 Gestión de Activos	Responsabilidad sobre los activos
	Clasificación de la Información
	Manejo de los soportes de almacenamiento

Tabla 1 (Continuación)

DOMINIOS	OBJETIVOS DE CONTROL
A.11 Seguridad Física y del entorno	Áreas Seguras
	Seguridad de los Equipos
A.12 Seguridad de las Operaciones	Responsabilidades y Procedimientos de Operación
	Protección contra código Malicioso
	Copias de Seguridad
	Registro de Actividad y Supervisión
	Control del Software en explotación
	Gestión de la Vulnerabilidad Técnica
	Consideraciones de las auditorias de los sistemas de información
A.14 Adquisición, Desarrollo y Mantenimiento de sistemas	Requisitos de Seguridad de los sistemas de Información
	Seguridad en los sistemas de Desarrollo y Soporte
A.15 Relaciones con los proveedores	Seguridad de la Información en las relaciones con suministradores
	Gestión de la Prestación del servicio por suministradores
A.16 Gestión de Incidentes de seguridad de la información.	Gestión de incidentes de seguridad de la información y mejoras
A.17Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio	Continuidad de la seguridad de la Información
	Redundancias
A.18 Cumplimiento	Cumplimiento de los requisitos legales y contractuales
	Revisiones de la Seguridad de la Información.

Fuente: La presente investigación

Modalidad

Este proyecto de trabajo de grado correspondió a la Modalidad de Trabajo de Aplicación, porque se aplicó para la Gobernación de Nariño, específicamente a la Secretaria de TIC, Innovación y Gobierno Abierto.

Descripción del problema

Planteamiento del problema

La Gobernación de Nariño tenía definido un Documento de Políticas de Seguridad de la Información, pero estas políticas no han sido difundidas e implementadas lo que ocasionaba que los funcionarios de esta entidad realizaran acciones inseguras, por ejemplo:

En cuanto a los sistemas de información no cambiar las claves de acceso, en la seguridad física no tener un registro de las personas que entran a la Gobernación a excepción de aquellas que llevan portátil, en ocasiones los equipos sufrían de calentamiento por no encontrarse ubicados en áreas con temperatura adecuada, el edificio por ser patrimonio arquitectónico no permitía hacer la adecuación del cableado de acuerdo a normas ISO o ICONTEC, el cableado estructurado del edificio en algunos casos no tenía protección, no contar con un firewall UTM físico para protección y aseguramiento de la red, con respecto a los aplicativos web se han presentado ataques a servidores internos en aquellos servicios que dan su cara a la nube, intrusiones en la página web.

Además, en la entidad no existieron unos procedimientos de seguridad informática orientados a la protección de los activos y manejo de la información.

De seguir funcionando así, la Gobernación podría estar expuesta a amenazas o ataques al sistema, lo que ocasionaría múltiples inconvenientes como pérdida total de la información, fuga de recursos económicos, filtración de información importante que no es de público conocimiento. Esta problemática hizo necesario proteger la

información, mediante el Diseño de Políticas y Procedimientos de Seguridad Informática basado en la norma ISO/IEC 27001, que proteja a la entidad de los posibles riesgos de seguridad de la información realizando un análisis y diagnóstico de los activos informáticos de la misma.

Formulación del problema

¿Cómo el Diseño de las Políticas y Procedimientos basados en el análisis y diagnóstico de la situación actual mediante la Norma IS0 27001 y el MAGERIT permitieron mejorar la seguridad informática y de información en la Gobernación de Nariño?

Sistematización del problema

- ¿Cuáles fueron las Políticas y Procedimientos de seguridad informática definidos y aplicados actualmente en la Gobernación de Nariño?
- ¿Cuál era el estado actual de la Gobernación en cuanto a seguridad informática y que cambios se requieren en las políticas de seguridad informática?
- ¿Cuáles fueron las vulnerabilidades, amenazas y riesgos en la seguridad informática a que se ve expuesta la gobernación de Nariño?
- ¿Cómo el plan de pruebas ejecutado permitió evidenciar los riesgos existentes en seguridad informática de la entidad?
- ¿Cómo diseñar las nuevas políticas de seguridad a partir de los hallazgos confirmados y los controles definidos en cada dominio evaluado?

Objetivo General

Diseñar Nuevas Políticas y Procedimientos de seguridad Informática y de información basados en la Norma ISO/IEC 27001/2013 y Magerit Versión 3.0, que permitieron mejorar la seguridad informática en la Gobernación de Nariño.

Objetivos Específicos

- Conocer la documentación de procesos y procedimientos de manejo de la información, la documentación de políticas de seguridad y determinar los activos informáticos y sistemas de información que funcionan en la Gobernación de Nariño.
- Realizar el proceso de análisis y evaluación de riesgos identificando mediante pruebas las vulnerabilidades y amenazas de seguridad a que está expuesta la Gobernación de Nariño.
- Verificar la existencia de controles de seguridad informática y de información de acuerdo a la norma ISO/IEC 27001 de control interno de seguridad informática.
- Diseñar las nuevas políticas y procedimientos de seguridad informática de acuerdo a los resultados obtenidos del proceso aplicado anteriormente.

Justificación

La Gobernación de Nariño siendo la más importante entidad administrativa en el departamento, actualmente cuenta con una infraestructura tecnológica amplia conformada por software, hardware, sistemas de información, comunicaciones, tecnologías de la información y plataformas tecnológicas en línea entre otros, se considera necesario que la entidad establezca acciones que garanticen la seguridad física y lógica de sus activos informáticos y que le permita valorar los riesgos informáticos que han sido identificados mediante el análisis de seguridad en toda su infraestructura tecnológica.

Teniendo en cuenta lo anterior, fue importante realizar este proyecto ya que con el Diseño de Políticas y procedimientos de seguridad informática los funcionarios conocieron la importancia y la sensibilidad de la información y sobre los métodos para asegurar el buen uso de los recursos informáticos, manteniéndolos libres de peligros, daños y riesgos, además tanto los usuarios internos como externos contaron con una información confidencial, integra y disponible al acceder a los sistemas de información y a las páginas web de la gobernación, dicho esto fue necesario tener unas políticas de seguridad informática bien concebidas y efectivas que pudieron proteger la inversión y los recursos de información de la entidad.

Con este proyecto la Gobernación de Nariño pudo mejorar la eficiencia gubernamental, minimizar los riesgos asociados a daños y asegurar que se cumplieran las funciones misionales de la entidad estableciendo políticas de seguridad y procedimientos de seguridad informática dando cumplimiento a la Estrategia de Gobierno en Línea (GEL) en cuanto al Componente TIC para Seguridad y Privacidad de la información.

Marco Referencial

Antecedentes

Para el proyecto se tuvo en cuenta los siguientes antecedentes:

- El proyecto desarrollado por: Ana Milena Pulido Barreto, Jenith Marsella Mantilla Rodríguez en la Universidad Nacional Abierta y a Distancia -Escuela de Ciencias Básicas Tecnología e Ingeniería, titulado: "MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA GENERAL DE SEGURIDAD INFORMÁTICA Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA OFICINA TIC DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO"[1].Este proyecto se considera importante y prioritario ya que contribuye al fortalecimiento de los procesos, actividades y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, así como también la Alcaldía Municipal de Fusagasugá contará con protocolos de seguridad y un Modelo para la implementación del Sistema Gestión de Seguridad de la información (SGSI), que estará alineado a la metodología del ciclo PHVA para realizar la implementación de un Sistema de Gestión de Seguridad de la Información que ha sido señalado en el manual de la estrategia de Gobierno en Línea (GEL) en su versión 3.0.

Del anterior proyecto se tomó como ejemplo el modelo de Sistema de Gestión de Seguridad de la información (SGSI) para tener una guía en la utilización de este modelo y así desarrollar las políticas de seguridad informática.

[1] PULIDO, Ana y MANTILLA, Jenith. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Tesis previa a la obtención del título de Especialización de Seguridad en Informática. Fusagasugá. Colombia: Universidad Nacional Abierta y a Distancia, 2016.

- El proyecto desarrollado por: Luis Olmedo Patiño Alpala en la Universidad Nacional Abierta y a Distancia "UNAD" titulado: "PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA CORPORATIVA, PROPOLSINECOR"[2]. Con el presente proyecto se pretende actualizar, apropiarse y establecer políticas de seguridad de la información, que protejan los activos de información, teniendo en cuenta la infraestructura y los últimos aplicativos o procesos de manejo de información implementados en la compañía, para ello se estudiará el marco teórico referente al tema, se identificarán activos de información, vulnerabilidades y amenazas en la seguridad informática, para estructurar una matriz de riesgos que permitirá determinar acciones de solución a corto, mediano y largo plazo, con el propósito de eliminar o mitigar el riesgo informático y salvaguardar activos de información que son el eje principal de toda gestión de seguridad de la información.

De este proyecto se tomó en cuenta el método para analizar las vulnerabilidades, amenazas y riesgos existentes en la seguridad informática, que puedan afectar los recursos y prestigio de la Gobernación; y de esta manera contrarrestar y mitigar los riesgos en seguridad informática, diseñando las Políticas de Seguridad de la Información, acordes al negocio y actividades de la empresa, para ser aprobadas por la alta gerencia, difundidas e implementación por la Gobernación de Nariño.

- El proyecto desarrollado por: David Hernando Alonso Torres en la Universidad

[2] PATIÑO, Luis. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR. Tesis previa a la obtención del título de Especialización de Seguridad en Informática. San Juan de Pasto. Colombia: Universidad Nacional Abierta y a Distancia, 2014.

de la Sabana titulado: “EVALUACIÓN DE SEGURIDAD A SISTEMAS DE INFORMACIÓN EN CUANTO A ATAQUES MALICIOSOS CON BASE EN NORMATIVIDAD, TENDENCIAS, IMPACTO Y TÉCNICAS VIGENTES PARA AMBIENTES EMPRESARIALES A NIVEL NACIONAL”[3]. En este proyecto se quieren compilar procedimientos consolidados en una metodología, apoyados con técnicas y herramientas de Ethical Hacking específicas, que sirva como guía para las empresas en el desarrollo e implementación de sistemas seguros, y así contrarrestar dichas vulnerabilidades; contribuir para que los ambientes informáticos en las empresas públicas y privadas en el país, cuenten con lo necesario de acuerdo a la normatividad y legislación vigente, para lograr un adecuado nivel de seguridad informática. El resultado será una investigación con el estado actual de los ataques maliciosos más comunes y el impacto que generan en las organizaciones en cuanto a robo o fuga de información, clasificación que será de acuerdo a unos criterios definidos a lo largo de la misma, apoyados en la legislación nacional.

Del proyecto se tomó dicha metodología para investigar el estado actual de los ataques maliciosos más comunes y el impacto que generan en las organizaciones en cuanto a robo o fuga de información.

Marco Contextual

Marco Institucional El lugar que hoy ocupa el edificio del PALACIO DE GOBIERNO DE NARIÑO, presenta históricamente la presencia de diferentes construcciones con diferente función social.

[3] ALONSO, David. Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base en normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional. Tesis previa a la obtención del título de Ingeniero en Informática modalidad independiente. Chía-Cundinamarca. Colombia: Universidad de la Sabana, 2014

Hasta 1581 fue la base de una vivienda particular de propiedad del presbítero Andrés Moreno Zúñiga quien la dono con el fin de convertirla en la sede del Convento de Las Conceptas, según lo refiere el historiador Sergio Elías Ortiz:

“Una vez decididos los vecinos de San Juan de Pasto a tomar la fundación del convento de Concepcionistas a su cargo, en lo primero en que pensaron fue en la ampliación y reconstrucción de una casa que para efecto dono el presbítero prebendano Andrés Moreno Zúñiga, a quien es preciso señalar como el verdadero fundador de dicho convento...”.

A continuación, la comunidad de vecinos de Pasto se dispone a interponer sus propios recursos para contar con un Convento de Religiosas:

“La necesidad de la obra no daba espera, sino antes bien urgía darles principio, pues que las doncellas principales por su falta de dote no podían casarse como su calidad lo requería y que lo que la prudencia aconsejaba en tal emergencia era meterlas a un Convento”.

Durante un año, la vivienda destinada para el Convento de religiosas de clausura sufrió remodelación y adaptación en estructura arquitectónica. Su extensión era considerable si se tiene en cuenta que para aquel entonces la construcción ocupaba más “De dos tercios de la manzana en que hoy se encuentra el edificio de la Gobernación.”

La historia lo sostiene así: “La obra de reparaciones y adaptación del edificio que dicho sea de paso, era una fábrica de construcción pesada en parte de mampostería y en parte de tierra apisonada y que ocupaba más de dos tercios de la manzana en que actualmente se levanta el edificio de la Gobernación del Departamento, quedo concluida en menos de un año, pues principalmente los trabajos en 1987 estuvo terminada a fines de septiembre de 1588, menos la ermita, que debía servir para uso público y para actos religiosos del convento la cual se concluyó 4 meses más tarde”

El 3 de octubre de 1588, se fundó el Ministerio de la Pura y Limpia Concepción de Nuestra Señora, contando por aquel entonces con 7 damas, 6 doncellas y 1 viuda. La ceremonia de clausura todavía la recuerda la historia; “El Vicario de Bracamonte puso cerrojo a las puertas y se guardó las llaves a la vista del numeroso concurro de habitantes que presencio la ceremonia en señal de que las monjas se quedaban enclaustradas”.

Es en febrero de 1864, cuando en aplicación del decreto de desamortización de bienes de manos muertas, las conceptas fueron obligadas por acciones de facto, a cambiar de domicilio, porque se había por orden superior que la edificación que ocupaban pasaría ahora a formar parte del patrimonio de la Republica”. (S.E. ORTIZ: 1929: 6L-62). Del paso de las Conceptas, quedo el recuerdo y el nombre de la calle, conocida popularmente como “La calle de las Monjas”. La construcción o el local sirvió a partir de entonces para diferentes fines. Al respecto dice Silvia Narváez que desde 1881, se había previsto que allí se levantaría un colegio, que siempre quedo solo como un proyecto.

“Como proyecto pendiente estaba el de levantar una construcción para que sirviera de sede de un colegio de señoritas. Para tal fin el gobierno tenía cedido el lote que contiene los vestigios del antiguo Convento de las Monjas”.

A finales del Siglo XIX y principios de XX, en el lote en mención, se formó una pequeña plaza de mercado con toldos y fogones al aire libre, lugar de encuentro y reunión, anexa a la Plaza de la Constitución.

En la plaza mayor de la Colonia, todavía se podía apreciar, hacia 1884, que las viviendas que enmarcaban el entorno eran: “casas porticadas” poseedoras de amplios aleros y corredores”.

En 1904, bajo la presidencia del General Rafael Reyes se erige el noveno departamento NARIÑO, en homenaje al precursor de la independencia Antonio Nariño y por efectos de la ley 1 del mes de agosto del mismo año en segregación

del antiguo departamento del Cauca. El primer gobernador de Nariño fue Julián Buchely Ayerbe, quien tomo posesión del cargo ante el doctor José María Navarrete en su calidad de Presidente del Tribunal del Sur, en la Casa de la calle 19 con carera 26, sede actual de la Casa de Cultura de Nariño, ante la situación presente de no contar en la fecha con sede propia del Gobierno Departamental.

Misión. La Gobernación de Nariño, como institución pública, está comprometida con el desarrollo regional bajo los principios de justicia social, democracia política, desarrollo humano sostenible, equidad de género, reconocimiento y protección de la diversidad étnica, respeto por derechos humanos y participación ciudadana; propiciando la concurrencia, complementariedad y subsidiaridad con las entidades territoriales de su jurisdicción y la Nación, coordinando esfuerzos con el sector público, privado y sociedad civil.

Figura 1. Gobernación de Nariño

Fuente: nariño.gov.co/inicio

Ubicación de la Entidad. El Palacio de la Gobernación de Nariño se encuentra ubicado:

Calle 19 No. 23-78 - Pasto-Nariño-Colombia**.**

Ubicación Georeferencial: Latitud: 1°12N Altitud: 2527 msnm

Horario de Atención: lunes a viernes 8:00am - 12:00m y 2:00pm - 6:00pm.

Línea gratuita de Atención: 018000949898

Pbx:(57)2 7235003- (57)2 7233600- (57)2 7232916- (57)2 7235329- (57)2 7235004- (57)2 7223846- (57)2 7235005.

Contáctenos (Correo Electrónico):contactenos@narino.gov.co

Visión. En el año 2019, El departamento de Nariño es un referente mundial de Nuevo Gobierno que se fundamenta en la participación, colaboración e innovación y avanza en la construcción de la Paz Territorial. El Cierre de Brechas Sociales y la Sostenibilidad Ambiental. Es un territorio integrado a nivel regional, nacional e internacional que trabaja por el logro de propósitos comunes y genera una gobernanza multinivel para la construcción corresponsable de derecho Humano Sostenible.[4]

Figura 2. Organigrama Gobernación de Nariño

Fuente:nariño.gov.co/inicio/index.php/gobernacion/informacion-organizacional/organigrama

[4] PAGINA WEB: Gobernación de Nariño. Disponible en: http://nariño.gov.co/inicio/

Marco Teórico

El diseño de Políticas y Procedimientos de seguridad informática y de información es el resultado de un Sistema de Gestión de Seguridad de la información el cual es para las organizaciones una herramienta que surge con el fin de concientizar a todos sus miembros sobre la importancia y la sensibilidad de la información, este Sistema permite a una entidad identificar las vulnerabilidades, amenazas y los riesgos a los que están expuestos los activos, permitiendo establecer las normas o controles adecuados para proteger y respaldar los activos garantizando la continuidad de los procesos de la organización.

Para la realización del proyecto se tuvo en cuenta las siguientes normas internacionales y teorías las cuales proporcionan la información necesaria para el cumplimiento de los objetivos de investigación.

Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se construye ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información corporativa en las empresas. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización[5].

Un SGSI es el conjunto de prácticas orientadas a garantizar la seguridad, la integridad y la confidencialidad de los datos.

Los Sistemas de Gestión de la Seguridad de la Información permiten a las organizaciones implementar políticas y procedimientos con el fin de reducir los riesgos de exposición de la información. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o

[5] Sistema de Gestión de la Seguridad de la Información. Disponible en: http://www.iso27000.es/sgsi.html#seccion2

controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Figura 3. SGSI

Fuente: www.iso27000.es

Norma ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

El eje central de ISO27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Sus objetivos son:

- ✓ Mantener una imagen excelente tanto interna, como externa (cliente-proveedor).
- ✓ Cumplimiento de la legislación vigente.
- ✓ Permear con claridad las directrices a seguir para mantener la seguridad de la información y datos,
- ✓ Identificación, análisis y mitigación de los riesgos asociados al sistema de información actual de la organización.
- ✓ Conocimiento de la importancia que tiene la información para la entidad, con el fin de armonizar la seguridad.
- ✓ Mejora procesos, procedimientos y actividades con que se desarrolla la gestión en cuanto a la información.

Dominios del Sistema de Gestión de seguridad de la Información

Los dominios seleccionados para gestionar la información e implementar el sistema de gestión de seguridad de la información fueron:

- ➢ **Políticas de la seguridad de la Información.**

Su objetivo es garantizar a la empresa el soporte y gestión necesarios para la seguridad de la información según todos los requisitos institucionales y normativos.

Se debe establecer la política según los objetivos establecidos por la empresa. Es necesario contar con el compromiso en cuanto a la seguridad de la información.

- Orientación de la dirección para la gestión de la seguridad de la información.

- **Organización de la seguridad de la información.**

El objetivo de este dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.

Para ello se debería definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades.
Para una actualización adecuada en materia de seguridad se debería contemplar la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

- Organización interna
- Dispositivos móviles y teletrabajo

- **Seguridad de los recursos humanos**

El objetivo de este dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.

- Antes de asumir el empleo
- Durante la ejecución del empleo
- Terminación y cambio de empleo

- **Gestión de Activos**

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Algunos ejemplos de activos son:

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

Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

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

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

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

- Responsabilidad por los activos
- Clasificación de la información.
- Manejo de medios

- **Seguridad Física y del Entorno**

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización esté físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud).

- Áreas seguras
- Equipos

- **Seguridad de las Operaciones**

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permite garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización.

Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.

Finalmente, se deberían verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

- Procedimientos operacionales y responsabilidades
- Protección contra códigos maliciosos

- Copias de respaldo
- Registro y seguimiento
- Control de software operacional
- Gestión de la vulnerabilidad técnica
- Consideraciones sobre auditorias de sistemas de información.

- **Adquisición, desarrollo y mantenimiento de sistemas**

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.
Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
Definir los métodos de protección de la información crítica o sensible.
Aplica a todos los sistemas informáticos, tantos desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

- Requisitos de seguridad de los sistemas de información.
- Seguridad en los procesos de desarrollo y de soporte
- Datos de prueba

- **Relaciones con los proveedores**

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.
La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

- Seguridad de la información en las relaciones con los proveedores

- Gestión de la prestación de servicios de proveedores

- **Gestión de incidentes de seguridad de la información.**

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

- Gestión de incidentes y mejoras en la seguridad de la información.

- **Aspectos de seguridad de la información de la gestión de continuidad del negocio.**

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

- Continuidad de seguridad de la información.
- Redundancias

- **Cumplimiento**

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

- Cumplimiento de requisitos legales y contractuales
- Revisiones de seguridad de la información. [6]

Norma ISO 27002

La norma ISO 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar,

[6] Norma ISO 27001/Dominios, Disponible en: http://iso27000.es/iso27002.html

implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad.

La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza, se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles.

El documento denominado política es aquel que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa.

El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas.[7]

Metodología de Gestión de Riesgos Magerit

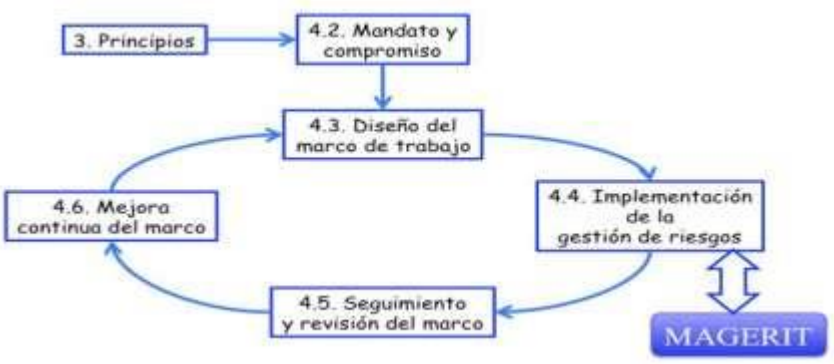
Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

[7] Norma ISO 27002. Disponible en: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista[8].

Figura 4. IS0 31000 Marco de trabajo para la gestión de Riesgos



Fuente: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wz69GdVKjIU

Marco Conceptual

Activo: Son todos los elementos que posee la Gobernación como son: los datos o información, servicios, aplicaciones (software), equipos (hardware), recursos físicos y recursos humanos, los cuales tiene algún valor para la entidad y por tanto deben protegerse.

[8] MAGERIT. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wz69GdVKjIU

Vulnerabilidad: Son las debilidades existentes en el sistema de información de la Gobernación y que pueden ser aprovechadas por una amenaza.

Riesgo: Es la probabilidad de sufrir un daño o pérdida si los activos no se protegen adecuadamente, se mide en términos de impacto y probabilidad de ocurrencia.

Confidencialidad: Indica que la información que se considera secreta no será divulgada, solo se permitirá el acceso a esta a quienes estén autorizados.

Disponibilidad: Acceso y utilización de la información por parte del personal de la Gobernación cuando lo requieran.

Integridad: Es la característica de mantener toda la información existente en la entidad de manera exacta y completa sin tener modificaciones.

Autenticidad: Corresponde a la originalidad de la información, es la acción que permite identificar la fuente de donde proceden los datos a manipular.

Trazabilidad: Habilidad del sistema para establecer quien, como y cuando se hizo a fin de detectar posibles incidentes de seguridad de la información.

Seguridad de la Información: En la Gobernación de Nariño es de vital importancia que la información esté resguardada bajo unas buenas medidas de seguridad. La seguridad de la información sirve para mantener a salvo todos los datos importantes de la entidad, desde los que pertenecen a la propia organización como los vinculados con trabajadores y clientes.

Este sistema asegura tres aspectos fundamentales: la confidencialidad, la disponibilidad y la integridad. Para llevar a cabo estas acciones se deberán establecer estrategias donde se redacten las políticas de actuación para cada uno de estos casos. También habrá que establecer el uso de las tecnologías, incluir controles de seguridad y todos los procesos que se van a llevar a cabo para detectar los riesgos a los que se puede ver expuesto el sistema. La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los

datos que se manejan dentro de la entidad y asegurar que no salgan de ese sistema establecido por la empresa.[9]

Seguridad Informática: Es el área que se enfoca en las metodologías, procesos y procedimientos para mantener salvaguardada la información y datos confidenciales de la Gobernación al interior de las herramientas informáticas. Dichos procesos se estructuran a través de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica.

Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas). Implica el proceso de proteger contra intrusos el uso de los recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

Marco Legal

El aumento de las nuevas tecnologías de la información ha propiciado la creación de un marco legal y jurídico que protege a todas las partes interesadas en el uso de estas tecnologías, el intercambio y tratamiento de la información a través de ellas. En cuanto a los delitos informáticos, cada día surgen nuevas formas de delitos que pueden afectar la seguridad de la información en las entidades.

[9] Seguridad de la información. Disponible en: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

Entre las principales leyes relacionadas con la seguridad de la información están:

Ley 1581 de 2012 protección de datos personales

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los principios y disposiciones contenidas en esta ley se aplican a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza ya sea pública o privada.[10]

Ley 527 de 1999 de comercio electrónico

Ley que aplica a todo tipo de información en forma de mensaje de datos, para los efectos de la presente ley se entenderá por:

Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, el Intercambio Electrónico de Datos y el correo electrónico.

Comercio electrónico. Abarca todo lo relacionado con lo comercial a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Comprende las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial, operaciones financieras, bursátiles, seguros de construcción, consultoría, ingeniería; servicios públicos, transporte de mercancías y pasajeros.

[10] Ley 1581 de 2012 Decreto 1377 de 2013. Colombia Digital, agosto 29, 2013, Disponible en: http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

Firma digital. Se entiende como el valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático, vinculado a la clave del creador, garantiza la transferencia de archivos electrónicos.

Entidad de Certificación. Entidad autorizada para emitir certificados electrónicos en relación con las firmas digitales de las personas.

Intercambio Electrónico de Datos. La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.

Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma de mensajes de datos.[11]

Ley 23 de 1982 Derechos de Autor

La ley colombiana otorga al Derecho de Autor sobre todas las formas en que se puede expresar las ideas, no requiere ningún registro y perdura durante toda la vida del autor, más 80 años después de su muerte, después de lo cual pasa a ser de dominio público. El registro de la obra ante la Dirección Nacional del Derecho de Autor tiene como finalidad brindar mayor seguridad a los titulares del derecho.

En el caso del Software, la legislación colombiana lo asimila a la escritura de una obra literaria, permitiendo que el código fuente de un programa esté cubierto por la ley de Derechos de Autor.[12]

Ley 1273 de 2009

Con la que se modifica el código penal, se crea un nuevo bien jurídico denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de información y de comunicaciones".[13]

---

[11] Ley 527 de 1999, agosto 18, El Congreso de Colombia, Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[12] Ley 23 de 1982, enero 01, El Congreso de Colombia, Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431

[13] Ley 1273 de 2009, Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

Diseño Metodológico

Tipo de investigación

La investigación fue descriptiva ya que se abordó la seguridad informática y las principales características que tiene la Gobernación de Nariño; de igual manera fue una investigación aplicada, orientada hacia la gestión de sistemas y en busca de generación de soluciones a los problemas que se encontraron en la entidad. Además, pudo caracterizarse como propositiva en vista de que se generó como producto una propuesta de políticas y procedimientos de seguridad informática y de Información.

Enfoque de Investigación

Según el autor Sampieri[14] la investigación cuantitativa usó la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías. Además, establece que se utiliza secundariamente la recolección de datos fundamentada en la medición, posteriormente se llevó a cabo el análisis de los datos y se contestaron las preguntas de investigación, de ésta manera prueba las hipótesis establecidas previamente, confiando en la medición numérica, el conteo, y en el uso de la estadística para establecer con exactitud patrones en una población

Por lo tanto, esta investigación se llevó a cabo bajo el enfoque cuantitativo considerando que se estudiaron variables susceptibles de cuantificación y medición con indicadores objetivos.

[14] Sampieri (1991: 5), “usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías”.

Población y Muestra

Se estudió todo el personal de la Gobernación de Nariño y de allí se sacó una muestra que fueron los funcionarios de la Secretaría TIC Innovación y Gobierno Abierto, que están involucrados con la administración o seguridad informática, además de los administradores de los diferentes aplicativos y base de datos existentes en la entidad y usuarios de los diversos sistemas de información.

La muestra se sacó de manera intencional porque se seleccionó a los directivos y usuarios de cada dependencia quienes administran aplicativos, bases de datos y sistemas de información.

Fuentes de recolección de información

Las fuentes de información que se tuvieron en cuenta para la realización del proyecto se pueden catalogar en información primaria y secundaria.

- ✓ **Fuentes de información primaria**. Las fuentes primarias están constituidas por la información original suministrada por los profesionales administradores de aplicaciones y Bases de Datos de la entidad; hechos surgidos a la seguridad informática y a la infraestructura de la Gobernación de Nariño.
- ✓ **Fuentes de información secundaria**. La información secundaria es toda la información documental que orienta al análisis y evaluación de la seguridad informática y que se encuentra consignada en documentos como: normas: NTC- ISO-IEC-27001, NTC- ISO-IEC-27002 y Metodología MAGERIT, documentos de la Gobernación y listas de chequeo.

Técnicas de análisis de datos

- Entrevista: para obtener información relevante para el proyecto se utilizó la entrevista de modelo conversacional, por ser una técnica eficaz para obtener datos relevantes y significativos, utilizando una entrevista no estructurada con el fin de obtener una opinión personalizada de los

Profesionales Universitarios quienes eran los encargados de la administración de las aplicaciones, base de datos y comunicaciones.

- Encuestas: Para determinar vulnerabilidades, conductas y conocimiento que tenían los usuarios de las políticas de seguridad informática, se aplicó una encuesta que fue contestada por el personal de la Secretaría TIC.
- Observación: Por otra parte, en la realización del proyecto se utilizó la observación para registrar patrones de conducta de los usuarios y del sistema informático.
- Revisión documental: Para ello se revisó los documentos existentes que brindan soporte a la seguridad informática y el control de los mismos como son: normas NTC-ISO-IEC- 27001, NTC-ISO-IEC-27002, Metodología MAGERIT y documentación de La Gobernación de Nariño que soportan el "SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN".
- Herramientas: Para realizar la recolección de información se utilizó grabadora, herramientas de Google drive y para el análisis herramientas de office (Excel).

Procesamiento de la Información

Metodología para el análisis y el diseño

Para el diseño de las Políticas y Procedimientos de Seguridad informática y de información, fue recomendable seguir una secuencia, con el fin de poder organizar las actividades para el desarrollo del proyecto, siempre teniendo presente el conjunto de métodos y técnicas que permitan llevar a cabo un SGSI de calidad.

Para el desarrollo del proyecto “Diseño de Políticas y Procedimientos de Seguridad Informática y de Información utilizando la norma ISO 27001/2013 y MAGERIT versión 3.0 para la Gobernación de Nariño”, se tomó como guía el método denominado Ciclo PHVA.

Para la implantación de un sistema de Gestión de la seguridad de la información, se requirió del desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PHVA, Planificar, hacer, verificar y actuar es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo permite en las organizaciones una mejora integral de la competitividad, de los productos y servicios, mejorando de forma continua la calidad, reduciendo costos, optimizando productividad, reduciendo precios, incrementando la participación del mercado e incrementando la rentabilidad de la organización.

Figura 5 Ciclo PHVA

Fuente: El Autor

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 la revaluación de las medidas de prevención, corrección y evaluación, mantuvo 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.

Planear

En esta etapa se enmarcó todo el proceso de análisis de la situación en que actualmente se encontraba la entidad respecto a los mecanismos de seguridad implementados. Así mismo en la etapa de planeación se organizan fases relevantes como fueron:

- Establecer el compromiso con los directivos de la Gobernación 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 evalúa los riesgos, se tratan y se seleccionan los controles a implementar.

Hacer

En esta etapa se implementaron todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de entidad.

Verificar

Consiste en efectuar el control de todos los procedimientos implementados en el SGSI. En este sentido, se realizaron exámenes periódicos para asegurar la eficacia del SGSI implementado, se revisaron los niveles de riesgos aceptables y residuales y periódicamente auditorías internas para el SGSI.

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.[15]

[15] CICLO PHVA. Disponible en:

Análisis de la encuesta realizada a los empleados de la secretaria de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño.

Luego de analizar las encuestas realizadas a los empleados de la Secretaria TIC, Innovación y Gobierno Abierto a través de varias preguntas que están encaminadas a evaluar aspectos como: Gestión de activos informáticos, Incidentes presentados, funcionamiento de los sistemas de información, manejo de contraseñas, seguridad del personal, funcionamiento administrativo dentro de la secretaría y medidas de políticas de seguridad actualmente por la Gobernación de Nariño, se pudieron exponer las siguientes conclusiones:

- **Con respecto a la Organización y Administración de la secretaria de TIC de la Gobernación de Nariño:**
  - El área no contaba con una estructura organizacional
  - Ausencia de manual de funciones para cada puesto de trabajo dentro del área.

Sugerencias

- Establecer una estructura organizacional en la SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO DE LA GOBERNACIÓN DE NARIÑO.
- Establecer un manual de funciones para cada uno de los cargos que desempeña cada empleado en la secretaria Tic.

Efectos y/o implicaciones probables por las deficiencias

- Por falta de una estructura organizacional la organización se veía afectada a estar en riesgo de pérdida de información, de documentos, datos digitados, por descuido de los que manejan los equipos de cómputo.
- Si no se obtenía un manual de funcionamiento para cada uno de los empleados la Gobernación se pudo ver afectada debido a que cada uno de

---

http://www.iso27000.es/download/doc_sgsi_all.pdf

los funcionarios no tenían ni la mínima idea de cumplir sus funciones para cada uno de los cargos y pueden intervenir en otras áreas que no les corresponde, esto obliga a que posiblemente haya pérdida de documentación o datos y puede ser muy difícil saber quién ocasiono tal pérdida.

- **Respecto a la seguridad física y lógica:**
  - No existía una vigilancia estricta en la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño por personal de seguridad dedicado a este sector.
  - No existía un puesto o cargo específico para la función de seguridad Informática.
  - Falta de alarmas y cámaras de seguridad.

Sugerencias

A los efectos de minimizar los riesgos descritos, se sugirió:

- Establecer guardia de seguridad, durante horarios no habilitados para el ingreso a la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño
- Instalar alarmas y cámaras como sugerencia de seguridad.

Efectos y/o implicaciones probables por las deficiencias

- Si no hay un guardia de seguridad en la Secretaría de TIC en horarios inhabilitados personas con mala intención podrían infiltrarse y robar información importante incluyendo los equipos de cómputo.
- Si no existía una persona responsable de la seguridad informática que proteja los recursos de las amenazas, estos se veían afectados a estar en riesgo de pérdida de información.
- Por falta de alarmas y cámaras de seguridad era más fácil la infiltración de personas y la pedida de los activos en la Secretaría de TIC.

- **Respecto al plan de prevención y contingencia:**
  - Ausencia de un Plan de Contingencia debidamente formalizado en la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño.
  - No existían normas y procedimientos que indicaran las tareas, manuales e informáticas que eran necesarias para realizar y recuperar la capacidad de procesamiento ante un eventual problema (desperfectos de equipos, incendios, cortes de energía con más de una hora), y que determinaran los niveles de participación y responsabilidades del área de sistemas y de los usuarios.
  - Ausencia de un plan de prevención en desastres en la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño.

Sugerencias

- Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operatoria normal de la organización y establecer los responsables de cada sistema.
- Efectuar pruebas simuladas en forma periódica a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.

1. SGSI PARA LA GOBERNACIÓN DE NARIÑO

De acuerdo al Ciclo (PHVA) de SGSI, donde se realizaron una serie de pasos y procesos, a continuación, se desarrollaron cada una de las etapas así:

1.1 ESTABLECER EL SGSI

1.1.1 Alcance:

Mejorar la calidad de los servicios que presta la Secretaria de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño, en la protección de sus recursos Informáticos y tecnológicos creando políticas para gestionar de forma correcta y satisfactoria la seguridad de la información donde todo el personal encargado del área de sistemas tenga conocimientos sobre cómo aplicar y cumplir todos los procesos del SGSI.

1.1.2 Política del Sistema de Gestión:

La Secretaría de TIC, de la Gobernación de Nariño pretendía que toda la información y los activos informáticos manejados por la entidad se encontraran debidamente protegidos con el fin de preservar y salvaguardar su confidencialidad, disponibilidad e integridad.

1.1.3 Metodología de Evaluación de Riesgo:

Para el desarrollo del proyecto se empleó la Metodología MAGERIT para el análisis y gestión de los riesgos por las siguientes razones:

- ✓ MAGERIT permite analizar el impacto que puede tener para una entidad la violación de la seguridad de la información, buscando identificar las

- ✓ amenazas y vulnerabilidades presentes en esta.
- ✓ Presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos.
- ✓ MAGERIT tiene una visión estratégica global de la Seguridad de los Sistemas de Información ISO 27001.

La metodología MAGERIT sigue los siguientes pasos:

Tabla 2 Pasos Metodología MAGERIT

Secuencia	Procesos
Paso 1	Inventario y Valoración de Activos
Paso 2	Identificación y Valoración de Amenazas y Vulnerabilidades
Paso 3	Medición del impacto
Paso 4	Medición del Riesgo

Fuente: La presente investigación

1.2 Análisis de Riesgos de la Secretaria de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño.

Hoy en día toda organización se encuentra expuesta a riesgos informáticos, debido a que no existe un entorno 100% seguro. Por tal motivo toda entidad deberá estar alerta a cualquier cambio o situación extraña que pueda afectar negativamente a un activo, a una dependencia o a toda su organización.

Esta etapa se constituyó en el núcleo central de MAGERIT, y su correcta aplicación de condicionar la validez y utilidad de todo el proyecto.

1.2.1 Identificación de Activos

Los activos son bienes tangibles e intangibles necesarios que posee la Entidad para su buen desempeño laboral.

1.2.1.1 Activos Esenciales: Información que se maneja y los servicios que presta.

Tabla 3 Activos Esenciales

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[vr]	Datos vitales (registros de la organización)	[Sistema Información]	Sistema de Información equipamiento hardware de la Gobernación
			Sistema de Información proyectos de la Gobernación
		[Sistema Información Bases de Datos]	Sistema de Información correo Institucional
			Sistema de Información plataformas web de la Gobernación
			Sistema de Información software a la medida de la Gobernación
			Sistema de Información equipamiento hardware de la Gobernación
			Sistema de Información proyectos de la Gobernación
[service]	Servicio	[Servicio Interno]	Correo electrónico institucional e Intranet

Fuente: La presente investigación

1.2.1.2 [D] Datos/Información: Los datos son el corazón que permite a la entidad prestar sus servicios.

Tabla 4 Datos/Información

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[files]	Ficheros de datos	[Archivo Informes]	Archivo de informes mensuales entregados por la Gobernación
		[Archivo Procesos Secretaria]	Archivo de certificaciones, actas, estudios previos y oficios desarrollados por la secretaria de TIC, Innovación y Gobierno abierto
		[Archivo Contratos]	Archivo de los contratos de los funcionarios TIC
		[Archivo GANAPAE]	Archivo de alertas, estadísticas e información personal de los niños GANAPAE
		[Archivo Presupuesto]	Archivo de presupuesto de los proyectos de Gobierno Abierto
[backup]	Copias de respaldo	[Archivo Copias de Respaldo]	Archivo de copias de seguridad de la Información
[password]	Credenciales	[Contraseñas Empleados]	Contraseñas de acceso de empleados

Tabla 4. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[source]	Código fuente	[Código fuente aplicativos Gobernación	Código fuente portal web de la Gobernación de Nariño, Portales

Fuente: La presente investigación

1.2.1.3 [S] Inventario de Servicios: Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

Tabla 5. Servicios

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[pub]	Al público en general (sin relación contractual)	[Servicio al público]	Servicios de proyectos de ciencia, tecnología e innovación
			Servicios de proyectos de recursos propios
			Servicios de proyectos vive digital
[ext]	A usuarios externos (bajo una relación contractual)	[Servicio Externo]	Servicio de cierre de brecha digital de primera y segunda generación
			Servicio de administración de la información y actividades de todas las secretarias Gobernación
			Servicio de apoyo en contrataciones/adquisición de software/hardware

Tabla 5 (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[ext]	A usuarios externos (bajo una relación contractual)	[Servicio Externo]	Servicios de validar/estructurar/consolidar/ingresar información al SEPAD
			Servicio técnico y de software equipos de computo
			Servicio de brindar información entidades minTIC
			Servicio de garantizar acceso a la información
[int]	Interno (usuarios y medios de la propia organización)	[Servicio Interno]	Servicio administración y soporte de sistemas de información
			Servicio de administración y contratación de servicios
			Servicio de administración servidores, máquinas virtuales, dispositivos cisco y mikrotik de la Gobernación
			Servicio de atención jurídica interna
			Servicio de manejo de la ficha MGA
			Servicio de desarrollo y mantenimiento plataformas Gobernación de Nariño
[www]	World wide web	[Servicio Internet]	Servicio de internet al que pueden acceder los empleados.
[email]	Correo electrónico	[Servicio Correo]	Manejo de correos electrónicos(entidad)

Tabla 5 (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[file]	Almacenamiento de ficheros	[S_A_Bases de datos]	Servicio de almacenamiento de información en los servidores de bases de datos.

Fuente: La presente investigación

1.2.1.4 [SW] Aplicaciones informáticas (Software): (Programas, Aplicativos, desarrollos, etc.)

Tabla 6 Aplicaciones informáticas

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[prp]	Desarrollo propio (in house)	[software propio]	Software GANA Gobernación
			Software Kiosco Box
			Software de justicia abierta
			Software SEPAD
			Software sistema de aplicaciones Intranet
			Software plataforma PDA
			Software BPID
			Software Portal Web Gobernación de Nariño.
[sub]	Desarrollo a medida (subcontratado)	[software a la medida]	Software SYSMAN
			Software SISCAR
[std]	Estándar (of the shelf)	[software nacional]	Software plataformas educativas
			Software SIAG, SIC Y SCHI

Tabla 6. (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[std]	Estándar (of the shelf)	[software nacional]	Software Colombia compra eficiente
			Software portal daros abiertos nacional
			Software portal MINTIC
			Software GESPROY
[browser]	Navegador Web	[Navegadores]	Navegadores Google Chrome y Mozilla Firefox
[app]	Servidor de aplicaciones	[Server Aplicación]	Servidores de Aplicaciones
[email server]	Servidor de correo electrónico	[Server Correo]	Servidor de Correo Electrónico
[file]	servidor de ficheros	[Server Ficheros]	Servidor de Ficheros
[dbms]	Sistema de gestión de bases de datos	[SG BaseDatos]	SQL server, Oracle, postgreSQL, MySQL
[Office]	Ofimática	[Office]	Office: 2010, 2013 y 2016
			Libre office(6.0.4; 5.4.7)
[av]	Antivirus	[Antivirus]	AVAST Endpoint Protection Version 8.0.1609 y windows defender
[os]	Sistema operativo	[OS Win]	Sistema operativo Windows 8 y Windows 10.
			Sistema operativo Linux

Tabla 6 (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[hipervisor]	Gestor de máquinas virtuales	[máquinas virtuales]	Máquina virtual Virtualbox
[backup]	Sistema de backup	[backup]	Sistema de backup en el servidor
[other]	Otros software	[software varios]	Software utilitarios
			Software AIDA64
			Software IDE´s para desarrollo para Windows y Linux
			Software de lenguajes de programación para Windows y Linux

Fuente: La presente investigación

1.2.1.5 [HW] Equipos informáticos (Hardware): Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad.

Tabla 7 Hardware

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[host]	Grandes equipos (host)	[Servicio Aplicaciones]	Servidor Aplicaciones
		[Servicio Data Base]	Servidor para copias de seguridad
[mid]	Equipos medios	[PC Equipos de Escritorio]	Computadores de escritorio
[pc]	Informática personal	[PC portátiles]	Computadores Portátiles

Tabla 7 (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[vhost]	Equipos virtuales (máquinas virtuales)	[máquinas virtuales Equipos virtual]	Máquinas virtuales con servicios internos y externos
[print]	Medios de impresión	[Equipamiento Impresoras]	Impresoras
[scan]	Escáner	[Servicio Scan]	Escáner
[switch]	conmutadores	[switch conmutadores]	conmutadores
[router]	Enrutadores	[Router enrutadores]	Dispositivos cisco y mikrotik
[other]	rack	[rack]	rack

Fuente: La presente investigación

1.2.1.6 [COM] Redes de Comunicación: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

Tabla 8. Redes de Comunicaciones

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[wifi]	Wifi	[Wifi]	Red Inalámbrica
[LAN]	Red local	[Red Local]	Red local
[Internet]	Internet	[Internet]	Internet
[Intranet]	Intranet	[intranet]	Intranet

Fuente: La presente investigación

1.2.1.7 [MEDIA] Soportes de Información. Electrónico/No Electrónico:
Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Tabla 9 Soportes de Información

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[disk]	Discos	[Almacenamiento CD]	Almacenamientos en Disco Duro
[USB]	Memorias USB	[Almacenamiento Memorias]	Almacenamiento en Memorias
[dvd]	DVD	[A_DVD]	Almacenamiento en DVD
[printed]	Material impreso	[Car]	Cajas con sus carpetas debidamente archivadas (Proyectos, procesos, correspondencia, contratos, reportes etc.)
		[archivadores]	Archivadores con sus carpetas debidamente archivadas (Proyectos, procesos, correspondencia, contratos, reportes etc.)
		[Informes]	Reportes de informes de todas las Secretarias
		[varios]	Carpetas varias

Fuente: La presente investigación

1.2.1.8 [AUX] Equipamiento Auxiliar: otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Tabla 10 Equipamiento auxiliar

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[power]	Fuentes de Alimentación	[Power Fuente]	Reguladores

Tabla 10 (Continuación)

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[ups]	Sistemas de Alimentación ininterrumpida	[Ups sala de comunicaciones]	UPS sala de comunicaciones
[Ac]	Equipos de Climatización	[Equipos Cli]	Aire Acondicionado en la sala de Comunicaciones
[wire]	Cable Eléctrico	[Cable Eléctrico]	Cable Eléctrico
[fiber]	Fibra Óptica	[Fibra óptica]	Transmisión de comunicación
[suplly]	Suministros Esenciales	[Suministro Esenciales]	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.

Fuente: La presente investigación

1.2.1.9 [L] Instalaciones: Lugares donde se hospedan los sistemas de información y comunicaciones.

Tabla 11 Instalaciones

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[building]	Edificio	[Edificio Secretaria TIC, Innovación y Gobierno Abierto]	Edificio Gobernación de Nariño

Fuente: La presente investigación

1.2.1.10 [P] Personal: Personas relacionadas con los sistemas de información.

Tabla 12 Personal

Código Clases de Activo Magerit	Nombre de la Clase de Activo Magerit	Código Activo de la Entidad	Nombre activo de la Entidad
[ui]	Usuarios internos	[personal interno]	Profesional Universitario
			Secretario Secretaría TIC, Innovación y Gobierno Abierto
			Contratistas
			Carrera Administrativa

Fuente: La presente investigación

1.2.2 Valoración de Activos

Todos los activos de las entidades son relevantes para las empresas. Esto significa que si alguno de ellos es atacado genera un tipo de impacto. A continuación, se realizó una valoración cuantitativa de los activos más importantes dentro de la Secretaría de TIC, teniendo presente las dimensiones: Confidencialidad, Integridad, Disponibilidad y de acuerdo a la siguiente tabla:

Tabla 13 Criterios de Valoración

VALOR		CRITERIO
5	Muy Alto	Daño muy grave
4	Alto	Daño grave
3	Medio	Daño importante
2	Bajo	Daño menor
1	Muy Bajo	Irrelevante a efectos prácticos

Fuente: MAGERIT- versión 3.0

Tabla 14 Valoración Cuantitativa de los Principales Activos de Información de la Secretaria TIC, Innovación y Gobierno Abierto.

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO		CUSTODIO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
STIC -01	Bases de Datos proyectos de la Gobernación	D	Uso Interno	Normal	Alta	**Medio**	**3**	Secretario TIC, Innovación y Gobierno y Abierto	Profesional Universitario
STIC -02	Código fuente portal web de la Gobernación de Nariño, Portales	D	Confidencial	Sensible	Muy Alta	**Muy Alta**	**5**	Secretario TIC, Innovación y Gobierno y Abierto	Área de apoyo TI
STIC -03	Correo electrónico Institucional	S	Uso Interno	Sensible	Alta	**Alta**	**4**	Secretario TIC, Innovación y Gobierno y Abierto	Área de soluciones TI
STIC -04	Servicio técnico y de software equipos de computo	S	Uso Interno	Normal	Alta	**Medio**	**3**	Secretario TIC, Innovación y Gobierno y Abierto	Soporte técnico
STIC -05	Servicio de administración, desarrollo y soporte de sistemas de información y plataformas gobernación de Nariño	S	Uso Interno	Sensible	Alta	**Alto**	4	Secretario TIC, Innovación y Gobierno y Abierto	Área de soluciones TI

Tabla 14 (Continuación)

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO		CUSTODIO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
STIC -06	Servicio de administración servidores, máquinas virtuales, dispositivos cisco y mikrotik de la Gobernación	S	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Secretario TIC, Innovación y Gobierno y Abierto	Soporte técnico
STIC -07	Software sistema de aplicaciones Intranet	SW	Uso Interno	Sensible	Alta	**Alto**	**4**	Secretario TIC, Innovación y Gobierno y Abierto	Apoyo TI
STIC-08	Sistema de Backup en el servidor.	SW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico
STIC -09	Software Portal Web Gobernación de Nariño	SW	Uso publico	Sensible	Alta	**Alto**	**4**	Secretario TIC, Innovación y Gobierno y Abierto	Área de soluciones TI
STIC -10	Software SYSMAN	SW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Secretario TIC, Innovación y Gobierno y Abierto	Profesional Universitario

Tabla 14 (Continuación)

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO		CUSTODIO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
STIC -11	Software SISCAR	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	Secretario TIC, Innovación y Gobierno y Abierto	Área de Apoyo TI
STIC -12	Servidores NS1 Y NS2	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico
STIC -13	Computadores de Escritorio	HW	Uso Interno	Sensible	Alta	Alto	4	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico
STIC -14	Computadores Portátiles	HW	Uso Interno	Sensible	Alta	Alto	4	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico
STIC -15	Impresoras	HW	Uso Interno	Normal	Media	Medio	3	Secretario TIC, Innovación y Gobierno y Abierto	Servicio tercerizado
STIC -16	Escáner	HW	Uso Interno	Normal	Media	Medio	3	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico
STIC -17	Red inalámbrica y local	COM	Uso Interno	Normal	Media	Medio	3	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico

Tabla 14 (Continuación)

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO		CUSTODIO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
STIC -18	UPS	AUX	Uso interno	Baja	Media Baja	**Bajo**	2	Secretario TIC, Innovación y Gobierno y Abierto	Servicios generales
STIC -19	Sala de Comunicaciones	L	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**	Secretario TIC, Innovación y Gobierno y Abierto	Soporte Técnico
STIC -20	Oficina Secretaria TIC, Innovación y Gobierno Abierto	L	Uso Interno	Sensible	Alta	**Alto**	4	Secretario TIC, Innovación y Gobierno y Abierto	Gobernación de Nariño
STIC -21	Personal TIC	P	Uso Interno	Normal	Media	**Medio**	3	-	-

Fuente: La presente investigación

1.2.3 Identificación de Amenazas

Luego de haber realizado la valoración de los principales activos se procedió a realizar la valoración de las amenazas a las que están expuestos dichos activos de la Secretaría de TIC, Innovación y Gobierno abierto.

A continuación, se observa las tablas de dimensiones de seguridad y las amenazas que se pueden presentar.

Tabla 15 Dimensiones de Seguridad según MAGERIT

Dimensiones de Seguridad a valorar	Identificación
Autenticidad	**A**
Confidencialidad	**C**
Integridad	**I**
Disponibilidad	**D**
Trazabilidad	**T**

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Tabla 16 Tipos de Amenazas

Identificación de las Amenazas	
[N]	Desastres naturales
[I]	De Origen Industrial
[E]	Errores y fallos no intencionados
[A]	Ataques intencionados

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Los objetivos planteados en este paso son:

- ✓ Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.
- ✓ Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

- **Frecuencia o Probabilidad de Ocurrencia:** Se refiere a los eventos que se producen en un tiempo determinado. Los valores tomados para determinar la frecuencia se muestran a continuación.

Tabla 17 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: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- **Impacto o Degradación:** Cuan perjudicado resultaría el valor del activo al materializarse las amenazas.

Tabla 18 Escala de Rango Porcentual de Impacto

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

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

A continuación, se evidencia la valoración de las amenazas de los principales activos con relación a la probabilidad de ocurrencia y la degradación que sufrirán estos en cada una de las dimensiones de seguridad.

1.2.3.1 Relación de amenazas por desastres naturales por activo identificando su frecuencia e impacto

Tabla 19 Identificación de Amenazas por Desastres Naturales

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[N.1] FUEGO	[HW_COMPUTADORES DE ESCRITORIO]	5				MA	
	[HW_COMPUTADORES PORTÁTIL]	5				MA	
	[HW_IMPRESORAS]	5				MA	
	[HW_ESCANER]	5				MA	
	[HW_SERVIDORES NS1 Y NS2]	5				MA	
	[AUX_UPS]	5				A	
	[L_SALA DE COMUNICACIONES]	5				M	
	[L_OFICINA SECRETARIA TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	5				M	
[N.2] DAÑOS POR AGUA	[HW_COMPUTADORES DE ESCRITORIO]	5				MA	
	[HW_COMPUTADORES PORTÁTIL]	5				MA	
	[HW_IMPRESORAS]	5				MA	
	[HW_SERVIDORES NS1 Y NS2]	5				MA	
	[AUX_UPS]	5				A	
	[L_SALA DE COMUNICACIONES]	5				M	
	[L_OFICINA SECRETARIA TIC]	5				M	
[N.7] DESASTRES NATURALES. FENÓMENO SÍSMICO	[HW_COMPUTADORES DE ESCRITORIO]	5				MA	
	[HW_COMPUTADORES PORTÁTIL]	5				MA	
	[HW_IMPRESORAS]	5				MA	
	[HW_ESCANER]	5				MA	
	[HW_SERVIDORES NS1 Y NS2]	5				MA	

Tabla 19 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[N.7] DESASTRES NATURALES. FENÓMENO SÍSMICO	[L_SALA DE COMUNICACIONES]	5				M	
	[L_OFICINA SECRETARIA TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	5				M	
[N8] DESASTRES NATURALES. FENÓMENO DE ORIGEN VOLCÁNICO	[HW_COMPUTADORES DE ESCRITORIO]	5				MA	
	[HW_COMPUTADORES PORTÁTIL]	5				MA	
	[HW_IMPRESORAS]	5				MA	
	[HW_SERVIDORES NS1 Y NS2]	5				MA	
	[AUX_UPS]	5				A	
	[L_SALA DE COMUNICACIONES]	5				M	
	[L_OFICINA SECRETARIA TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	5				M	

Fuente: La presente investigación

1.2.3.2 Relación de amenazas de origen industrial por activo identificando su frecuencia e impacto

Tabla 20 Identificación de Amenazas de Origen Industrial

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[I.1] FUEGO	[HW_COMPUTADORES DE ESCRITORIO]	5				MA	
	[HW_COMPUTADORES PORTÁTIL]	5				MA	
	[HW_IMPRESORAS]	5				MA	

Tabla 20 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[I.1] FUEGO	[HW_SERVIDORES NS1 Y NS2]	5				MA	
	[AUX_UPS]	5				MA	
	[L_SALA DE COMUNICACIONES]	5				A	
	[L_OFICINA SECRETARIA TIC, INNOVACIÓN Y GOBIERNO A]	5				M	
[I.2] DAÑOS POR AGUA	[HW_COMPUTADORES DE ESCRITORIO]	5				MA	
	[HW_COMPUTADORES PORTÁTIL]	5				MA	
	[HW_IMPRESORAS]	5				MA	
	[HW_ESCANER]	5				MA	
	[HW_SERVIDORES NS1 Y NS2]	5				MA	
	[AUX_UPS]	5				MA	
	[L_SALA DE COMUNICACIONES]	5				A	
	[L_OFICINA SECRETARIA TIC, INNOVACIÓN Y GOBIERNO A]	5				M	
[I.3] CONTAMINACIÓN MECÁNICA	[HW_COMPUTADORES DE ESCRITORIO]	10				M	
	[HW_COMPUTADORES PORTÁTIL]	10				M	
	[HW_IMPRESORAS]	10				M	
	[HW_ESCANER]	10				M	
	[HW_SERVIDORES NS1 Y NS2]	10				M	
	[AUX_UPS]	10				B	
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[HW_COMPUTADORES DE ESCRITORIO]	10				MA	
	[HW_COMPUTADORES PORTÁTIL]	10				MA	
	[HW_IMPRESORAS]	10				MA	

Tabla 20 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[I.4] CONTAMINACIÓN ELECTROMAGNÉTICA	[HW_SERVIDORES NS1 Y NS2]	10				MA	
	[AUX_UPS]	10				MA	
[I.5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[SW_SISTEMA DE APLICACIONES INTRANET]	50				MA	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	50				MA	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	50				MA	
	[SW_SYSMAN]	50				MA	
	[SW_SISCAR]	10				MA	
	[HW_COMPUTADORES DE ESCRITORIO]	10				MA	
	[HW_COMPUTADORES PORTÁTIL]	10				MA	
	[HW_IMPRESORAS]	10				MA	
	[HW_ESCANER]	10				MA	
	[HW_SERVIDORES NS1 Y NS2]	10				MA	
	[AUX_UPS]	5				B	
[I.6] CORTE SUMINISTRO ELÉCTRICO	[HW_COMPUTADORES DE ESCRITORIO]	10				MA	
	[HW_COMPUTADORES PORTÁTIL]	10				A	
	[HW_IMPRESORAS]	10				MA	
	[HW_ESCANER]	10				MA	
	[HW_SERVIDORES NS1 Y NS2]	10				MA	
	[AUX_UPS]	10				MB	
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[HW_COMPUTADORES DE ESCRITORIO]	10				A	
	[HW_COMPUTADORES PORTÁTIL]	10				A	
	[HW_IMPRESORAS]	10				A	

Tabla 20 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[HW_ESCANER]	10				A	
	[HW_SERVIDORES NS1 Y NS2]	10				A	
	[AUX_UPS]	10				M	
[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[COM_WIFI]	50				MA	
	[COM_LOCAL]	50				MA	
[I.9] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	[AUX_UPS]	10				M	

Fuente: La presente investigación

1.2.3.3 Relación de amenazas de errores y fallos no intencionados por activo identificando su frecuencia e impacto.

Tabla 21 Identificación de Amenazas Errores y Fallos No Intencionados

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.1] ERRORES DE LOS USUARIOS	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10		A	A	A	
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	50		M	A	A	
	[S_MANEJO DE CORREO ELECTRÓNICO ENTIDAD]	50		A	M	B	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10		B	A	B	

Tabla 21 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.1] ERRORES DE LOS USUARIOS	[ADMINISTRACIÓN DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10		B	A	B	
	[ADMINISTRACIÓN SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK]	10		A	A	B	
	[SW_SISTEMA DE APLICACIONES INTRANET]	50		M	A	B	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		A	A	A	
[E.2] ERRORES DEL ADMINISTRADOR	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10		M	A	A	
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10		B	A	A	
	[S_MANEJO CORREO ELECTRÓNICO ENTIDAD]	5		A	A	M	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	5		B	A	B	
	[ADMINISTRACIÓN DESARROLLO/SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	5		B	A	B	
	[ADMINISTRACIÓN SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK]	5		M	A	B	
	[SW SISTEMA DE APLICACIONES INTRANET]	5		B	A	A	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	5		A	A	A	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	5		A	MA	MA	
	[SW_SYSMAN]	5		A	MA	MA	
	[SW_SISCAR]	5		A	A	A	
	[HW_COMPUTADORES DE ESCRITORIO]	5		A	A	A	
	[HW_COMPUTADORES PORTÁTIL]	5		MB	MB	M	
	[HW_IMPRESORAS]	5		MB	MB	M	
	[HW_ESCANER]	5		MB	MB	M	

Tabla 21 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.2] ERRORES DEL ADMINISTRADOR	[HW_SERVIDORES NS1 Y NS2]	5		B	MA	A	
	[COM_WIFI]	5		B	B	MA	
	[COM_LOCAL]	5		B	B	MA	
[E.7] DEFICIENCIAS EN LA ORGANIZACIÓN	[P_PERSONAL SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	5				MA	
[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[SW SISTEMA DE APLICACIONES INTRANET]	70		M	M	A	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	70		M	M	A	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	70		A	M	MA	
	[SW_SYSMAN]	70		A	M	MA	
	[SW_SISCAR]	70		M	M	A	
[E.9] ERRORES DE [RE-] ENCAMINAMIENTO	[CORREO ELECTRÓNICO ENTIDAD]	10		A			
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	5		B			
	[ADMINISTRACIÓN DESARROLLO/SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	5		M			
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	5		M			
	[SW SISTEMA DE APLICACIONES INTRANET]	5		M			
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	5		M			
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	5		A			
	[SW_SYSMAN]	5		A			
	[SW_SISCAR]	5		B			
	[COM_WIFI]	5		M			

Tabla 21 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.9] ERRORES DE [RE-] ENCAMINAMIENTO	[COM_LOCAL]	5		M			
[E.15] ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10				A	
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10				A	
[E.18] DESTRUCCIÓN DE INFORMACIÓN	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10				MA	
	[D_CODIGO FUENTE PORTAL WEB GOBERNACIÓN, PORTALES]	10				A	
	[SW SISTEMA DE APLICACIONES INTRANET]	10				A	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10				A	
	[SW_PORTAL WEB GOBERNACIÓN]	10				A	
	[SW_SYSMAN]	10				A	
	[SW_SISCAR]	10				A	
[E.19] FUGAS DE INFORMACIÓN	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10		A			
	[D_CODIGO FUENTE PORTAL WEB GOBERNACIÓN, PORTALES]	10		A			
	[S_CORREO ELECTRÓNICO ENTIDAD]	10		M			
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10		MB			
	[S_ADMINISTRACION DESARROLLO/SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10		M			

Tabla 21 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.19] FUGAS DE INFORMACIÓN	[S_ ADMINISTRACIÓN SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10		M			
	[SW SISTEMA DE APLICACIONES INTRANET]	10		A			
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		M			
	[SW_PORTAL WEB GOBERNACIÓN]	10		A			
	[SW_SYSMAN]	10		A			
	[SW_SISCAR]	10		A			
	[P_PERSONAL SECRETARIA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10		A			
[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[SW SISTEMA DE APLICACIONES INTRANET]	50		A	A	A	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	50		A	A	A	
	[SW_PORTAL WEB GOBERNACIÓN]	50		A	A	MA	
	[SW_SYSMAN]	50		A	A	MA	
	[SW_SISCAR]	50		A	A	A	
[E.21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[SW SISTEMA DE APLICACIONES INTRANET]	50			B	M	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	50			M	A	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	50			M	A	
	[SW_SYSMAN]	50			M	A	
	[SW_SISCAR]	50			M	A	
[E.23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE EQUIPOS (HARDWARE)	[HW_COMPUTADORES DE ESCRITORIO]	50				A	
	[HW_COMPUTADORES PORTÁTIL]	50				A	
	[HW_IMPRESORAS]	50				A	

Tabla 21 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE EQUIPOS (HARDWARE)	[HW_ESCANER]	10				A	
	[HW_SERVIDORES NS1 Y NS2]	10				A	
	[AUX_UPS]	10				M	
[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[S_CORREO ELECTRÓNICO ENTIDAD]	10				A	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10				M	
	[S_ADMINISTRACION DESARROLLO/SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10				A	
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10				M	
	[S_DESARROLLO Y MANTENIMIENTO PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10				M	
	[HW_COMPUTADORES DE ESCRITORIO]	10				A	
	[HW_COMPUTADORES PORTÁTIL]	10				A	
	[HW_IMPRESORAS]	10				A	
	[HW_ESCANER]	10				A	
	[HW_SERVIDORES NS1 Y NS2]	10				MA	
	[COM_WIFI]	10				MA	
	[COM_LOCAL]	10				MA	

Tabla 21 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[E.25] PERDIDA DE EQUIPOS/ROBO	[HW_COMPUTADORES DE ESCRITORIO]	5		MB		MA	
	[HW_COMPUTADORES PORTÁTIL]	5		MB		M	
	[HW_IMPRESORAS]	5		B		M	
	[HW_ESCANER]	5		MB		M	
	[HW_SERVIDORES NS1 Y NS2]	5		MA		MA	
	[AUX_UPS]	5		MB		B	
[E.28] INDISPONIBILIDAD DEL PERSONAL	[P_PERSONAL SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10				A	

Fuente: La presente investigación

1.2.3.4 Relación de amenazas por ataques intencionados por activo identificando su frecuencia e impacto

Tabla 22 Identificación de Amenazas por Ataques Intencionados.

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.5] SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10	A	A	A		
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10	MA	A	A		
	[S_MANEJO DE CORREO ELECTRÓNICO ENTIDAD]	10	A	A	A		

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.5] SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10	A	A	A		
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10	MA	A	A		
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10	A	A	A		
	[SW_SISTEMA DE APLICACIONES INTRANET]	10	A	M	M		
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10	MA	MA	A		
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10	MA	MA	A		
	[SW_SYSMAN]	10	MA	A	A		
	[SW_SISCAR]	10	MA	A	A		
	[COM_WIFI]	10	MA	A	A		
	[COM_LOCAL]	10	MA	MA	A		
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10		M	M	M	
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10					
	[S_MANEJO DE CORREO ELECTRÓNICO ENTIDAD]	10		A	A	M	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10		B	M	A	
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10		B	M	A	
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK]	10		B	M	A	
	[SW_SISTEMA DE APLICACIONES INTRANET]	10		B	M	M	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		B	M	M	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10		M	A	M	

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	[SW_SYSMAN]	10		M	M	M	
	[SW_SISCAR]	10		M	M	M	
	[HW_COMPUTADORES DE ESCRITORIO]	10		A	A	M	
	[HW_COMPUTADORES PORTÁTIL]	10		B	M	A	
	[HW_IMPRESORAS]	10		B	M	A	
	[HW_ESCANER]	10		B	M	A	
	[HW_SERVIDORES NS1 Y NS2]	10		B	M	M	
	[COM_WIFI]	10		B	M	M	
	[COM_LOCAL]	10		M	A	M	
[A7] USO NO PREVISTO	[S_MANEJO CORREO ELECTRÓNICO ENTIDAD]	10		B	B	B	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10		B	B	M	
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10		B	B	M	
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10		B	B	M	
	[SW_SISTEMA DE APLICACIONES INTRANET]	10		B	B	M	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		B	B	M	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10		B	B	B	
	[SW_SYSMAN]	10		B	B	M	
	[SW_SISCAR]	10		B	B	M	
	[HW_COMPUTADORES DE ESCRITORIO]	50		B	B	A	
	[HW_COMPUTADORES PORTÁTIL]	50		B	B	A	
	[HW_IMPRESORAS]	50		B	B	A	

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.7] USO NO PREVISTO	[HW_ESCANER]	50		B	B	A	
	[HW_SERVIDORES NS1 Y NS2]	10		B	B	M	
	[COM_WIFI]	70		B	B	A	
	[COM_LOCAL]	70		B	B	A	
	[AUX_UPS]	10		MB	B	B	
	[L_SALA DE COMUNICACIONES]	10		MB	B	B	
	[L_ SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10		MB	B	M	
[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[SW_SISTEMA DE APLICACIONES INTRANET]	10		A	A	A	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		M	M	M	
	[SW_PORTAL WEB GOBERNACIÓN]	10		M	A	A	
	[SW_SYSMAN]	10		A	A	A	
	[SW_SISCAR]	10		A	M	A	
[A.11] ACCESO NO AUTORIZADO	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10		A	A		
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10		A	A		
	[S_MANEJO DE CORREO ELECTRÓNICO ENTIDAD]	10		A	A		
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10		M	A		
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10		M	A		
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK]	10		M	MA		
	[SW_SISTEMA DE APLICACIONES INTRANET]	10		M	M		
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		M	M		
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10		M	M		

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.11] ACCESO NO AUTORIZADO	[SW_SYSMAN]	10		A	M		
	[SW_SISCAR]	10		A	M		
	[HW_COMPUTADORES DE ESCRITORIO]	10		A	M		
	[HW_COMPUTADORES PORTÁTIL]	10		A	M		
	[HW_IMPRESORAS]	10		B	B		
	[HW_ESCANER]	10		B	B		
	[HW_SERVIDORES NS1 Y NS2]	10		A	A		
	[COM_WIFI]	10		A	B		
	[COM_LOCAL]	10		A	B		
	[AUX_UPS]	10		MB	MB		
	[L_SALA DE COMUNICACIONES]	10		A	A		
	[L_SECRETARIA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10		A	M		
[A.13] REPUDIO	[S_CORREO ELECTRÓNICO ENTIDAD]	10			M		A
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10			M		A
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10			M		A
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10			M		A
[A.14] INTERCEPTACIÓN DE INFORMACIÓN	[COM_WIFI]	50		A			
	[COM_LOCAL]	50		A			

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.15] MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10			A		
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10			MA		
	[S_MANEJO DE CORREO ELECTRÓNICO ENTIDAD]	10			A		
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10			A		
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10			A		
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK]	10			A		
	[SW_SISTEMA DE APLICACIONES INTRANET]	10			A		
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10			A		
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10			A		
	[SW_SYSMAN]	10			MA		
	[SW_SISCAR]	10			MA		
[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10				MA	
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10				MA	
	[S_CORREO ELECTRÓNICO ENTIDAD]	10				MA	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10				B	
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10				M	
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10				MA	
	[SW_SISTEMA DE APLICACIONES INTRANET]	10				A	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10				A	

Tabla 22. (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10				A	
	[SW_SYSMAN]	10				MA	
	[SW_SISCAR]	10				MA	
[A.19] REVELACIÓN DE INFORMACIÓN	[D_BASES DE DATOS PROYECTOS DE LA GOBERNACIÓN]	10		A			
	[D_CODIGO FUENTE PORTAL WEB GOBERNACION,PORTALES]	10		A			
	[S_MANEJO DE CORREO ELECTRÓNICO ENTIDAD]	10		A			
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10		M			
	[S_ADMINISTRACION DESARROLLO /SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10		A			
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK]	10		A			
[A.22] MANIPULACIÓN DE PROGRAMAS	[SW_SISTEMA DE APLICACIONES INTRANET]	10		M	M	M	
	[SW_SISTEMA DE BACKUP EN EL SERVIDOR]	10		M	M	M	
	[SW_PORTAL WEB GOBERNACIÓN DE NARIÑO]	10		M	A	M	
	[SW_SYSMAN]	10		M	M	M	
	[SW_SISCAR]	10		MA	M	M	
[A.23] MANIPULACIÓN DE LOS EQUIPOS	[HW_COMPUTADORES DE ESCRITORIO]	10		A		A	
	[HW_COMPUTADORES PORTÁTIL]	10		A		A	
	[HW_IMPRESORAS]	10		A		A	
	[HW_ESCANER]	10		B		A	
	[HW_SERVIDORES NS1 Y NS2]	10		B		A	
	[AUX_UPS]	10		B		A	

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.24] DENEGACIÓN DE SERVICIOS	[S_MANEJO_CORREO ELECTRÓNICO ENTIDAD]	10				MA	
	[S_SERVICIO TÉCNICO Y DE SOFTWARE EQUIPOS DE COMPUTO]	10				MA	
	[S_ADMINISTRACION DESARROLLO/SOPORTE DE SISTEMAS DE INFORMACIÓN Y PLATAFORMAS GOBERNACIÓN DE NARIÑO]	10				MA	
	[S_ADMINISTRACION SERVIDORES/MAQUINAS VIRTUALES/DISPOSITIVOS CISCO_MIKROTIK GOBERNACIÓN]	10				MA	
	[HW_COMPUTADORES DE ESCRITORIO]	10				MA	
	[HW_COMPUTADORES PORTÁTIL]	10				MA	
	[HW_IMPRESORAS]	10				A	
	[HW_ESCANER]	10				A	
	[HW_SERVIDORES NS1 Y NS2]	10				A	
	[COM_WIFI]	10				A	
	[COM_LOCAL]	10				A	
[A.25] ROBO	[HW_COMPUTADORES DE ESCRITORIO]	10		A		MA	
	[HW_COMPUTADORES PORTÁTIL]	10		A		MA	
	[HW_IMPRESORAS]	10		A		MA	
	[HW_ESCANER]	10		B		MA	
	[HW_SERVIDORES]	10		B		MA	
	[AUX_UPS]	10		M		MA	
[A.26] ATAQUE DESTRUCTIVO	[HW_COMPUTADORES DE ESCRITORIO]	10				MA	
	[HW_COMPUTADORES PORTÁTIL]	10				MA	
	[HW_IMPRESORAS]	10				MA	
	[HW_ESCANER]	10				MA	
	[HW_SERVIDORES NS1 Y NS2]	10				MA	

Tabla 22 (Continuación)

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %				
			[A]	[C]	[I]	[D]	[T]
[A.26] ATAQUE DESTRUCTIVO	[AUX_UPS]	10				A	
	[L_SALA DE COMUNICACIONES]	10				A	
	[L_ SECRETARIA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10				A	
	[AUX_UPS]	10				A	
	[L_SALA DE COMUNICACIONES]	10				A	
	[L_ SECRETARIA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10				A	
[A.28] INDISPONIBILIDAD DEL PERSONAL	[P_PERSONAL SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10				A	
[A.29] EXTORSIÓN	[P_PERSONAL SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	10		A	A	A	
[A.30] INGENIERÍA SOCIAL	[P_PERSONAL SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO]	50		A	A	A	

Fuente: La presente investigación

En las anteriores tablas se identificaron las amenazas por desastres naturales, de origen industrial, de errores y fallos no intencionados y ataques intencionados a las que estaban expuestos cada uno de los activos de la Gobernación, así mismo se midió su frecuencia, es decir la probabilidad de que pudieran suceder estas amenazas.

Para cada activo se identificó las dimensiones que se vieron afectadas por amenaza según la Metodología Magerit, como son Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad y así se dio una valoración del impacto que causaría si se materializan dichas amenazas.

Con esta valoración se determinó que la probabilidad de ocurrencia en cuanto a desastres naturales y de origen industrial es muy poco frecuente, pero si se llegan a presentar estas amenazas, el impacto que causaría en la Gobernación sería muy alto; por otro lado la probabilidad de ocurrencia de errores y fallos no intencionados y ataques intencionados es más frecuente, lo que ocasiono en los activos un impacto medio, alto y muy alto para el funcionamiento de las actividades que se desarrollan diariamente en la Gobernación.

1.2.4 Identificación de Vulnerabilidades

Se llevó a cabo mediante una visita a las instalaciones de La Secretaría de TIC de la Gobernación de Nariño para realizar una inspección visual de los activos de información, entrevistas con los administradores, revisión de la información y documentación suministrada (políticas de uso, manual de funciones y competencias laborales, procedimientos, formatos y hojas de vida de los equipos) y análisis de vulnerabilidades.

Inspección visual de los activos de información.

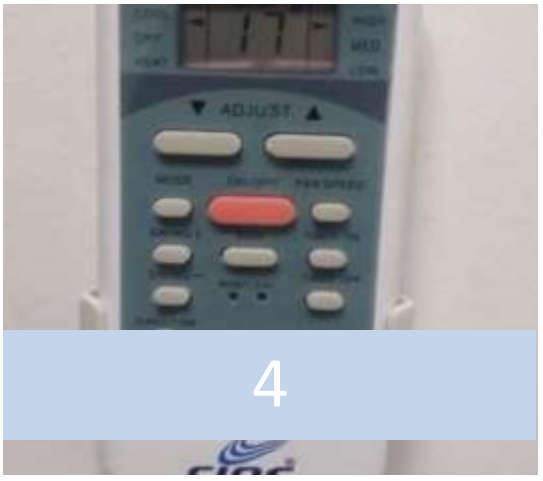
- **Inspección visual a la sala de comunicaciones**

Figura 6 Puerta Sala de Comunicación

Fuente: La presente investigación

El acceso a la sala de comunicaciones no contaba con un protocolo de seguridad, tenía una puerta de vidrio de chapa común con llave, se debería contar con un sistema de cerradura biométrico que garantice el ingreso del personal autorizado.

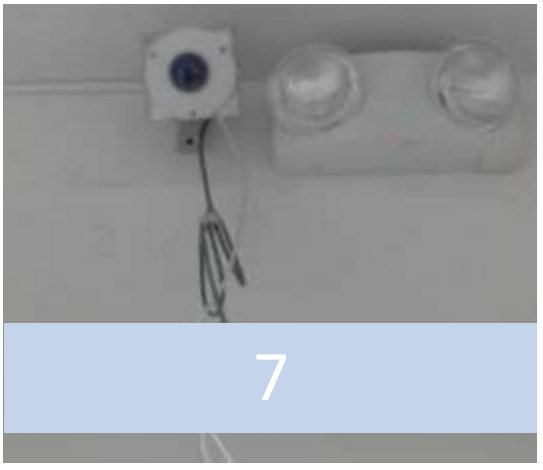
Figura 7 Aire Acondicionado y Cámaras de Seguridad



4

5

6



7

Fuente: La presente investigación

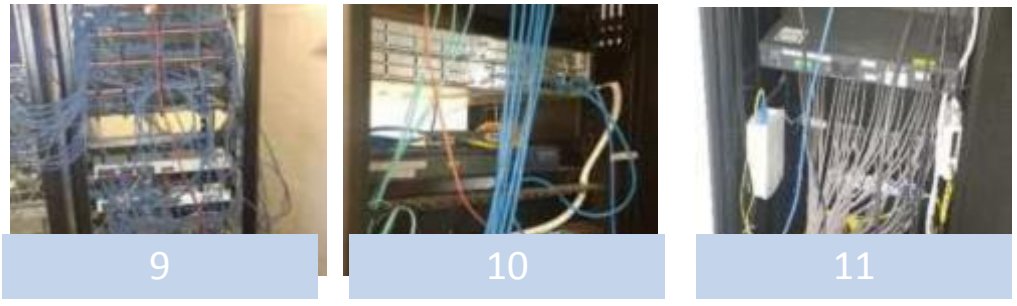
Se evidenció que la sala de comunicaciones contaba con sistema de aire acondicionado y cámara de seguridad en su interior, pero esta se encontraba desconectada, la sala no contaba con una cámara que estuviera dirigida a esta.

Figura 8.Falta de Medidores de Temperatura y Humedad y Alarmas de Humo

Fuente: La presente investigación

La sala no contaba con medidores de temperatura y humedad, ni tampoco tenía alarmas de humo, lo que ocasionaba deterioro en las paredes de la sala.

Figura 9 Rack de Comunicaciones



Fuente:La presente investigación

Con respecto al rack se observó que el cableado eléctrico y el cableado de datos se encontraban por separado, sin embargo no contaban con aisladores de

emanaciones electromagnéticas y además se evidencio que no existía orden en la parte del cableado.

Figura 10 Panel Eléctrico

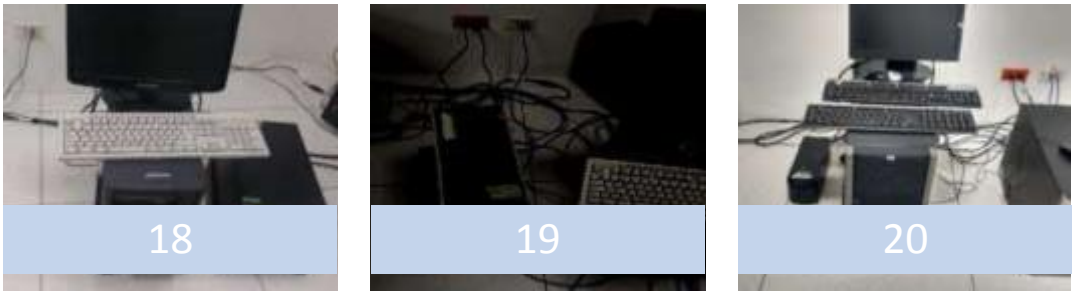
Fuente: La presente investigación

El panel eléctrico contaba con un mensaje de alerta alto voltaje y además con sus debidas precauciones de seguridad. En la sala de comunicaciones no se evidenció la existencia de un extintor especializado para equipos de cómputo en caso de incendio.

Figura 11 Equipos Mal Ubicados

Fuente: La presente investigación

Figura 11 (Continuación)



Fuente: La presente investigación

Para evitar el sobrecalentamiento en los equipos, es indispensable que haya un espacio adecuado entre ellos y se observó que estos tenían entre si un espacio limitado. Por otra parte, se observó que sobre algunos equipos ubicaban toda clase de papelería, útiles, herramientas y demás que deberían estar ubicados en otro sitio. En la sala de comunicaciones se pudo observar una mala organización de los monitores, teclados, mouse, cpus, demás equipamiento informático, los cuales en el caso de una inundación, un corto circuito o el polvo por estar ubicados en el piso tendían a dañarse por causa de estas amenazas.

Figura 12 Servidores Mal Ubicados

Fuente: La presente investigación

Los servidores se encontraban mal ubicados lo que podía ocasionar un mal funcionamiento.

Figura 13 Impresoras

Fuente: La presente investigación

Se evidenció impresoras en el piso con mucho riesgo de ser dañadas por causa de alguna inundación, corto circuito. Además, sobre ellas se ubicaban bolsas que no deberían estar allí.

Figura 14. Fuente de Energía

Fuente: La presente investigación

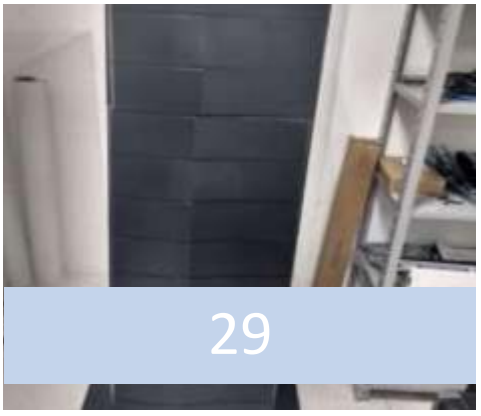
Se observó que no existían planos, esquemas, avisos adecuados que indicaran que había una fuente de energía y señales de estas mismas.

Figura 15 Cableado

Fuente: La presente investigación

La disposición desordenada de cableado de alimentación eléctrica y de comunicaciones podría ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones.

Figura 16 Ups

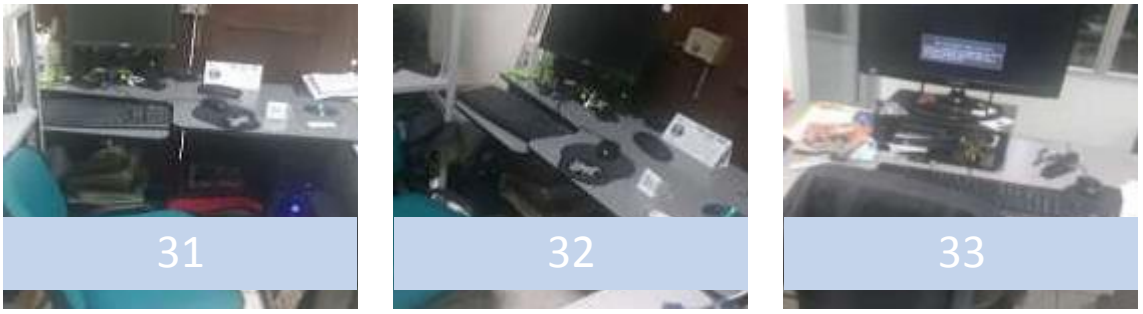


Fuente: La presente investigación

La UPS que se encontraba en la sala de servidores sufría a veces algunas falencias.

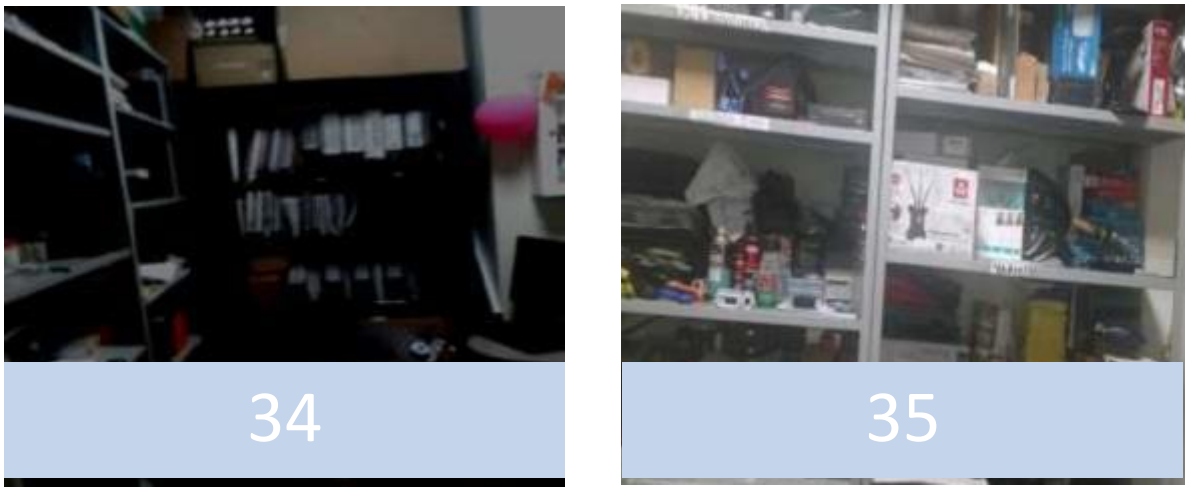
- **Inspección visual a la oficina de Soporte Técnico**

Figura 17 Puestos de Trabajo Oficina Soporte Técnico



Fuente: La presente investigación

Figura 18 Oficina Soporte Técnico



Fuente: La presente investigación

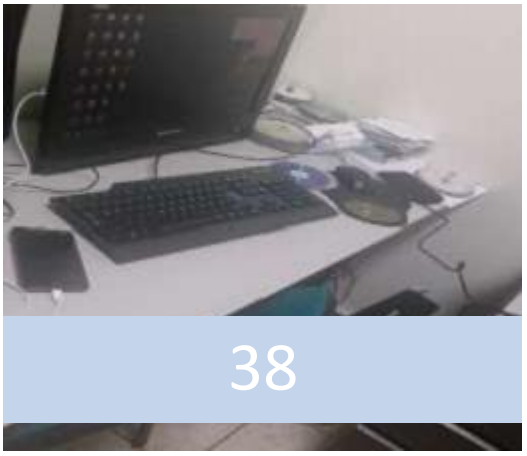
Se pudo observar que los puestos de trabajo de los funcionarios contaban con un limitado espacio libre; así mismo no existía una puerta que impidiera el acceso al personal no autorizado.

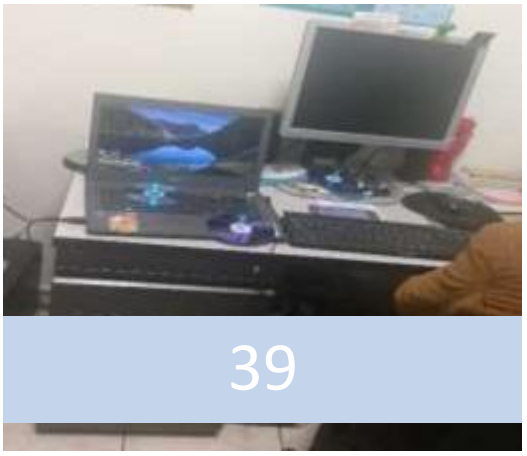
Figura 19 Cámaras de Seguridad y Extintor de la Oficina de Soporte Técnico

Fuente: La presente investigación

El área de soporte técnico contaba con una cámara de seguridad y un extintor en caso de incendio, pero este se encontraba mal ubicado.

Figura 20 Computadores de Escritorio y Portátiles Área de Soporte técnico





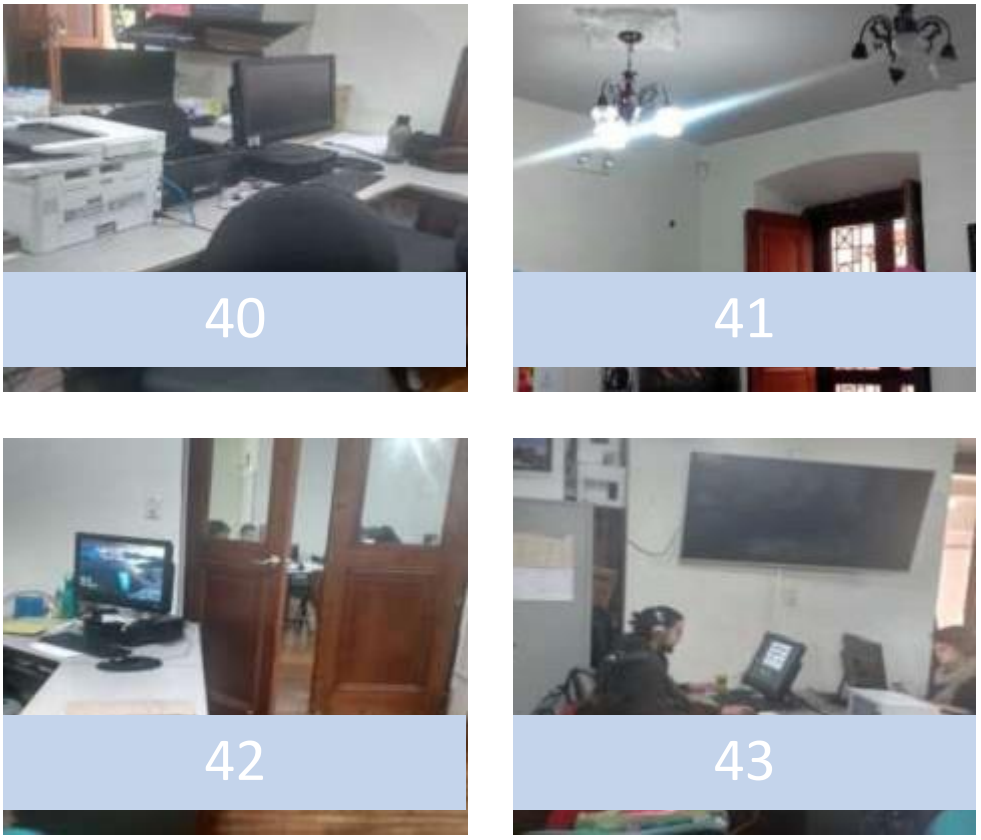
Fuente: La presente investigación

Los técnicos contaban con computadores de escritorio y portátiles, teclados, mouse, archivos y demás equipamiento informático, los cuales tenían una buena

distribución para el desarrollo de su trabajo; sin embargo, al no estar restringido el acceso al personal no autorizado se podría presentar perdida de dichos activos.

- **Inspección visual a la oficina de la secretaria de TIC, innovación y Gobierno Abierto.**

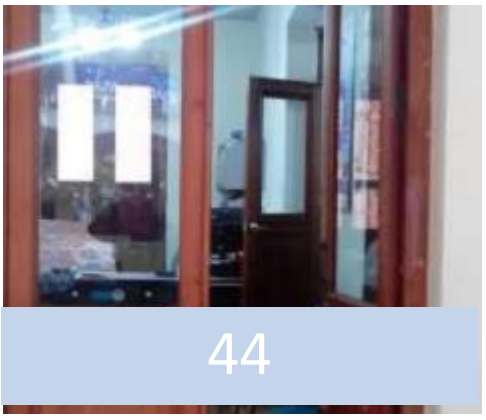
Figura 21 Puestos de Trabajo de la Oficina TIC, Innovación y Gobierno Abierto

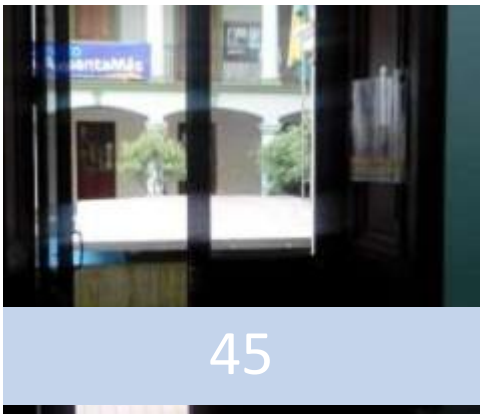


Fuente: La presente investigación

Cada puesto de trabajo tenía su propio computador de escritorio y estos con sus respectivos reguladores, ademas existía una buena organización en la oficina.

Figura 22 Entrada a la Secretaria de TIC, Innovación y Gobierno Abierto

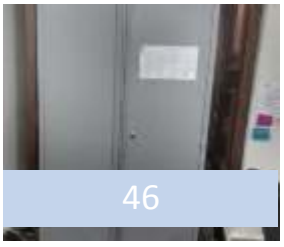


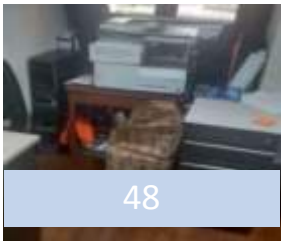


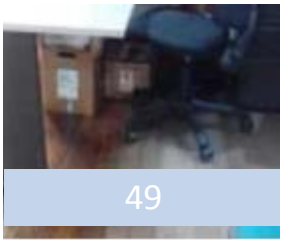
Fuente: La presente investigación

En la oficina no se contaba con un sistema de camaras de seguridad, ni tampoco con el suficiente personal para vigilancia interna, los controles de ingreso eran únicamente puertas de madera con ventanas de vidrio, donde cada puerta contaba con una sola cerradura de seguridad.

Figura 23 Soportes de Información







Fuente: La presente investigación

La secretaría de Tic, Innovación y Gobierno abierto guardaba los soportes de información en archivadores y en cajas, pero estas últimas estaban mal ubicadas lo que podría ocasionar que estén expuestas al polvo y finalmente su deterioro.

Como se observó en las imágenes anteriores, se puede concluir que la sala de comunicaciones no contaba con la debida seguridad que se requiere, puesto que solo tenía una puerta de vidrio sin un sistema de cerradura biométrico, esto ocasionaba que no se permitía identificar al personal autorizado para ingresar al sitio, ni tampoco existía un registro de entrada y salida, ni justificación de ingreso; de igual manera a pesar de que existía una cámara de seguridad en el interior de la sala, esta se encontraba desconectada imposibilitando la vigilancia en su interior. Así mismo se pudo observar que las paredes se encontraban deterioradas por falta de medidores de temperatura y humedad.

Con respecto al cableado se evidenció que no se utilizaba paneles de obturación para el cableado en la sala de servidores ni tampoco se contaba con aisladores de emanaciones electromagnéticas; con respecto a los equipos ubicados en la sala de comunicaciones se pudo identificar que el espacio entre cada equipo era muy limitado para que fluya el aire. Se debían separar un poco para mejorar la ventilación entre estos equipos y así evitar que los dispositivos se sobrecalienten, disminuyan su velocidad de procesamiento y por último que puedan apagarse por sobrecalentamiento. En el interior de la sala tampoco se contaba con un extintor en caso de incendio.

Con lo anterior se pudo concluir que existían grandes falencias en la sala de comunicaciones ubicada en el interior de la Secretaria de TIC, Innovación y Gobierno Abierto, y que de no ser corregidas se podría presentar grandes daños en el funcionamiento de los servidores, equipos, comunicaciones, etc.

Con respecto a la Oficina de Soporte Técnico se observó que existía un limitado espacio entre los puestos de trabajo, lo anterior facilitaría la perdida de información, equipos y herramientas necesarias para el adecuado desempeño de esta área. No existía además una puerta para impedir el acceso al personal no autorizado; es decir a esta oficina entra y sale cualquier personal de la gobernación.

La Oficina de la Secretaria de TIC, Innovación y Gobierno Abierto tenía unos puestos de trabajo de forma organizada, pero dentro de ella no existía una cámara de seguridad que monitoree el acceso de personas a la misma, esto imposibilitaba que en caso de haber perdida de equipamiento informático o demás herramientas de la oficina se pudiera identificar al responsable; la oficina contaba con archivadores y cajas para guardar todo el soporte de información, pero algunas de las cajas estaban ubicadas en el piso, provocando a un corto plazo la perdida de esta información a causa del polvo al que se encontraban expuestas.

2.2.5 Análisis de Vulnerabilidades

A continuación, se realizó la identificación de vulnerabilidades, basados en las visitas a las instalaciones de la secretaría de TIC, con el fin de observar cada uno de los activos allí presentes realizando entrevistas al personal encargado de los activos informáticos, las vulnerabilidades identificadas se realizaron para cada uno de los activos que se encuentran en el proceso de la secretaría de TIC, innovación y Gobierno abierto de la Gobernación de Nariño.

En la siguiente tabla se muestra las vulnerabilidades de los activos **Software Sistema de Aplicaciones Intranet**

Tabla 23 Vulnerabilidades Software Sistema de Aplicaciones Intranet

Activo STIC-07	**STIC-07 Software Sistema de Aplicaciones INTRANET.**		
Administrador	**Apoyo TI**		
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información. Falta de plan o Política de registro de Bitácoras.
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.

Tabla 23 (Continuación)

Activo STIC-07		**STIC-07 Software Sistema de Aplicaciones INTRANET.**	
Administrador		**Apoyo TI**	
Tipo activo		**Software**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E19	Fugas de información	Los datos de los sistemas de información y plataformas no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.
	E21	Errores de Mantenimiento/actualización Software	Software no Licenciado Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.
Ataques intencionados	A5	Suplantación de la identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.
	A18	Destrucción de información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.

Fuente: La presente investigación

En la siguiente tabla se muestra las vulnerabilidades del activo **Servidores NS1 y NS2.**

Tabla 24. Vulnerabilidades Servidores NS1 y NS2

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**		
Administrador	**Soporte técnico**		
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.

Tabla 24. (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**		
Administrador	**Soporte técnico**		
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De Origen Industrial	I3	Contaminación Mecánica	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad.
	I4	Contaminación Electromagnética.	Los racks no cuentan con aisladores de emanaciones electromagnéticas.
	I5	Avería de Origen físico o lógico.	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad. Falta de controles físico y lógicos como el mantenimiento preventivo de hardware.
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.

Fuente: La presente investigación

Tabla 24 (Continuación)

Activo STIC-12		**STIC-12 Servidores NS1 y NS2**	
Administrador		**Soporte técnico**	
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del Administrador	Falta de conocimiento del administrador. Sobrecarga de trabajo
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de los servidores NS1 y NS2 Falta de controles de mantenimiento preventivo y periódico a los servidores. Falta de plan de Gestión y control de recursos vs requerimientos.
	E24	Caída del sistema por agotamiento de recursos.	Carencia de restitución de Equipos. Falta de planes de continuidad del Negocio.
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad enfocadas a la sala de comunicaciones. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.
Ataques intencionados	A6	Abuso de Privilegios de acceso	El acceso a la sala de comunicaciones no cuenta con un protocolo de seguridad, tiene una puerta de vidrio de chapa común con llave, no tiene un sistema de cerradura biométrico que garantice el ingreso del personal autorizado.
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.
	A23	Manipulación de los equipos.	Falta de controles para el ingreso a la sala de comunicaciones.

Tabla 24 (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**		
Administrador	**Soporte técnico**		
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Ataques intencionados	A24	Denegación de servicio	Falta de controles físicos y lógicos que permitan la continuidad del negocio.
	A25	Robo	No existen cámaras de seguridad enfocadas a la sala de comunicaciones. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.

Fuente: La presente investigación

1.2.6 Estimación del impacto

Mediante el uso de tablas de doble entrada, en donde:

Impacto = Valor del activo x Degradación

Tabla 25 Estimación del Impacto

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El objetivo fue conocer el alcance del daño producido en la Secretaria de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño derivado de la materialización de las amenazas sobre los activos de información, mediante el uso de tablas de doble entrada para la obtención de resultados. A partir de los datos obtenidos en las fases anteriores, se procede a estimar el impacto.

El primer dato requerido fue el “Nivel del activo” valorado cuantitativa y/o cualitativamente

El segundo dato necesario para la valoración del impacto fue la “Degradación”, el cual nos indica que tan perjudicado resulta el [valor del] activo de información (1%, 50%, 100%), como resultado de la materialización de las amenazas:

- **90% a 100%**: Degradación muy considerable del activo
- **25% a 89%:** Degradación medianamente considerable del activo
- **1% a 24%**: Degradación poco considerable del activo

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.
Mayor (5): Impacta en la operatividad de los procesos.
Moderado (3): Impacta en la operatividad del macro proceso.
Menor (2): Impacta en la operatividad del proceso.
Insignificante (1): Impacta levemente en la operatividad del proceso

A continuación, se realizó la estimación del impacto para el activo **Software Sistema de Aplicaciones Intranet.**

Tabla 26 Valoración Activo Software Sistema de Aplicaciones Intranet

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 07	Software sistema de aplicaciones Intranet	SW	Uso Interno	Sensible	Muy Alta	**Muy Alto**	**4**

Fuente: La presente investigación

Para el caso del **Software sistema de aplicaciones Intranet** con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Software, las principales amenazas que recaen sobre esta clase de activos son errores del administrador, Difusión de software dañino, fugas de información, vulnerabilidades de los programas, errores de mantenimiento/actualización de software, ataques intencionados como suplantación de la identidad del usuario, Difusión de software dañino, modificación deliberada de la información, y destrucción de información; que lo afectarían fuertemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido fue 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacto fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 27 Estimación del Impacto Software Sistema de Aplicaciones Intranet

IMPACTO		Degradación		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Por lo tanto, el daño producido del activo será:

Desastroso (8): Impacta fuertemente en la operatividad de los procesos

A continuación, se realizó la estimación del impacto para el activo **Servidores NS1 y NS2.**

Tabla 28 Valoración Activo Servidores NS1 y NS2

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 12	Servidores NS1 Y NS2	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	5

Fuente: La presente investigación

Para el caso del activo **Servidores NS1 y NS2** con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres industriales y robo; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 29 Estimación del Impacto Servidores NS1 y NS2

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Por lo tanto, el daño producido del activo será:

Desastroso (8): Impacta fuertemente en la operatividad de los procesos

1.2.7 Estimación de la probabilidad

El objetivo consistió en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir (a mayor número de vulnerabilidades, mayor probabilidad de ocurrencia de las amenazas) y se utilizó la siguiente escala:

Tabla 30 Escala de Frecuencia de Amenazas

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

A continuación, se visualizó el impacto y la frecuencia de materialización de cada una de las amenazas sobre el activo **Software sistema de aplicaciones intranet.**

Tabla 31. Impacto y Frecuencia Software Sistema de Aplicaciones Intranet

Activo STIC-07		**STIC-07 Software Sistema de Aplicaciones Intranet.**			
Administrador		**Apoyo TI**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Software**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.	Baja	3
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.	Media	4

Tabla 31 (Continuación)

Activo STIC-07		**STIC-07 Software Sistema de Aplicaciones Intranet.**			
Administrador		**Apoyo TI**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Software**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E19	Fugas de información	Los datos de los sistemas de información y plataformas no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.	Media	4
	E21	Errores de Mantenimiento/actualización Software	Software no Licenciado Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Baja	3
Ataques Intencionados	A5	Suplantación de la identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3
	A18	Destrucción de información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3

Fuente: La presente investigación

A continuación, se visualizó el impacto y la frecuencia de materialización de cada una de las amenazas sobre el activo **Servidores NS1 y NS2.**

Tabla 32 Impacto y Frecuencia Servidores NS1 y NS2

Activo STIC-12		**STIC-12 Servidores NS1 y NS2**			
Administrador					
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Hardware**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Media	4

Tabla 32 (Continuación)

Activo STIC-12		**STIC-12 Servidores NS1 y NS2**		
Administrador		**Soporte Técnico**		
Degradación		**100%**		
Impacto		**8**	**Desastroso**	
Tipo activo		**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**
De origen industrial	I3	Contaminación Mecánica	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad.	Baja 3
	I4	Contaminación Electromagnética.	Los racks no cuentan con aisladores de emanaciones electromagnéticas.	Muy baja 2
	I5	Avería de Origen físico o lógico.	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad. Falta de controles físico y lógicos como el mantenimiento preventivo de hardware.	Baja 3
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.	Muy baja 2
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja 3

Tabla 32 (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**				
Administrador	**Soporte Técnico**				
Degradación	**100%**				
Impacto	**8**	**Desastroso**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del Administrador	Falta de conocimiento del administrador. Sobrecarga de trabajo	Muy baja	2
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de los servidores NS1 y NS2 Falta de controles de mantenimiento preventivo y periódico a los servidores. Falta de plan de Gestión y control de recursos vs requerimientos.	Baja	3
	E24	Caída del sistema por agotamiento de recursos.	Carencia de restitución de Equipos. Falta de planes de continuidad del Negocio.	Baja	3
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad enfocadas a la sala de comunicaciones. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Muy baja	2
Ataques Intencionados	A6	Abuso de Privilegios de acceso	El acceso a la sala de comunicaciones no cuenta con un protocolo de seguridad, tiene una puerta de vidrio de chapa común con llave, no tiene un sistema de cerradura biométrico que garantice el ingreso del personal autorizado.	Baja	3
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3

Tabla 32 (Continuación)

Activo STIC-12		**STIC-12 Servidores NS1 y NS2**			
Administrador		**Soporte Técnico**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Hardware**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Ataques Intencionados	A23	Manipulación de los equipos.	Falta de controles para el ingreso a la sala de comunicaciones.	Baja	3
	A24	Denegación de servicio	Falta de controles físicos y lógicos que permitan la continuidad del negocio.	Baja	3
	A25	Robo	No existen cámaras de seguridad enfocadas a la sala de comunicaciones. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Baja	3

Fuente: La presente investigación

1.2.8 Estimación del Riesgo

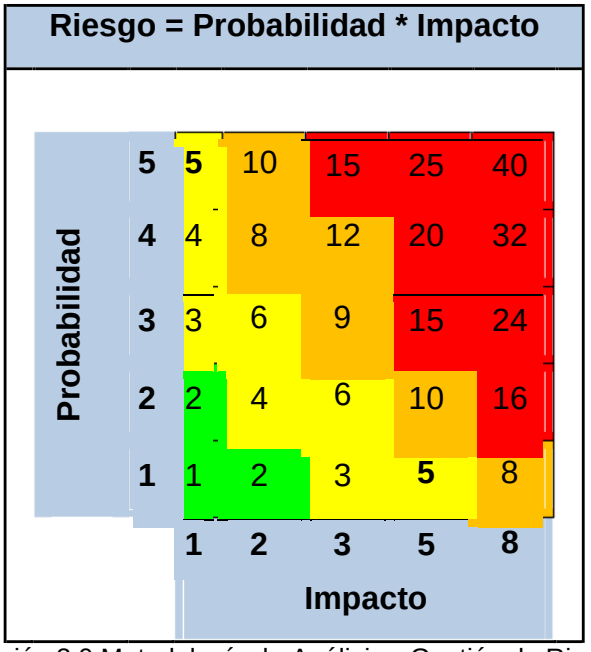
Luego de realizar el impacto y la frecuencia de cada uno de los activos, el siguiente paso fue la estimación del riesgo.

Este valor se obtiene como resultado de la siguiente fórmula:

$$Riesgo\ (R) = Probabilidad\ (F) \times Impacto$$

El valor **NR** (Nivel de Riesgo) obedece al Mapa de Riesgos:

Tabla 33 Mapa de Riesgos



Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Tabla 34 Nivel de Riesgos

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Por último, con ayuda de la función promedio se obtuvo el Nivel de Riesgo total del activo de información.

Con los resultados obtenidos en este análisis se procedió a la evaluación de riesgos. Para cada activo de información, el proceso concluye si el Nivel de Riesgo es

aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles necesarios.

A continuación, se realizó la estimación del riesgo para el activo **Software sistema de aplicaciones intranet.**

Tabla 35. Estimación del Riesgo Software Sistema de Aplicaciones Intranet.

Activo STIC-07	**STIC-07 Software Sistema de Aplicaciones Intranet**		
Administrador	**Apoyo TI**		
Degradación	**100%**		
Impacto	**8**	**Desastroso**	
Tipo activo	**Software**		

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
							4	Extremo
				Frecuencia (F)		R		NR
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.	Baja	3	24	4	extremo
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.	Media	4	32	4	extremo
	E19	Fugas de información	Los datos de los sistemas de información y plataformas no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3	24	4	extremo
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.	Media	4	32	4	extremo

Tabla 35 (Continuación)

Activo STIC-07	**STIC-07 Software Sistema de Aplicaciones Intranet**							
Administrador	**Apoyo TI**							
Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Software**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**		**NR**
Errores y fallos	E21	Errores de Mantenimiento/actualización Software	Software no Licenciado Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Media	4	32	4	extremo
Ataques Intencionados	A5	Suplantación de la identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	24	4	extremo
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3	24	4	extremo
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3	24	4	extremo
	A18	Destrucción de información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3	24	4	extremo

Fuente: La presente investigación

A continuación, se realizó la estimación del riesgo para el activo **Servidores NS1 y NS2.**

Tabla 36 Estimación del Riesgo Servidores NS1 y NS2

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**							
Administrador	**Soporte técnico**							
Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
				Frecuencia (F)		**R**		**NR**
							4	Extremo
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2	16	4	Extremo
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	16	4	Extremo
Ataques Intencionados	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2	16	4	Extremo

Tabla 36 (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**							
Administrador	**Soporte técnico**							
Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia **(F)**		**R**		**NR**
De Origen industrial	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Media	4	32	4	Extremo
	I3	Contaminación Mecánica	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad.	Baja	3	24	4	Extremo
	I4	Contaminación Electromagnética.	Los racks no cuentan con aisladores de emanaciones electromagnéticas.	Muy baja	2	16	4	Extremo

Tabla 36 (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**							
Administrador	**Soporte Técnico**							
Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
				Frecuencia (F)		**R**	**NR**	
De Origen industrial	I5	Avería de Origen físico o lógico.	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad. Falta de controles físico y lógicos como el mantenimiento preventivo de hardware.	Baja	3	24	4	Extremo
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.	Muy baja	2	16	4	Extremo
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja	3	24	4	Extremo
Errores y	E2	Errores del Administrador	Falta de conocimiento del administrador. Sobrecarga de trabajo	Muy baja	2	16	4	Extremo

Tabla 36 (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**		
Administrador	**Soporte técnico**		
Degradación	**100%**		
Impacto	**8**	**Desastroso**	
Tipo activo	**Hardware**		

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
				Frecuencia (F)		R	4	Extremo NR
Errores y fallos	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de los servidores NS1 y NS2 Falta de controles de mantenimiento preventivo y periódico a los servidores. Falta de plan de Gestión y control de recursos vs requerimientos.	Baja	3	24	4	Extremo
	E24	Caída del sistema por agotamiento de recursos.	Carencia de restitución de Equipos. Falta de planes de continuidad del Negocio.	Baja	3	24	4	Extremo
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad enfocadas a la sala de comunicaciones. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Muy baja	2	16	4	Extremo
Ataques intencionados	A6	Abuso de Privilegios de acceso	El acceso a la sala de comunicaciones no cuenta con un protocolo de seguridad, tiene una puerta de vidrio de chapa común con llave, no tiene un sistema de cerradura biométrico que garantice el ingreso del personal autorizado.	Baja	3	24	4	Extremo
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3	24	4	Extremo

Tabla 36 (Continuación)

Activo STIC-12	**STIC-12 Servidores NS1 y NS2**		
Administrador	**Soporte técnico**		
Degradación	**100%**		
Impacto	**8**	**Desastroso**	
Tipo activo	**Hardware**		

Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
Errores y fallos	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de los servidores NS1 y NS2 Falta de controles de mantenimiento preventivo y periódico a los servidores. Falta de plan de Gestión y control de recursos vs requerimientos.	Baja	3	24	4	Extremo
	E24	Caída del sistema por agotamiento de recursos.	Carencia de restitución de Equipos. Falta de planes de continuidad del Negocio.	Baja	3	24	4	Extremo
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad enfocadas a la sala de comunicaciones. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Muy baja	2	16	4	Extremo
Ataques intencionados	A6	Abuso de Privilegios de acceso	El acceso a la sala de comunicaciones no cuenta con un protocolo de seguridad, tiene una puerta de vidrio de chapa común con llave, no tiene un sistema de cerradura biométrico que garantice el ingreso del personal autorizado.	Baja	3	24	4	Extremo
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3	24	4	Extremo

Fuente: La presente investigación

- Para el activo **Software Sistema de Aplicaciones Intranet**, como el Nivel de Riesgo fue extremo; fue necesario definir el tratamiento a seguir.

  El tratamiento a seguir consistió en la definición de nuevos controles de tipo preventivo y/o correctivo que permitieron reducir los niveles de riesgo del activo.

- Para el activo **Servidores NS1 y NS2** como el Nivel de Riesgo fue extremo; fue necesario definir el tratamiento a seguir.

  Primero, se descarta la opción de evitar el riesgo, ya que este es un activo de muy alto valor y el retiro del mismo no permitiría la prestación de muchos servicios fundamentales para la Gobernación de Nariño.

  La opción de transferir el riesgo por medio de la adquisición de un seguro tampoco fue la adecuada, puesto que los costos de las pólizas en la mayoría de los casos son muy elevados y la Secretaría de TIC no contaba con los recursos necesarios para adquirirlos.

  No obstante, el tratamiento a seguir consistió en la definición de nuevos controles de tipo preventivo y/o correctivo que permitieron reducir los niveles de riesgo del activo Servidores NS1 y NS2 y pase de un nivel extremo a un nivel tolerable, o en el mejor de los casos a un nivel aceptable de ser posible; que es lo que se esperaba que suceda con los demás activos de información que tenían un nivel de riesgo similar o peor.

1.3 PLAN DE TRATAMIENTO DE RIESGOS CONTROLES PROPUESTOS

Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definieron las salvaguardas que son procedimientos tecnológicos que reducen el riesgo, de acuerdo a los activos que se iban a proteger, en este caso se tuvo en cuenta las salvaguardas definidas en Magerit.

Tabla 37 Tratamiento 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: Metodología MAGERIT Versión 3.0

SALVAGUARDAS A IMPLEMENTAR PARA EL ACTIVO SOFTWARE SISTEMA DE APLICACIONES INTRANET

Tabla 38 Salvaguardas Software Sistema de Aplicaciones Intranet

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Software Sistema de Aplicaciones Intranet	[E2] Errores del administrador	DC	4	7.2.2,12.4.3, 12.6.1,14.1.1,14.1.2,14.2.1,14.2.5,14.2.8,14.2.9, 14.3.1	* Todos los empleados de la Gobernación y los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos. *Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad. * Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la Gobernación a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. * Los requisitos relacionados con la entidad de la información se deberían incluir en los requisitos para nuevos SI o para mejoras en los sistemas de información existentes. * La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas. * Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la Gobernación de Nariño.

Tabla 38 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Software Sistema de Aplicaciones Intranet	[E2] Errores del administrador	DC	4	7.2.2,12.4.3, 12.6.1,14.1.1,14.1.2,14.2.1,14.2.5,14.2.8,14.2.9, 14.3.1	* Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. * La Gobernación de Nariño debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. * Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad. * Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de pruebas para aceptación y criterios de aceptación relacionados. * Los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente.
	[E8] Difusión de software dañino	DC	4	7.1.2,12.2.1, 12.6.2	* Los acuerdos contractuales con empleados y contratistas deberían establecer sus responsabilidades en cuanto a la seguridad de la información. *Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos. * Se debería establecer e implementar las reglas para la instalación de software por parte de los usuarios.

Tabla 38. (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Software Sistema de Aplicaciones Intranet	[E19] Fugas de información	DC	4	7.2.2, 9.4.1,9.4.2,9.4.3,8.2.1,12.3.1,14.2.8,14.3.1, 16.1.1,16.1.2, 16.1.4,16.1.5, 16.1.6,16.1.7	* Todos los empleados de la Gobernación de Nariño y en donde sea pertinente, los contratistas, debería recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Gobernación pertinentes para su cargo. * El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso. * Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. * Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar la calidad de las contraseñas. * La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. * Se deberían hacer copias de respaldo de la Información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo. * Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad. * Los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente.

Tabla 38 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Software Sistema de Aplicaciones Intranet	[E19] Fugas de información	DC	4	7.2.2, 9.4.1,9.4.2,9.4.3,8.2.1,12.3.1,14.2.8,14.3.1,16.1.1, 16.1.2,16.1.4,16.1.5,16.1.6,16.1.7	* Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible. *Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información. * Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo a procedimientos documentados. * El conocimiento adquirido al analizar y resolver incidentes de seguridad de la Información se debería usar para reducir la posibilidad o el impacto de incidentes futuros. *La Gobernación debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
	[E20] Vulnerabilidades de los programas	DC	4	18.1.5,10.1.1,10.1.2	*Se deberían usar controles criptográficos en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. * Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. * Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

Tabla 38 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Software Sistema de Aplicaciones Intranet	[E20] Vulnerabilidades de los programas	DC	4	18.1.5,10.1.1,10.1.2,14.2.1,14.2.5,14.2.8,14.2.9.	* Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de SI. * Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad. *Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de pruebas para aceptación y criterios de aceptación relacionados. * Los datos de prueba se deberían seleccionar, proteger y controlar cuidadosamente.
	[E21] Errores de mantenimiento/actualización software	DC	4	12.1.1,12.2.1,12.6.2,14.2.2,14.2.5,	* Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que lo necesitan. * Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos. * Se debería establecer e implementar las reglas para la instalación de software por parte de los usuarios.

Tabla 38 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Sistema de Aplicaciones Intranet	[E21] Errores de mantenimiento/actualización software	DC	4	12.1.1,12.2.1,12.6.2,14.2.2,14.2.5,	* Los cambios a los sistemas dentro del ciclo de vida del desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios. *Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
	[A5] Suplantación de la Identidad del Usuario	DC	4	7.2.3,9.1.1, 9.2.1,9.2.2, 9.2.3,9.4.3,	* Se debería contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados. *Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. *Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Tabla 38 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Sistema de Aplicaciones Intranet	[A5] Suplantación de la Identidad del Usuario	DC	4	7.2.3,9.1.1, 9.2.1,9.2.2, 9.2.3,9.4.3,	* Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. * Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
	[A8] Difusión de software dañino	DC	4	12.2.1,14.2 .2.	* Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos. * Los cambios a los sistemas dentro del ciclo de vida del desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
	[A15] Modificación deliberada de la información	DC	4	12.3.1,14.1 .1,16.1.5	*Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. *Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. * Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

Tabla 38 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Sistema de Aplicaciones Intranet	[A18] Destrucción de información	DC	4	12.3.1,14.1.1,16.1.5	* Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. * Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. * Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

Fuente: La presente investigación

SALVAGUARDAS A IMPLEMENTAR PARA EL ACTIVO SERVIDORES NS1 Y NS2

Tabla 39. Salvaguardas Servidores NS1 y NS2

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[N1] Fuego	DC	4	11.1.4	* Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.
	[N8]Desastres Naturales Fenómeno de Origen Volcánico	DC	4	11.1.4	* Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.
	[I1] Fuego	DC	4	11.1.4	* Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.
	[I*] Desastres Industriales	DC	4	11.1.1,11.1.3,11.2.2,11.2.3	* Se deberían definir y usar perímetros de seguridad en instalaciones de manejo de información. * Se debería diseñar y aplicar seguridad física a oficinas, * Los equipos se deberían proteger contra falla de energía y Otras interrupciones causadas por fallas en los servicios de suministros. * El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debería proteger contra interceptación, interferencia o daño.

Tabla 39 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[I3] Contaminación Mecánica	DC	4	11.2.1	* Los equipos deberían estar ubicados y protegidos para reducir los riegos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado
	[I4] Contaminación Electromagnética	DC	4	11.2.2,11.2.3	* Los equipos se deberían proteger contra falla de energía y otras interrupciones causadas por fallas en los servicios de suministros. * El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debería proteger contra interceptación, interferencia o daño.
	[I5] Avería de Origen Físico o lógico	DC	4	11.2.1,11.2.4	* Los equipos deberían estar ubicados y protegidos para reducir los riegos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. * Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

Tabla 39 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[I6] Corte del suministro eléctrico	DC	4	11.2.2,11.2.3	* Los equipos se deberían proteger contra falla de energía y otras interrupciones causadas por fallas en los servicios de suministros. * El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debería proteger contra interceptación, interferencia o daño.
	[I7] Condiciones inadecuadas de temperatura o humedad	DC	4	11.1.4, 11.2.1	* Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes. * Los equipos deberían estar ubicados y protegidos para reducir los riegos de amenazas y peligros del entorno.
	[E2] Errores del administrador	DC	4	7.2.1,17.2.1	* La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información. * Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Tabla 39 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[E23] Errores de mantenimiento/actualización de equipos	DC	4	11.2.4,12.1.2,17.2.1,	* Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continua. * Se deberían controlar los cambios en la Gobernación, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información. *Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
	E24] Caída del sistema por agotamiento de recursos	DC	4	12.1.3,17.1.2,17.1.3,17.2.1	* Se debería hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. *La Gobernación debería verificar a intervalos regulares los controles de continuidad de seguridad de la información con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

Tabla 39 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[E25] Pérdida de equipos/robo	DC	4	11.1.1,11.1.2, 11.1.3,11.2.1	*Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. *Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. *Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. *Los equipos deberían estar ubicados y protegidos para reducir los riegos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
	[A6] Abuso de privilegios de acceso	DC	4	11.1.2,11.1.3	*Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. *Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

Tabla 39 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[A11] Acceso no autorizado	DC	4	11.1.2,11.1.3	* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. * Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
	[A23] Manipulación de los equipos	DC	4	11.1.2,11.1.3	* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. * Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
	[A24] Denegación de servicio	DC	4	17.1.1,17.1.2,17.1.3	* La Gobernación debería 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 y desastre. *La Gobernación debería establecer, mantener procesos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. * Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Tabla 39 (Continuación)

ACTIVO	AMENAZA	TRATAMIENTO	NIVEL DE CRITICIDAD	CONTROL ISO 27001	SALVAGUARDAS
Servidores NS1 y NS2	[A25] Robo	DC	4	11.1.1,11.1.2,11.1.3,11.2.1	*Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. *Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. * Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. *Los equipos deberían estar ubicados y protegidos para reducir los riegos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

Fuente: La presente investigación

2. DECLARACIÓN DE APLICABILIDAD SOA

Para la declaración de aplicabilidad de la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño, se tuvo en cuenta los siguientes documentos: Los 133 controles en la norma ISO 27002, la evaluación y tratamiento de riesgos. Una vez identificados los riesgos, la declaración de aplicabilidad permitió identificar los controles necesarios documentando si cada uno de estos controles eran aplicables o si ya estaban implementados.

Tabla 40. Declaración de Aplicabilidad

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN					
A.5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	X			La Secretaria de TIC, no tiene definidas una Políticas para la seguridad de la Información, La implementación de las políticas de seguridad debe estar debidamente documentada y para que sirva como guía en la implementación del SGSI
	A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	X			En el momento en que estén creadas las Políticas es necesario revisarlas seguidamente por parte del comité de seguridad de la información.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	X			Cada funcionario de la Secretaria de TIC debe conocer cuáles son sus responsabilidades frente al manejo de la información.
	A 6.1.2 SEPARACIÓN DE DEBERES	X			Es importante separar los deberes y áreas de responsabilidad de cada funcionario de la Secretaria de TIC.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.3 CONTACTO CON LAS AUTORIDADES	X			En caso de alguna emergencia como robo, pérdidas se debe mantener contacto con las autoridades pertinentes.
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	X			Para mantener la información lo más segura posible es necesario mantener contactos apropiados con especialistas en el tema.
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.		X		No se aplica este control debido a que la gestión de proyectos no es un activo de prioridad dentro de la secretaria TIC.
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES		X		El uso de dispositivos móviles no genera amenazas importantes dentro de la entidad debido a que su uso es personal.
	A 6.2.2 TELETRABAJO		X		La Secretaria de TIC no implementa el teletrabajo, por lo tanto, no es necesario el control.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS					
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN		X		La Secretaria de TIC verifica los antecedentes de los candidatos a un empleo antes de la selección, por eso no es necesario el control.
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	X			Dentro de los acuerdos contractuales se debe estipular la seguridad de la información.
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDAD DE LA DIRECCIÓN	X			A las áreas de la Secretaria TIC deben asociarse las responsabilidades frente al Sistema de Gestión de Seguridad de la Información.
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN.	X			Ser competitivos es de gran importancia para la implementación y mantenimiento del SGSI, esto implica que la entidad debe capacitar a los funcionarios frente a los temas de seguridad de la información.
	A.7.2.3 PROCESO DISCIPLINARIO	X			El control es fundamental en cualquier organización, las faltas de los empleados deben ser investigadas y sancionadas.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS					
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A 7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO		X		Cuando se realiza la terminación o cambio de empleo cada funcionario realiza la devolución de sus activos.
A.8 GESTIÓN DE ACTIVOS					
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS		X		La Secretaria de TIC mantiene un inventario de los activos asociados con información e instalaciones de procesamiento de información.
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS		X		Cada activo dentro de la Secretaria de TIC tiene relacionado un responsable de la seguridad.
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	X			Deben existir políticas sobre manejo de la información y de activos las cuales permitan tener claridad acerca de un manejo adecuado.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.8 GESTIÓN DE ACTIVOS					
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	X			Es importante clasificar la información de acuerdo a su valor para evitar su divulgación o modificación no autorizada.
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN		X		La Secretaria de TIC tiene un procedimiento para el etiquetado de la información.
	A 8.2.3 MANEJO DE ACTIVOS	X			Es necesario tener un procedimiento para el manejo adecuado de los activos.
A 8.3 MANEJO DE MEDIOS	A 8.3.1 GESTIÓN DE MEDIOS REMOVIBLES		X		Todos los medios removibles que salen de la gobernación cuentan con un etiquetado de la información.
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS		X		Todos los medios se encuentran almacenados cuando ya no se les da uso.
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS		X		Los medios físicos se encuentra protegido correctamente.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 11 SEGURIDAD FÍSICA Y DEL ENTORNO					
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	X			Se debe garantizar la seguridad de las zonas que manejan información confidencial o crítica (archivo físico, ubicación de servidores, equipos, almacenamiento copias de seguridad etc.).
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	X			Sólo personal autorizado debe acceder a áreas que contengan activos sensibles. (Archivo histórico físico, almacenamiento de copias de seguridad, uso de servidor).
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	X			Los funcionarios de la Secretaría de TIC son los únicos que deben tener acceso a información sensible.
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	X			Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidos contra amenazas físicas y ambientales

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 11 SEGURIDAD FÍSICA Y DEL ENTORNO					
A 11.1 ÁREAS SEGURAS	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	X			Las áreas sobre las que se desarrollan las actividades deben cumplir estándares de seguridad lo cual es muy importante tanto para equipos.
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA			X	En la Secretaría de TIC no existen áreas de despacho y carga
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	X			Es necesario tener protecciones contra daños ambientales, especialmente para los servidores que se maneja al interior de la Gobernación.
	A 11.2.2 SERVICIOS DE SUMINISTRO	X			La integridad de los equipos depende de los controles para la protección antes fallas eléctricas, ya que un fallo de energía puede dejar inutilizable un equipo, dañar su disco duro etc.
	A 11.2.3 SEGURIDAD EN EL CABLEADO	X			Se debe garantizar que las redes de datos no vean afectada su integridad y confidencialidad de los datos que transportan.
	A 11.2.4 MANTENIMIENTO DE EQUIPOS	X			Se debe realizar mantenimiento preventivo, correctivo y detectivo periódico de los equipos como política interna de la entidad.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 11 SEGURIDAD FÍSICA Y DEL ENTORNO					
A 11.2 EQUIPOS	A 11.2.5 RETIRO DE ACTIVOS		X		Ningún activo dentro de la Secretaría de TIC es retirado sin autorización previa.
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES		X		Todo equipo que trabaja fuera de la Gobernación, tiene reglas y restricciones de acceso.
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	X			Al dar de baja un equipo se realiza copia de seguridad mas no se borra la información del equipo y esto puede comprometer la confidencialidad de la Gobernación,
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO		X		En la Secretaría de TIC no existe ningún activo al que no se le de uso.
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	X			Es necesario una Política de Escritorio y pantalla limpia para que sea implementada por todos los funcionarios de la Secretaria de TIC.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 12 SEGURIDAD DE LAS OPERACIONES					
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	X			Para garantizar la continuidad de procesos se debe contar con bitácoras que permitan conocer los procedimientos operacionales especialmente los que tengan que ver con activos esenciales.
	A 12.1.2 GESTIÓN DE CAMBIOS		X		Cuando se realizan cambios en la Gobernación se lleva un control adecuado.
	A 12.1.3 GESTIÓN DE CAPACIDAD	X			Es importante que dentro de las políticas internas sea planificado el crecimiento de la Gobernación para que los recursos sean acordes con el mismo.
	A 12.1.4. SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN		X		Cada área dentro de la Secretaria de TIC está separada de acuerdo a sus funciones y competencias.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 12 SEGURIDAD DE LAS OPERACIONES					**-**
A 12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	X			Se deben tener controles que garanticen que códigos maliciosos no terminen afectando el sistema.
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	X			Respaldar la información garantiza que ante cualquier problema de seguridad se tendrá una fácil recuperación de la información, bases de datos, archivo de contabilidad, archivo de manejo técnico, proyectos, de acuerdo con la política de recuperación.
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	X			Se debe realizar monitoreo de cualquier cambio en los sistemas de información, revisando sus resultados. Revisar todos los registros de las actividades del usuario.
	A12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	X			Se debe tener control sobre los registros de actividad para que no puedan ser alterados (intentos forzosos o no autorizados)

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 12 SEGURIDAD DE LAS OPERACIONES					
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.3 REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR	X			Es muy importante que la actividad de quienes tengan mayores privilegios sean monitoreados.
	A12.4.4 SINCRONIZACIÓN DE RELOJES		X		Todos los relojes de los equipos, servidores y demás sistemas se encuentran debidamente sincronizados
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	X			Como principio de seguridad de la información, se debe contar con controles para la instalación de software, por tanto se debe contar con este control implementado.
A 12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	X			Se debe estar verificando constantemente las vulnerabilidades que puedan presentar los sistemas o tecnologías usadas Y realizar mantenimiento preventivo a los equipos dentro de la Secretaría de TIC.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 12 SEGURIDAD DE LAS OPERACIONES					**-**
A 12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACIÓN DE SOFTWARE	X			Es necesario controlar la instalación de software por parte de los usuarios de tal manera que responda a las necesidades de la entidad.
A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	A 12.7.1 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	X			Como principio de seguridad de la información, explícitamente se debe contar con controles de auditoría, por tanto se debe contar con este control implementado.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN.	X			Es importante que todo nuevo sistema de seguridad especifique los controles necesarios para su implementación.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	X			Como principio de seguridad de la información, y específicamente los sistemas de información que son expuestos a redes públicas, se debe contar con este control implementado.
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	X			Como principio de seguridad de la información, y específicamente en la protección de los servicios de las aplicaciones, se debe contar con este control implementado
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	X			Es necesario establecer Políticas para el desarrollo de software dentro de la Secretaria de TIC.
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	X			Se debe tener control de versiones de aplicaciones para que los cambios sean realizados conforme a necesidades reales de la entidad.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN		X		Se revisa la funcionalidad de las aplicaciones tras realizar cambios para no crear conflictos
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE		X		Se tiene control de cualquier modificación en el software de la entidad.
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	X			Como principio de seguridad informática se deben establecer los principios de construcción de sistemas de información seguros, por tanto se debe contar con este control implementado.
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO		X		Los lugares de desarrollo de software cuentan con un ambiente adecuado.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	X			Los servicios de desarrollo tercerizados se deben controlar adecuadamente, por tanto se debe realizar un seguimiento a estos.
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	X			Como principio de seguridad informática se deben realizar pruebas de seguridad a los sistemas de información durante el desarrollo.
	A 14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	X			Como principio de seguridad informática se deben realizar pruebas de aceptación a los sistemas de información.
A 14.3 DATOS DE PRUEBA	A 14.3 DATOS DE PRUEBA	X			Como principio de seguridad de la información se deben proteger los datos de prueba adecuadamente en los sistemas de información.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.15 RELACIONES CON LOS PROVEEDORES					
A. 15.1 RELACIONES CON LOS PROVEEDORES	A 15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	X			Como principio de seguridad de la información, la Entidad debe contar con la Política de seguridad de la información en la relación con los proveedores a fin de mitigar los riesgos que se puedan presentar durante la prestación de los servicios.
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	X			Es necesario establecer requisitos de seguridad de la información con proveedores que puedan tener acceso a los componentes de TI.
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	X			Es importante establecer acuerdos con proveedores para tratar los riesgos de seguridad de la información.

Tabla 40. (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.15 RELACIONES CON LOS PROVEEDORES					
A 15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES		X		La secretaria de TIC realiza el seguimiento a los servicios de los proveedores.
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	X			Los cambios en los servicios de los proveedores se deben gestionar.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	X			Se debe establecer quién es el responsable de manejar determinado tipo de incidente para que sea mucha más rápida la respuesta.
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	X			Como principio de seguridad de la información la Entidad debe gestionar adecuadamente los eventos de seguridad de la información.

Tabla 40 (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	X			Como principio de seguridad de la información la Entidad debe reportar adecuadamente las debilidades de seguridad de la información, por tanto se debe contar con este control implementado.
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	X			Como principio de seguridad de la información la Entidad debe evaluar los eventos de seguridad de la información.
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	X			Como principio de seguridad de la información la Entidad debe dar respuesta a los incidentes de seguridad de la información, por tanto se debe contar con este control implementado.
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	X			Se debe poder establecer el costo de un evento de seguridad de la información.

Tabla 40. (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	X			Se deben tener mecanismos para determinar la forma como se debe actuar contra personas que se les compruebe la generación de eventos de seguridad informática.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO					
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	X			La Entidad debe contar con los requisitos establecidos para garantizar la continuidad del servicio en situación de crisis o desastre.
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SI	X			La Entidad debe establecer los lineamientos para iniciar un mantenimiento al momento de una situación adversa.
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	X			La Entidad debe contar con controles de revisión de dispositivos al momento de situaciones adversas.

Tabla 40. (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO					
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	X			Como principio de la información se debe contar con redundancias en las instalaciones de procesamiento de información para tener disponibilidad de la información.
A. 18 CUMPLIMIENTO					
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES		X		La Gobernación de Nariño por ser una entidad pública es consciente de sus obligaciones legales para garantizar el cumplimiento de las mismas.
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL		X		La Gobernación garantiza el uso de cualquier material y/o software de acuerdo a las licencias definidas para los mismos.

Tabla 40. (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 18 CUMPLIMIENTO					
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.3 PROTECCIÓN DE REGISTROS	X			Se debe garantizar la integridad de los registros importantes para evitar cualquier pérdida de información.
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES		X		La Gobernación garantiza la protección de los datos personales en concordancia con requerimientos de carácter legal.
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	X			Falta de controles cifrados para asegurar concordancia con la legislación vigente teniendo en cuenta el tipo de información que se maneja.
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	X			Se incluye como parte integral de los requisitos del estándar para el SSI en la entidad.

Tabla 40. (Continuación)

	DECLARACIÓN DE APLICABILIDAD (SOA)				
Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**				
OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACIÓN**
		SI	**NO**		
A. 18 CUMPLIMIENTO					
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.2. CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	X			Por disposición del Gobierno Nacional, la seguridad de la información debe estar presente en los procesos de la Entidades del Estado.
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	X			Es importante que los procedimientos de seguridad estén en concordancia con los estándares definidos para los mismos.

Fuente: La presente investigación

3. PRUEBAS REALIZADAS

Para las pruebas se realizó un proceso denominado ethical hacking que expone los problemas de seguridad que existían en los sistemas informáticos. Para ello se trabajó con las principales herramientas de seguridad y se trató algunas vulnerabilidades importantes. Este proceso se realizó con el sistema operativo Kali Linux, 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.

Kali Linux: Es una distribución de Linux, su propósito fue la auditoria y seguridad informática. Kali Linux persigue tener la mejor colección de herramientas de código abierto destinadas a pruebas de penetración, bajo un análisis y con el uso de diferentes herramientas que cumplían este propósito, así que se buscaron nombres de domino, direcciones IP, posibles nombres de usuario, bases de datos públicas, se buscaron las versiones de los sistemas operativos, los parches de seguridad, etc.

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

Nmap: Es una herramienta de escaneo de redes que permitió identificar qué servicios se estaban ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, entre otros.

Zenmap: Es multiplataforma, libre y gratuito**,** Zenmap es la interfaz gráfica oficial de Nmap, el conocido programa de código abierto para hacer escaneo de puertos a fondo de cualquier equipo conectado. Zenmap proporciono una interfaz gráfica para ejecutar los diferentes tipos de análisis de puertos.

Con todas estas herramientas se realizó las Pruebas Penetración Testing obteniendo los siguientes resultados:

Pruebas con la herramienta Kali Linux

Se utilizó una máquina virtual en la que se instaló el sistema operativo Kali Linux, se ejecutó la terminal en donde se utilizó el comando ping al dominio de la Gobernación de Nariño www.nariño.gov.co el cual nos arrojó la siguiente dirección IP:

ping www.narino.gov.co

IP 66.70.193.68

Con la dirección IP obtenida se utilizó la herramienta nmap que se encuentra en Kali Linux y se ejecutó el comando **nmap 66.70.193.68** en la terminal obteniendo el siguiente resultado:

Tabla 41. Resultados Comando Nmap

PORT	STATE	SERVICE
21	Open	**ftp**
22	Open	**ssh**
25	Open	**smtp**
53	Open	**domain**
80	Open	**http**

Tabla 41 (Continuación)

PORT	STATE	SERVICE
106	open	**pop3pw**
110	open	**pop3**
111	open	**rpcbind**
143	open	**imap**
443	open	**https**
445	filtered	**microsoft-ds**
465	open	**smtps**
993	open	**imaps**
995	open	**pop3s**
8443	open	**https-alt**

Fuente: La presente investigación

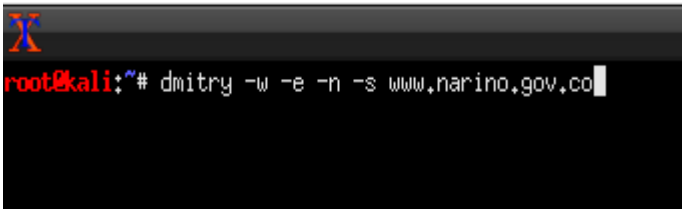
nmap informó que el servidor tiene 14 puertos abiertos y también informó cuales son los servicios ofrecidos**,** son los puertos de conexión remota segura (ssh) por el puerto 22, el servicio web por el puerto 80 y el servicio de webseguro por el puerto 443.

El único puerto que estaba filtrado es el puerto 445/TCP que corresponde al servicio de microsoft-ds, el filtrado puede provenir de un dispositivo de cortafuegos dedicado, de las reglas de un enrutador, o por una aplicación de cortafuegos instalada en el propio equipo. Estos puertos suelen frustrar a los atacantes, porque proporcionaron muy poca información.

En la terminal de Kali Linux se utilizó el comando dmitry para obtener todos los subdominios relacionados al dominio narino.gov.co

 # dmitry –w –e –n –s www.narino.gov.co

Figura 24. Ejecución Comando Dmitry



Fuente: Imagen tomada del resultado de ejecutar Dmitry en la terminal de Kali Linux

Este comando permitió obtener toda la información posible sobre un host, esta incluyo 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, los subdominios asociados y sus respectivas direcciones IP. También se obtuvo los siguientes hosts con sus respectivas IP

HostName: www.narino.gov.co

Host IP: 66.70.193.68

HostName: datos.narino.gov.co

Host IP: 198.100.153.250

HostName: ganadatos.narino.gov.co

Host IP: 198.100.153.250

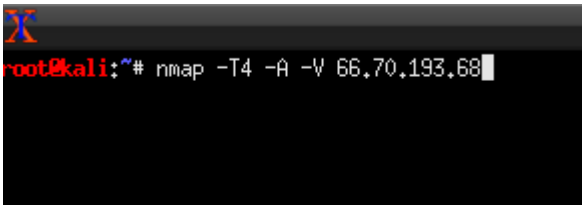
HostName: aplicaciones.narino.gov.co

Host IP: 190.14.247.68

En la terminal de Kali Linux se ejecutó el siguiente comando la opción –T4 del comando nmap el cual acelero el proceso de búsqueda y escaneo, mientras que la opción –A permitió identificar el sistema operativo de los servidores atacados y la opción –v arroja la versión de los servicios instalados en el mismo.

#nmap –T4 –A –v 66.70.193.68

Figura 25 Ejecución Comando Nmap



Fuente: Imagen tomada del resultado de ejecutar Nmap en la terminal de Kali Linux

Dando como resultado el estado, el servicio y la versión de los puertos.

En la terminal de Kali Linux se ejecutó el siguiente comando: **whois narino.gov.co** el cual trato de recolectar la mayor parte de información posible acerca del dominio.

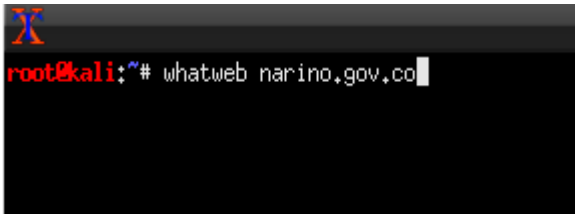
Figura 26 Ejecución Comando Whois

Fuente: Imagen tomada del resultado de ejecutar whois en la terminal de Kali Linux

Dando como resultado la información sobre el Dominio, la ubicación de la empresa, número de teléfono, correo electrónico, nombre de la persona de contacto “Brenda Rivas Martínez” contacto técnico y dns del registrante del dominio, en este caso .co Internet S.A.S.

En la terminal de Kali Linux se ejecutó el siguiente comando: **whatweb narino.gov.co** el cual mostro la información del sitio web.

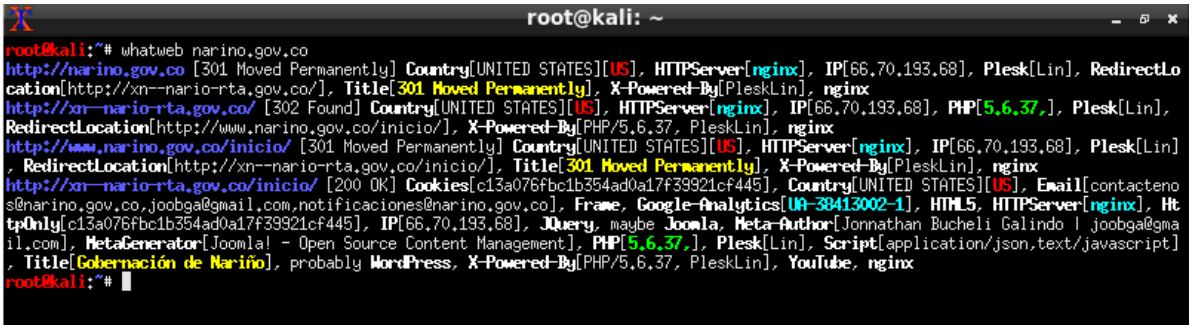
Figura 27 Ejecución Comando Whatweb



Fuente: Imagen tomada del resultado de ejecutar whatweb en la terminal de Kali Linux

Dando como resultado el escaneo del sitio web de la Gobernación de Nariño

Figura 28. Resultado Comando Whatweb



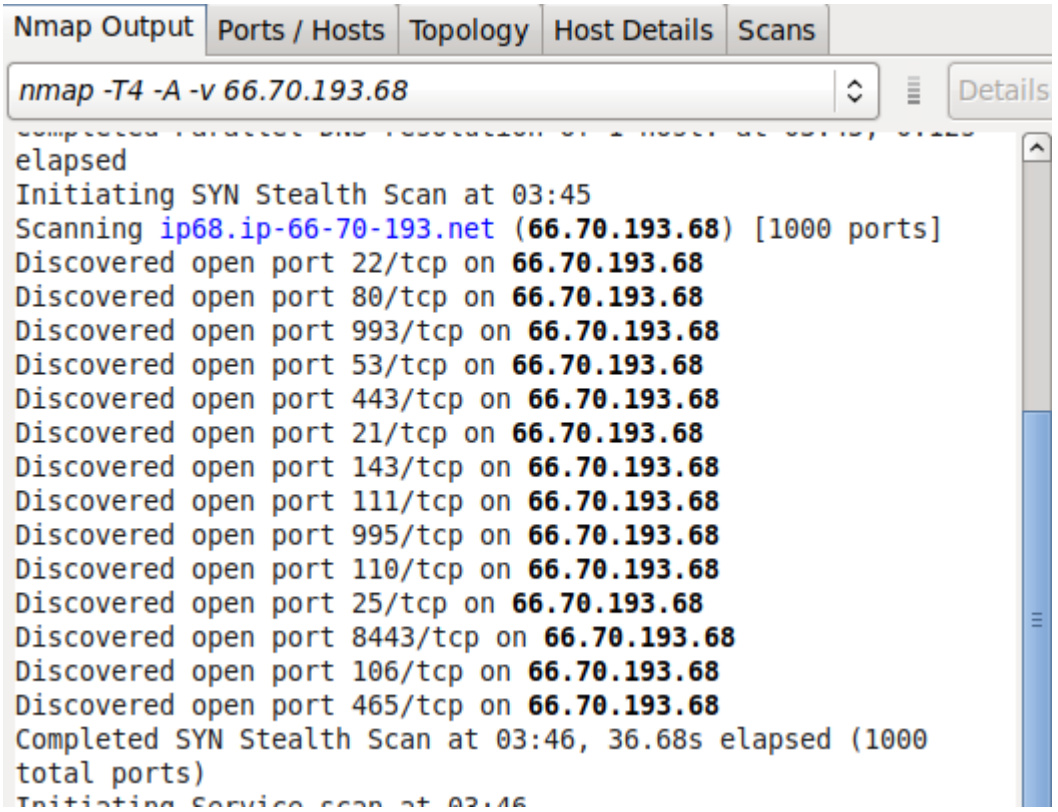
Fuente: Imagen tomada del resultado de ejecutar whatweb en la terminal de Kali Linux

Pruebas con la Herramienta Zenmap

Ahora se realizaron las pruebas con la herramienta Zenmap, en la interfaz gráfica se ejecutó el siguiente comando: **nmap –T4 –A –v (IP),** donde (IP) es la dirección IP del dominio de la Gobernación de Nariño.

nmap –T4 –A –v 66.70.193.68

Figura 29 Ejecución Comando Nmap en Zenmap



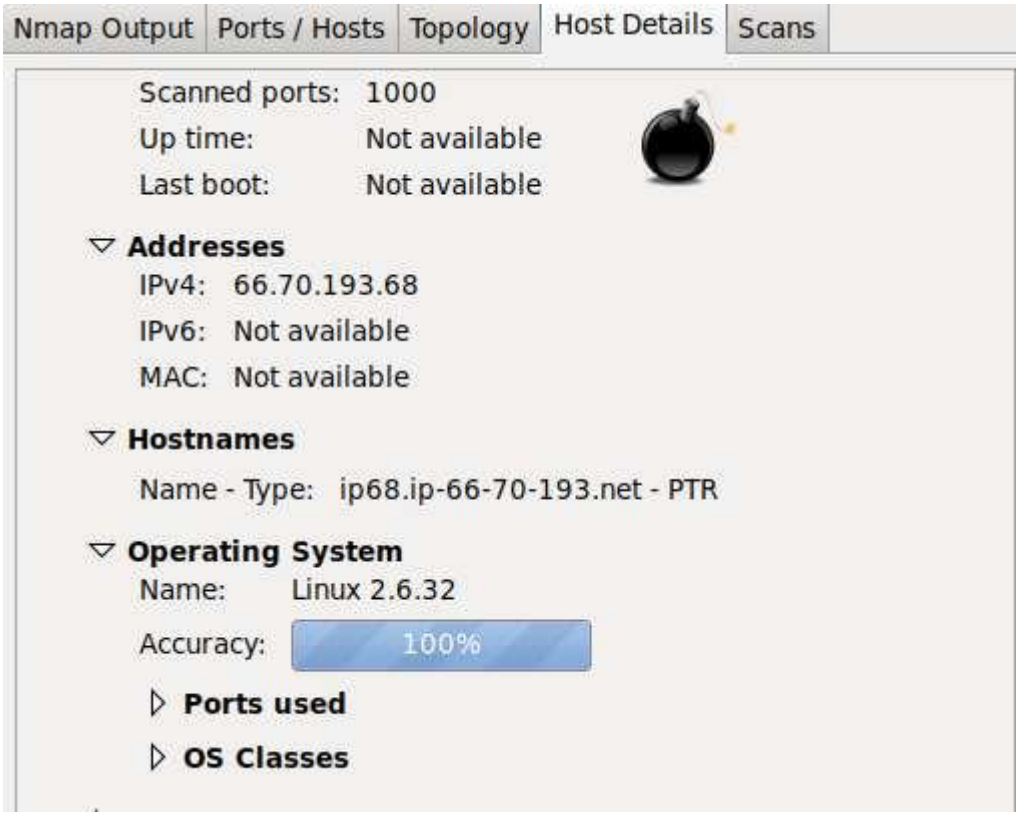
Fuente: Imagen tomada del resultado de análisis de puertos realizado con Zenmap

Aquí se evidencia los puertos abiertos, pero en entorno gráfico junto con el nombre de cada servicio.

En la herramienta Zenmap, en la interfaz gráfica se ejecutó el siguiente comando**:** **nmap -O (IP)**

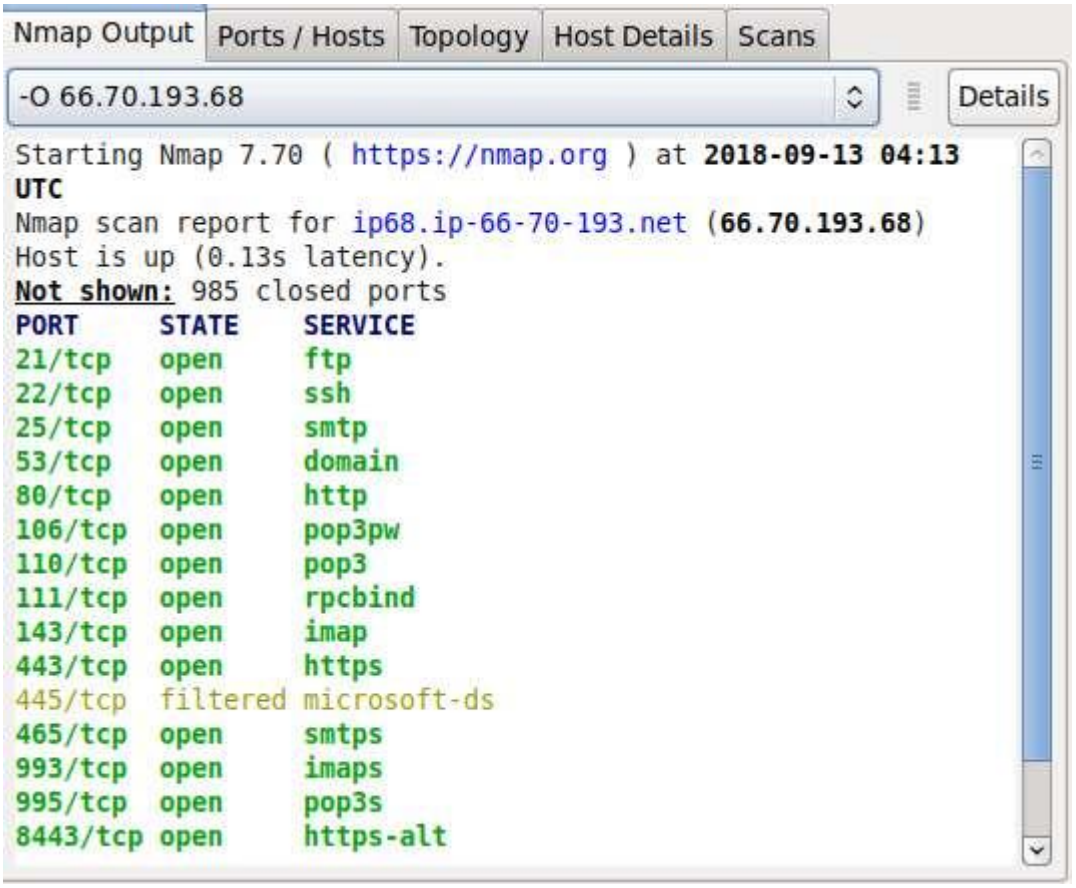
nmap -O 66.70.193.68

Figura 30 Ejecución Comando Nmap –O



Fuente: Imagen tomada del resultado de análisis de puertos realizado con Zenmap

Figura 30 (Continuación)



Fuente: Imagen tomada del resultado de análisis de puertos realizado con Zenmap.

Dando como resultado el sistema operativo que se está utilizando en el objetivo, en este caso el Sistema Operativo Utilizado es Linux 2.6, también se observó que algunos puertos se encuentran cerrados.

HALLAZGOS DE LAS PRUEBAS REALIZADAS

- Con las pruebas realizadas al servidor de la Gobernación nariño.gov.co, se pudo verificar que existían varios puertos abiertos, además conocer los servicios que se encuentran publicados en este servidor.
- Con una de las herramientas de Kali Linux se pudo identificar el Sistema Operativo con el que trabajaba la Gobernación, esta puede ser una vulnerabilidad que permitiría a los atacantes iniciar una búsqueda de herramientas de explotación específicas, según el sistema operativo que se encuentre tras los equipos explorados.
- Mediante la herramienta Zenmap se realizó el mapeo de red, a partir de las direcciones IP obtenidas, los resultados obtenidos fueron conocer en detalle los puertos, el estado y sus servicios que están abiertos.
- Se realizó pruebas de inyección SQL a la página de la Gobernación de Nariño, teniendo como resultado una página segura o poco vulnerable ante ataques de este tipo.

.

4. CONCLUSIONES

- De la metodología Magerit versión 3.0 aplicada en este proyecto para la gestión de riesgos, se pudo concluir que esta metodología fue completa y permitió clasificar los activos informáticos de la gobernación de manera ordenada y la identificación de las vulnerabilidades y las amenazas, la evaluación de riesgos y las salvaguardas para mitigar los riesgos y puede ser aplicada a cualquier empresa u organización.
- De la Norma Internacional ISO/IEC 27001/2013 y la Norma ISO/IEC 27002/2013 aplicadas, se concluye que estas normas permitieron el diseño, implementación e implantación del SGSI en cada una de las fases del ciclo de mejora continua PHVA teniendo en cuenta los riesgos identificados en cada uno de los dominios aplicados y determinando la existencia de los controles de acuerdo a dicha norma en la Gobernación de Nariño.
- De los conceptos de seguridad informática y la seguridad de la información aplicados en la Gobernación de Nariño, se concluye que a pesar de tener documentadas algunas políticas y procedimientos de seguridad, estos no se habían comunicado y aplicado, ya que se detectaron muchas falencias en cuanto a la exposición de los activos informáticos a factores de amenaza que pueden aprovechar las vulnerabilidades existentes.
- Respecto al talento humano de la Gobernación de Nariño, se concluye que a pesar de que conocían la existencia de algunas políticas de seguridad para la protección de los activos informáticos, estas no habían sido aplicadas por lo que continuaban las vulnerabilidades que pudieron ser explotadas por usuarios internos y externos.
- Respecto a la planeación de actividades para el diseño del SGSI, se concluyó que todas las actividades fueron planeadas anticipadamente en diferentes eventos por la secretaría de las TIC, lo que garantizo que la información

recolectada este completa y sea veraz, y se garantizó la participación de los usuarios en el proceso de Diseño y la Implementación del SGSI.

- Respecto al documento del diseño de Políticas y Procedimientos de Seguridad Informática y de Información mediante el SGSI en la Secretaría de TIC de la Gobernación de Nariño, se concluyó que estas políticas y procedimientos aplicados por los usuarios permitieron mejorar los procesos y minimizar las vulnerabilidades existentes y contribuir a fortalecer la continuidad de los servicios que presta la Gobernación de Nariño a los usuarios y ciudadanos.

5. RECOMENDACIONES

- Respecto a los resultados del diseño del SGSI, se recomendó capacitar al personal en cuanto a las políticas de seguridad Informática y de la Información permitiendo con ello minimizar las márgenes de riesgo de los activos de la Gobernación de Nariño.
- Respecto a la difusión del SGSI, se recomendó realizar campañas de concientización entre los funcionarios de la Gobernación desde los guardias de seguridad hasta los administrativos, con la finalidad de que ellos comprendan:
  - ✓ Que es información confidencial, secreta, sensible o clasificada, y porque dicha información está catalogada de esta forma.
  - ✓ Conozcan las implicaciones legales que puedan tener si comparten, copian o divulgan dicha información, en la que se pueden presentar consecuencias desde una amonestación, el despido o incluso la cárcel.
  - ✓ Hacer revisiones de las contrataciones para verificar que dichos contratos tengan cláusulas de confidencialidad de la información y protección de los datos.
- Respecto al proceso realizado de análisis y evaluación de riesgos de seguridad y la identificación de controles, se recomendó que haya una revisión periódica de las amenazas y riesgos ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas.

BIBLIOGRAFÍA

ALONSO, David. Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base a normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional. Trabajo de grado Ingeniería en Informática. Cundinamarca.: Universidad de la Sabana. 2014.

BALDECCHI, Rodrigo. Implementación efectiva de un SGSI ISO 27001 [En línea]. Montevideo: Sonda, 4 de Septiembre de 2014. Disponible en: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf.

CAO, Javier. Sistemas de Gestión Seguridad de la Información [En línea]. España: Blog spot, Junio de 2014. Disponible en: http://sgsi-iso27001.blogspot.com.

Guía de Implantación de un Sistema De Gestión de Seguridad de la Información Une–ISO/IEC 27001:2007 con la herramienta GLOBAL SGSI [En línea]. Disponible en: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf

ISO27000. El portal de ISO 27001 en español [En línea]. Octubre de 2005. Disponible en Internet: http://www.iso27000.es/.

PATIÑO, Luis. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR. Tesis de

Especialización en Seguridad Informática. San Juan de Pasto.: Universidad Nacional Abierta y a Distancia UNAD. 2014. 130p.

CONTRERAS. Lidia. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la dirección de sistemas de la Gobernación de Boyacá. Tesis de Especialización en Seguridad Informática. Tunja.: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas e Ingeniería. 2017. 300p.

SARRIA, 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. Tesis de Especialización en Seguridad Informática. Florencias.: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2015. 175p.

BUENO. Shirley. Diseñar de un sistema de gestión de seguridad de la información mediante la norma ISO 27001 en el Instituto Colombiano de Bienestar Familiar Centro Zonal Virgen y Turístico de la Regional Bolívar. Tesis de Especialización en Seguridad Informática. Cartagena.: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2015. 155p.

HENAO, Jaime. Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 para la empresa USOMET LTDA. En la ciudad de Ibagué. Tesis de Especialización en Seguridad Informática. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2016. 130p.

PULIDO, Ana Milena y MANTILLA, Jenith. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina tic de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Tesis de Especialización en Seguridad Informática. Fusagasugá.: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2016. 11p.

ANEXOS

ANEXO A Políticas y Procedimientos de Seguridad Informática y de Información Para la Gobernación de Nariño.

GOBERNACIÓN DE NARIÑO

CONTENIDO

1. INTRODUCCIÓN

La Gobernación de Nariño reconoce la importancia de identificar y proteger sus activos informáticos y de información, así mismo determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, por lo tanto es necesario implementar controles y procedimientos que permitan proteger la continuidad de los niveles de competitividad, de gestión pública, y de conformidad legal necesarios para alcanzar las metas administrativas y del plan departamental de desarrollo Nariño Corazón del mundo 2016-2019.

El presente documento estableció las políticas y procedimientos de seguridad informática y de la información definidas por la Gobernación de Nariño. Para la elaboración del mismo, se tomaron como referencia la norma ISO 27001:2013 y las recomendaciones del entandar ISO 27002: 2013.

Las políticas de seguridad presentes en este documento son de gran importancia para el Sistema de Gestión de Seguridad de la Información SGSI, ya que permitieron minimizar los riesgos encontrados en la entidad y garantizar la integridad, confidencialidad y disponibilidad de la información.

2. OBJETIVO

Definir y explicar las políticas y procedimientos de seguridad informática y de información, permitiendo la protección de los activos de la entidad.

3. ALCANCE

Esta política es de aplicación en el conjunto de Secretarías, Departamentos, subsecretarías, oficinas y dependencias que componen la Gobernación de Nariño, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal de Gobernación, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

4. DEFINICIONES

Confidencialidad: Los activos de información solo pueden ser accedidos y custodiados por usuarios que cuente con permisos para ello.

Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que cuenten con los permisos adecuados.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Trazabilidad: Las actuaciones de la entidad pueden ser imputadas exclusivamente a la dicha entidad.

Activo: Son elementos que tienen valor para una organización tales como: datos/información, servicios, aplicaciones (software), equipos (hardware), medios de almacenamiento (físico y electrónico), equipamiento auxiliar, instalaciones y personal.

Amenaza: Es cualquier situación que se puede presentar en la entidad, dañando un activo mediante la presencia de una vulnerabilidad.

Vulnerabilidad: Debilidad de un activo que puede ser aprovechada por una amenaza.

Riesgo: Es el daño que se le puede presentar a un activo cuando se encuentra desprotegido.

Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Control: Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

5. COMITÉ PARA LA SEGURIDAD DE LA INFORMACIÓN.

La Gobernación de Nariño, proyecta la organización de la Seguridad de la información, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

Secretario de Gobierno o Líder GEL

Secretaria General del Departamento.

Subsecretaria Talento Humano

Jefe Oficina de Control Interno de la Gestión

Jefe Archivo General

Oficina de Gestión Tecnológica.

Los integrantes del comité deberán revisar y actualizar anualmente la Política de Seguridad de la Información, presentando los proyectos o propuestas al Gobernador del Departamento para su aprobación mediante acto administrativo correspondiente.

Los Secretarios, Directores de departamento o Jefes de Dependencias u Oficinas, deben identificar y valorar los activos de información que pertenecen a las respectivas áreas, y deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados y adoptados por el Gobernador.

6. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Establecer las políticas y procedimientos de seguridad de información para el uso de Tecnologías de Información y comunicación de la Secretaria de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño, donde se denote lo siguiente: Objetivos organizacionales en donde se proteja los activos de información, responsabilidades y los derechos que se deben conocer y cumplir los funcionarios internos y externos, propietarios y administradores de la infraestructura tecnológica para lograr que los recursos tecnológicos de la entidad presten su servicio de manera accesible, confiable y oportuna.

Responsabilidades Asignadas: La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Gobernación de Nariño, independiente del tipo de vinculación, el área o dependencia a la cual se encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El Gobernador del Departamento de Nariño aprueba esta Política y es responsable de la aprobación y adopción de las actualizaciones.

El Comité de Seguridad de la Información de la entidad es responsable de revisar, proyectar y proponer a la administración departamental en cabeza del Gobernador, para su aprobación, el documento de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de Información de la Gobernación de Nariño. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Administración Departamental.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la socialización, implementación, seguimiento y control de la política.

Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilidad de mantener de forma integral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Quien ejerza el cargo de Subsecretaria de Talento Humano, deberá notificar a todo el personal que se vincule con la Gobernación de Nariño, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación y socialización de la presente Política y de los cambios o actualizaciones que en ella se produzcan a todo el personal, a través de la suscripción de los acuerdos de Confidencialidad y de labores de capacitación continua en materia de seguridad según los lineamientos establecidos por el Comité de Seguridad de la Información de la Entidad.

Los profesionales universitarios y equipo de trabajo de la Oficina de Gestión Tecnológica en coordinación con la Secretaría General del Departamento deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información e infraestructura tecnológica de la Entidad.

El Archivo General del Departamento en colaboración con la oficina de Gestión tecnológica determinara el inventario de activos de información y recursos

tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Almacén General del Departamento en responsabilidad de los respectivos líderes.

Quien ejerza el cargo de Director@ del Departamento Administrativo de Contratación verificará que los contratos, convenios u otra documentación de la entidad con servidores públicos y con terceros incluya los lineamientos de la Política de Seguridad de la Información de la Entidad.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

La Oficina de Control Interno de la Gestión, es responsable de realizar seguimiento y control periódico sobre información contenida en documentos, sistemas de información y/o actividades vinculadas con la gestión de activos de información. Es responsabilidad de esta área informar sobre el cumplimiento de los lineamientos y medidas de seguridad de la información establecidas por esta Política, y normas adicionales vigentes.

7. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

7.1 ORGANIZACIÓN INTERNA

Objetivo:

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Gobernación.

Política:

La Secretaría de TIC, Innovación y Gobierno abierto debe conformar el Comité para la Seguridad de la Información conformado por Directores y coordinadores de la Gestión Tecnológica.

Los integrantes del comité deberán revisar y actualizar anualmente la Política de Seguridad de la Información, presentando los proyectos o propuestas al Gobernador del Departamento para su debida aprobación.

8. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

8.1 ANTES DE ASUMIR EL EMPLEO

Objetivo:

Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Política:

Todos los empleados de la Gobernación de Nariño deberán conocer los términos y las condiciones del contrato laboral haciendo énfasis en los aspectos relativos a la seguridad de la información y se debe verificar que los contratos estén firmados .El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento.

8.2 DURANTE LA EJECUCIÓN DEL EMPLEO

Objetivo:

Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Política:

La Secretaría de TIC deberá exigir que los empleados y contratistas cumplan a cabalidad con las políticas de seguridad establecidas por la Gobernación. Para esto debe darles a conocer las políticas y procedimientos pertinentes para su cargo, así mismo capacitara e informara cuando se presenten modificaciones y será estricta en el cumplimiento de las mismas, tomando las medidas disciplinarias o legales del caso, cuando dichas políticas no sean cumplidas por el personal.

9. POLÍTICAS DE GESTIÓN DE ACTIVOS

9.1 RESPONSABILIDAD POR LOS ACTIVOS

Objetivo:

Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

Política:

La Gobernación de Nariño deberá implementar reglas para el uso aceptable de los activos informáticos, esto implica la aceptación por parte de los usuarios, de las normas, políticas y estándares establecidos para garantizar la seguridad informática. Este trámite de sebe estandarizar según las normas de calidad, para el cuidado, buen manejo y entrega definitiva de los activos.

9.2 CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo:

Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la Gobernación.

Política:

Cada una de las dependencias de la Gobernación de Nariño deberá clasificar su información sea física o electrónica, de acuerdo a sus necesidades para compartir o restringir la información, igualmente deben existir procedimientos para el adecuado manejo de todos los activos en la organización.

10. POLÍTICAS SEGURIDAD FÍSICA Y DEL ENTORNO

10.1 ÁREAS SEGURAS

Objetivo:

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Gobernación de Nariño.

Política:

La Secretaría de TIC definirá las áreas restringidas las cuales se identifican porque allí se almacenan, se procesan o utilizan activos de tecnología e informática, activos considerados como críticos con un grado de confidencialidad.

El acceso de personal externo a áreas protegidas se limitará. Este se dará cuando sea necesario y en acompañamiento de personal autorizado. Se debe llevar un registro del ingreso y salida del personal del área protegida, identificando hora, fecha, motivos de ingreso, identificación del personal que ingresa, así como del acompañante autorizado.

Para la seguridad física a oficinas e instalaciones, definirá:

- La ubicación segura de los equipos de soporte como son los equipos, impresoras y escáner.
- El bloqueo de los equipos de cómputo cuando los usuarios están fuera de su sitio de trabajo.
- Control de movimientos para los equipos portátiles
- Control de la utilización de discos duros externos, memorias USB.
- El no consumo de comida y bebidas en la sala de comunicaciones y oficinas.
- Almacenamiento bajo llave de documentos de carácter confidencial y crítico.

La Gobernación dentro de su Dirección administrativa de Gestión del riesgo de desastres deberá establecer las políticas necesarias para proteger al personal como los activos de información en caso de desastres naturales. Para ello deberá demarcar las zonas seguras, así como dotarlas con extintores, igualmente deberá evaluar las condiciones en las que se encuentran estas zonas seguras con el fin de adecuar los diseños en pro de evitar inundaciones y/o riesgos eléctricos.

El trabajo en áreas seguras, se fortalece estableciendo barreras físicas y de acceso a estas áreas, para ello la Gobernación definirá que:

- Ningún funcionario deberá permanecer en un área segura fuera del horario normal de trabajo.
- Los accesos a las zonas restringidas deberán ser controlados y asignados de acuerdo a sus roles y responsabilidades.
- Las zonas identificadas como restringidas deberán contar con extintores y equipo que permita controlar incidentes como incendios.

10.2 EQUIPOS

Objetivo:

Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Política:

Para la protección de los equipos y mantener su vida útil se implementarán los siguientes lineamientos:

- Se establecerán normas para el consumo de alimentos en los puestos de trabajo.
- Se realizará monitoreo permanente al ambiente con el fin de mantener las temperaturas adecuadas a cada uno de los centros de procesamiento.

- Ubicar los equipos de cómputo de tal forma que se impida que la información sea visible por terceros.

Es necesario que los servicios de suministro que soportan todo el procesamiento de información como son el servicio de energía, UPS, equipos de comunicación entre otros se estén monitoreando y realizando mantenimiento preventivo para identificar fallas y corregirlas, y así mitigar los impactos que la no prestación de estos servicios pudiera ocasionar en los servicios de procesamiento con los cuales hoy cuenta la Gobernación.

El cableado estructurado de la Gobernación debe estar diseñado de tal forma que soporte los servicios tecnológicos y de comunicaciones que requiere, su diseño debe estar documentado de tal forma que se identifique la topología, los puntos, la categoría de los cables y la tecnología utilizada. Dentro de esta estructura se debe definir que la alimentación eléctrica debe estar separada del cableado estructurado con el fin de evitar interferencias.

Garantizar la disponibilidad e integridad de todos los componentes Hardware y Software de la entidad mediante un adecuado mantenimiento preventivo y correctivo de tal manera que los procesos normales de la entidad no se vean afectados por fallas en los equipos de cómputo.

El mantenimiento preventivo debe definirse dentro de un cronograma donde se establezca la ubicación del equipo y la clase de mantenimiento que se le hará, si es físico y/o lógico. El personal que realice los mantenimientos debe ser capacitado y autorizado, ya que tiene acceso a información sensible, pública, restringida, la cual debe conservar y proteger mientras realiza estas actividades.

Dentro de las hojas de vida de cada equipo se debe consignar la novedad de mantenimiento realizada de forma detallada, igualmente llevará libro de bitácora para registrar los mantenimientos realizados según cronograma.

Antes de dar de baja un equipo o reasignarlo, se debe eliminar la información sensible que este contenga, con el fin de evitar la pérdida o recuperación de

información no autorizada, igualmente se debe desinstalar cualquier software, de tal forma que se evite tener problemas de licenciamiento.

La Gobernación de Nariño deberá adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Desconectar de la red / sistema / servicio los computadores personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo.
- Bloquear las impresoras o protegerlas de alguna manera del uso no autorizado fuera del horario normal de trabajo.

11. POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES

11.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Objetivo:

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Política:

La Gobernación a través de la Secretaria de TIC, documentará y mantendrá actualizados los procedimientos operativos en ésta política, los cuales deben ser solicitados y autorizados por el área que los requiera. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:
Procesamiento y manejo de la información.
Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
Restricciones en el uso de utilidades del sistema.
Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.
Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- Instalación y mantenimiento de las plataformas de procesamiento.
- Monitoreo del procesamiento y las comunicaciones

- Inicio y finalización de la ejecución de los sistemas.
- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- Uso del correo electrónico.
- Gestión de cambios

La Secretaría de TIC deberá realizar monitoreo y análisis permanente a toda su infraestructura tecnológica de procesamiento de información, con el fin de identificar el estado y la utilización de todos los recursos.

Con esto se busca optimizar los recursos existentes, y apreciar las proyecciones de crecimiento, con el fin de identificar las necesidades y asegurar que la infraestructura esté en las condiciones necesarias para atender la demanda existente y la futura.

11.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Objetivo:

Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Política:

La secretaria de TIC definirá e implementará controles de detección y prevención para la protección contra software malicioso, además desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado
- Instalar y actualizar periódicamente software de detección y reparación de virus.
- Tener las últimas actualizaciones de seguridad disponibles en los sistemas.
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Gobernación, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a estos.

11.3 COPIAS DE RESPALDO

Objetivo:

Proteger contra la pérdida de datos

Política:

La Gobernación deberá asegurar que la información de los funcionarios se mantenga protegida contra pérdidas, alteración o divulgación por actos accidentales o malintencionados o por fallas de los equipos y/o redes. Para ello, deberá establecer Políticas para realizar las copias de seguridad a los servidores y bases de datos que soportan los activos de información de la entidad.

Estas Políticas deben ser explicitas en indicar la periodicidad y el tiempo con que se deben realizar las copias, definir los dispositivos de almacenamiento, la

identificación que debe llevar cada copia, el lugar de almacenamiento, la responsabilidad de realizar las copias y sus actualizaciones por evolución de tecnología.

11.4 REGISTRO Y SEGUIMIENTO

Objetivo:

Registrar eventos y generar evidencia

Política:

Se deben elaborar registros de auditoría que contengan excepciones, fallas y otros eventos relativos a la seguridad de la información.
Los registros de auditoría deberán incluir:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad o ubicación del equipo, si se hubiera dispuesto identificación automática para la misma.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

El propietario de la información o en su defecto quien sea propuesto por el Comité para la Seguridad de la Información, definirá un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.
La secretaría de TIC y los propietarios de la información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.
La Secretaría de TIC asegurará el registro y la protección de las actividades realizadas por los administradores y operadores en los sistemas, incluyendo según corresponda:

- Tiempos de inicio y cierre del sistema.
- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
- Ejecución de operaciones críticas
- Cambios a información crítica

11.5 CONTROL DE SOFTWARE OPERACIONAL

Objetivo:
Asegurarse de la integridad de los sistemas operacionales.

Política:
Únicamente el personal de la secretaría de TIC deberá realizar los procesos de instalación, desinstalación, actualización y/o modificación de software; ningún usuario que no pertenezca a dicha dependencia está autorizado para realizar ninguna de las anteriores gestiones sobre el software.
Deberá solicitarse a la Secretaria de TIC cualquier requerimiento que implique la modificación o cambio de software y estos deberán ser debidamente documentados por el área encargada con el fin de soportar los cambios realizados.

11.6 GESTIÓN DE VULNERABILIDAD TÉCNICA

Objetivo:
Prevenir el aprovechamiento de las vulnerabilidades técnicas

Política:
La Gobernación establecerá un procedimiento para la controlar las vulnerabilidades técnicas de los sistemas de información, el cual deberá:

- Contar con un inventario detallado, clasificado y actualizado de los activos de información.
- Disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas.
- Realizar un análisis detallado a los activos de información para identificar posibles vulnerabilidades con el fin de definir y aplicar las acciones apropiadas que permitan minimizar el impacto de las amenazas sobre la entidad.

Los usuarios de la Gobernación deben abstenerse de instalar cualquier tipo de software en sus computadores, de requerirlo deben solicitarlo a la Secretaria de TIC quien es la responsable de la instalación de los programas en todos los computadores de la Gobernación. Todo software que se instale en los computadores de la Gobernación deberá contar con su respectiva licencia y la instalación solo deberá estar permitida en equipos pertenecientes e la entidad.

11.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

Objetivo:

Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos

Política:

La realización de actividades de auditoría que involucren verificaciones de los sistemas en producción, implican una planificación de los requerimientos y tareas, a fin de minimizar el riesgo de interrupción en los procesos de las áreas involucradas en la auditoría.

Para tal efecto se tendrá en cuenta lo siguiente:

- Acordar con el Área que corresponda los requerimientos de auditoría.
- El responsable de auditoría deberá controlar el alcance de las verificaciones.

- Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán las contramedidas necesarias a fin de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
    - Eliminar archivos transitorios.
    - Eliminar entidades ficticias y datos incorporados en archivos maestros.
    - Revertir transacciones.
    - Revocar privilegios otorgados
- Identificar claramente los recursos necesarios para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores.
- Identificar y acordar los requerimientos de procesamiento especial o adicional.
- Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir:
    - Fecha y hora.
    - Puesto de trabajo.
    - Usuario.
    - Tipo de acceso.
    - Identificación de los datos accedidos.
    - Estado previo y posterior.
    - Programa y/o función utilizada.
- Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

12. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

12.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Objetivo:

Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Política:

La Gobernación deberá implementar una política para incorporar controles de seguridad de la información a los sistemas desarrollados, para aquellos que sean adquiridos a terceros, y para las actualizaciones que se realicen a los sistemas ya existentes.

La evaluación de los requerimientos de seguridad debe incluir un análisis costo - beneficio, frente a la implementación de acciones de seguridad en el activo que se quiere proteger y frente al daño potencial que pudiera ocasionar a las actividades realizadas.

Para la información involucrada en los servicios de las aplicaciones que pasan a través de redes públicas, la Gobernación implementará un procedimiento, que incluya la aplicación de las políticas de Seguridad Informática implantadas en la entidad, este procedimiento debe garantizar la protección de la información, la autenticidad y confiabilidad de la “entidad” con la que se esté haciendo el vínculo comercial.

Para la información involucrada en las transacciones de los servicios de las aplicaciones que pasan a través de redes públicas, la Gobernación aplicará todas las políticas de Seguridad Informática definidas al interior de la entidad, garantizando la integridad de la misma, realizando operaciones en línea bajo los

parámetros de integridad, confiabilidad y seguridad, para evitar cualquier posible fraude o intrusión sin autorización a la información vital de la Gobernación.

Para garantizar transacciones por redes telemáticas seguras, es relevante tener en cuenta lo siguiente:

- Utilizar siempre un computador personal con antivirus para acceder a sitios de comercio electrónico y asegurarse de que la dirección que se presenta en el navegador corresponde al sitio que realmente se quiere visitar.
- No utilizar links en páginas de terceros o recibidos vía email y asegurarse de que el sitio tenga una conexión segura, es decir, que los datos transmitidos entre el navegador y el sitio están encriptados.
- Configurar el programa de e-mail para que no ejecute programas automáticamente.
- No realizar transacciones con empresas que solicitan un depósito y no dan la opción de pagar con tarjeta de crédito.
- Realizar transacciones sólo en sitios de instituciones que se consideren confiables, dando preferencia a las empresas grandes y conocidas.
- Nunca digitar la clave o datos personales en emails, aunque se hayan recibido de la empresa.

12.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

Objetivo:

Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

Política:

La Gobernación deberá establecer y aplicar controles para el desarrollo interno o externo de los sistemas de información que cumplan con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de

aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, cuenta con el nivel de soporte requerido por la entidad.

Para minimizar los riesgos de alteración de los sistemas de información, la Gobernación implementará procedimientos para el control de cambios a los sistemas dentro del ciclo de vida de desarrollo; dichos procedimientos deben incluir:

- Únicamente usuarios autorizados realizaran cambios en las aplicaciones, basándose en las políticas establecidas por la entidad y a las licencias de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del propietario de la información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- La Secretaría de TIC aprobará las tareas necesarias para la gestión de los cambios, antes de que éstas inicien.
- La Secretaría de TIC deberá verificar y garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Las pruebas deben ser realizadas en el ambiente correspondiente y las mismas deben ser aprobadas por parte del usuario final autorizado para tal fin.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Informar a las áreas afectadas antes de la implementación de un cambio que pueda afectar sus operaciones.

- La Secretaría de TIC es la encargada de efectuar la actualización de los datos en el nuevo sistema de información.

La secretaría de TIC de la Gobernación aplicará los principios de desarrollo seguros, documentando y aplicando procesos en la implementación de cualquier sistema de información.

En caso de que la Gobernación requiera del desarrollo de software por parte de terceros, deberá establecer normas y procedimientos que contemplen lo siguiente:

- Acuerdos de licencias, propiedad de código y derechos conferidos.
- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- Una vez finalizado el proyecto software, el contratista entregará a la Gobernación el código fuente, manuales de usuario, documentos de ingeniería de software y cualquier tipo de información relacionada con el mismo.

La Secretaría de TIC de la Gobernación deberá llevar a cabo las pruebas de la funcionalidad durante el desarrollo del sistema, las cuales deberán quedar debidamente documentadas, además deberá establecer los requisitos para poner en producción un sistema nuevo o una actualización a un sistema ya existente.

Antes de pasar a ambientes de producción se requiere realizar y documentar las pruebas de funcionamiento en ambientes de pruebas, en compañía de los usuarios que utilizarán la aplicación para conocer que todas las formas a actualizar o poner en producción satisfacen las necesidades expuestas por los usuarios, antes definidas en los requisitos funcionales entregados.

12.3 DATOS DE PRUEBA

Objetivo:

Asegurar la protección de los datos usados para pruebas

Política:

Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente, para ello se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

13. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

13.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Objetivo:

Asegurar la protección de los activos de la Gobernación que sean accesibles a los proveedores.

Política:

La Secretaría de TIC y el propietario de la información, llevarán a cabo y documentarán una evaluación de riesgos a la hora de otorgar acceso a terceras partes a la información de la Gobernación, para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la Seguridad Informática de la Organización.
- Tener estrategias para evitar el mínimo necesario de permisos a otorgar.

Los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, deben quedar claramente estipulados dentro del contrato de prestación de servicios a firmar entre las partes. Dentro de los acuerdos con terceros, se debe incluir:

- Cumplimiento de la Política de Seguridad Informática de la Organización.
- Protección de los activos de la Gobernación, incluyendo:

- Procedimientos para proteger los bienes de la Organización, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Nivel de servicio esperado y niveles de servicio aceptables.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

- Existencia de Derechos de Propiedad Intelectual.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
  - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
  - Proceso de autorización de accesos y privilegios de usuarios.
- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

Todos los requisitos de seguridad informática pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la Gobernación, quedando éstos debidamente estipulados en el contrato con el respectivo proveedor.

La Gobernación incluirá en el respectivo contrato los requisitos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos.

13.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES

Objetivo:

Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

Política:

Cualquier cambio o modificación en los servicios por parte de los proveedores, deberá estar debidamente sustentado y autorizado por la Gobernación, siguiendo las políticas internas de la entidad.

14. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

14.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Política:

La Gobernación establecerá responsabilidades y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Se deben considerar los siguientes ítems:

- ✓ Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:
  - Fallas operativas
  - Código malicioso
  - Intrusiones
  - Fraude informático
  - Error humano
  - Catástrofes naturales
- ✓ Registrar pistas de auditoría y evidencia similar para:
  - Análisis de problemas internos.
  - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.

- Negociación de compensaciones por parte de los proveedores de software y de servicios.

✓ Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

- Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
- Documentación de todas las acciones de emergencia emprendidas en forma detallada.
- Comunicación de las acciones de emergencia al personal encargado de restablecer el servicio y revisión de su cumplimiento.
- Constatación de la integridad de los controles y sistemas de la Gobernación en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del área jurídica de la Gobernación en el tratamiento de incidentes de seguridad ocurridos y sus implicaciones en todos los niveles.

Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como se tenga conocimiento del incidente.
Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre estos.
La Secretaría de TIC será informada ante la detección de un supuesto incidente o violación de la seguridad, tan pronto como se haya tomado conocimiento. Esta indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Así mismo, mantendrá al Comité de Seguridad de la información al tanto de la ocurrencia de incidentes de seguridad.
La Gobernación evaluará el incidente, y si lo estima pertinente, informará a las autoridades competentes de la ocurrencia del mismo.

Es responsabilidad de los funcionarios informar de cualquier incidente de seguridad del que tenga conocimiento directo o indirecto, con el fin de tomar las acciones para mitigar los posibles impactos del mismo.

Ningún funcionario está autorizado a realizar pruebas para detectar posibles fallas de seguridad; dichas acciones sólo podrán ser realizadas por el personal designado para tal fin.

La Gobernación evaluará los eventos de Seguridad Informática ocurridos en su interior, a fin de valorarlos y clasificarlos o no como incidentes; para realizar la corrección pertinente sobre los hallazgos arrojados en la evaluación de dichos eventos.

La Gobernación proporcionará los recursos suficientes para dar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la misma y que afecten la continuidad de su operación. Además, se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. Así mismo se definirá un proceso para documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías de seguridad, con el fin de identificar aquellos que sean recurrentes o de mayor impacto para la entidad.

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién, dónde, cuándo se halló y quién presenció el hallazgo.

- Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Ante cualquier medida legal que involucre personas ajenas a la Gobernación u otras organizaciones, la entidad deberá contar con asesoría jurídica a fin de no incurrir en violaciones a la ley y a los derechos sobre quien recaiga la acción judicial.

15. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO.

15.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la Gobernación.

Política:

La Gobernación determinará los requisitos para la seguridad de la información, y deberá establecer, documentar, implementar y mantener procesos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información en situaciones adversas. Estos controles se verificarán a intervalos regulares con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

15.2 REDUNDANCIAS

Objetivo:

Asegurar la disponibilidad de instalaciones de procesamiento de información

Política:

La Gobernación propenderá por la existencia de recursos tecnológicos redundantes que satisfagan los requerimientos de disponibilidad aceptables para la misma.

16. POLÍTICAS DE CUMPLIMIENTO

16.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Objetivo:

Evitar el incumplimiento de las obligaciones legales, estatuarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Política:

Toda información soportada por la infraestructura tecnológica de la Gobernación deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

El almacenamiento de la información de la entidad deberá realizarse interna y/o externamente, esto de acuerdo con la importancia que dicha información tenga para las operaciones de la Gobernación.

En cuanto a los soportes de información físicos, la entidad aplicará los controles que tiene establecidos para tal fin, los cuales se ajustan a la normatividad en esa materia, con el fin de garantizar la conservación de dichos soportes y efectuar una debida destrucción de los mismos, cuando sea necesario.

Es obligación de la Gobernación hacer las gestiones y consultas legales pertinentes para el uso de controles criptográficos, a fin de no incurrir en faltas a la ley, ya sea para el manejo de información dentro o fuera del país.

16.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Política:

Es obligación del Comité para la seguridad de la Información revisar independientemente a intervalos planificados y realizar una evaluación periódica de los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información a fin de evaluar su eficacia y efectividad y tomar las acciones correctivas pertinentes o si es del caso replantear las políticas que no proporcionan los resultados esperados por la Gobernación.

La Secretaria de TIC verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

El resultado de la evaluación debe quedar consignado en un informe técnico para su interpretación por parte de los especialistas.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados.

Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

ANEXO B: Procedimientos Documentados

GOBERNACIÓN DE NARIÑO

CONTENIDO

1. PROCEDIMIENTOS DOCUMENTADOS

En este documento se describieron algunos de los procedimientos de las políticas establecidas en el anexo A. Un procedimiento es la secuencia de actividades mediante un método explicando de manera clara y sencilla las indicaciones de los pasos a realizar.

En la Gobernación de Nariño se cuenta con los siguientes procedimientos:

- Procedimiento para copias de seguridad
- Procedimiento para instalación de software
- Procedimiento para actualización de software
- Procedimiento para adquisición de software
- Procedimiento para cambio de hardware

1.1 PROCEDIMIENTO PARA COPIAS DE SEGURIDAD

Este procedimiento describe el método para realizar las copias de seguridad de la información de la Gobernación de Nariño.

Objetivo:

Establecer en la Gobernación la realización de copias de seguridad al principal activo informático, la información para garantizar su disponibilidad integridad y confidencialidad.

Alcance:

Empieza con establecer necesidad de respaldo de la información del equipo y finaliza con el cierre del servicio y verificación del cumplimiento de los lineamientos.

1.1.3 Definiciones:

Carpeta: Parte específica donde se almacenan archivos informáticos en un equipo de cómputo.

Frecuencia: Periodicidad con la cual se realizan copias de respaldo.

Copia de respaldo: Copia de archivos de trabajo en medio digital sobre servidor del sistema de información.

1.1.4 Condiciones generales:

Bajo ninguna circunstancia debe dejarse de realizar este procedimiento por parte del responsable de mimo o por quien haga sus veces en su ausencia, por lo cual también debe conocer cabalmente este procedimiento.

1.1.5 Descripción del procedimiento:

El procedimiento de copia de seguridad se base en el respaldo necesario para los datos de la gestión de la empresa.

Tabla 42. Procedimiento Copia de Seguridad

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
1	Establecer la necesidad de respaldar la información	El funcionario que requiera que se respalde la información que contiene su equipo computo debe crear una carpeta llamada “User Data” en la carpeta Mis Documentos	Carpeta creada	Funcionario

Tabla 42 (Continuación)

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
		La Información a trasladar debe ser solo de uso laboral		
3	Solicitar el servicio de respaldo de la Información	Solicitar el servicio de Respaldo de información corporativa a la Secretaria TIC indicando el tamaño de la carpeta.	Solicitud de respaldo de información	Personal Secretaría TIC
4	Autorizar el respaldo de la Información	Autorizar o denegar la copia de respaldo de la información.	Registrar nota de observación con la Autorización y/o denegación dejando la justificación.	Personal Secretaría TIC
5	No Autoriza el respaldo de la información	Se deja nota de negación del servicio y se finaliza el procedimiento. Si acepta el servicio se continúa con el paso 6.		Personal Secretaría TIC
6	Realizar copia de respaldo	Realizar las copias de respaldo de la información, software e imágenes requeridas.		Personal Secretaría TIC
7	Verificar la copia de respaldo	Revisar que la información de respaldo haya quedado grabada		Personal Secretaría TIC
8	Fin del procedimiento.			

Fuente: La presente investigación

1.1.6 Responsables:

Responsable estratégico: Profesional Universitario - Secretaría TIC; Responsable Operativo: Técnico Administrativo**.**

1.1.7 Duración del procedimiento:

El tiempo total empleado en este proceso es de alrededor de 30 minutos.

1.2 PROCEDIMIENTO PARA ACTUALIZACIÓN DE SOFTWARE

Este procedimiento describe el método para actualización de software de la empresa.

1.2.1 Objetivo:

Mantener disponibles y óptimos los sistemas de información que la institución requiere para la toma de decisiones, para el control de las operaciones, el análisis de los problemas y la creación de nuevos servicios y/o trámites. Asegurar que la actualización de software se realice en forma autorizada, previa verificación de calidad de la nueva versión.

1.2.2 Alcance:

Inicia con la conformación de un inventario de sistemas de información y termina con el seguimiento permanente. Mantener actualizado él software de la empresa para que se aprovechen las últimas mejoras en funcionalidad y corrección de errores.

1.2.3 Definiciones:

Sistema de información: Es un sistema de información basado en computadora, que presenta una colección de personas, procedimientos, bases.

1.2.4 Condiciones generales:

Cuando se tenga conocimiento de la disponibilidad de una nueva versión del software se procederá a indagar sus bondades y a determinar su adquisición.

1.2.5 Descripción del procedimiento:

El procedimiento de actualización de software se realiza cada vez que se tiene conocimiento de que una nueva versión está disponible.

Tabla 43 Procedimiento Actualización de Software

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
1	Inventario	Conformación de inventario de Sistemas de información.	Hoja de vida Sistemas de Información, formulario de seguimiento, plataforma web	Profesional Universitario
2	Administrar sistemas de información	Revisión de contratos, convenios o actos administrativos de adquisición, revisión de manuales de usuario y diccionario de datos.	Documentos soporte	Profesional Universitario
3	Caracterización de usuarios	Creación y/o modificación de usuarios por perfiles y roles, asignar privilegios en el sistema de información.	Designación de responsabilidades Correos Electrónicos	Profesional Universitario
4	Parametrizar el Sistema de Información	Configurar el sistema de Información con datos relevantes y estandarizados en tablas maestras, para la ejecución de procesos.	Oficios, correos electrónicos, solicitudes soportadas, normatividad	Profesional Universitario.
5	Actualización de base de datos.	Revisar, controlar y actualizar de forma constante las bases de datos de acuerdo a los requerimientos de los usuarios del sistema de información.	Oficios, correos electrónicos, solicitudes soportadas, normatividad	Profesional Universitario, Administrador del Sistema de Información.
6	Mantenimiento de Sistemas de Información	Realizar mantenimiento preventivo en los sistemas de información, realizar copias de seguridad periódicas, indexación de base de datos, depuración de errores en datos, consolidación de base de datos.	Copias de Seguridad y bitácora de mantenimiento y backups.	Profesional Universitario, Administrador del Sistema de Información.
7	Actualización de Sistemas de Información	Solicitar actualizaciones a los proveedores de los sistemas de información y/o realizar actualizaciones de acuerdo a los requerimientos realizados por los usuarios, normas o leyes.	Documentos Soporte, requerimientos, normatividad	Profesional Universitario, Administrador del Sistema de Información.

Tabla 43 (Continuación)

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
8	Pruebas de Funcionamiento	Crear instancias para pruebas de funcionamiento cuando se emita una nueva actualización.	Acta de creación de instancia-software	Profesional Universitario, Administrador del Sistema de información o Tercero.
9	Implementación de actualización	Instalar actualización para funcionamiento en el sistema de información.	Acta de entrega de actualización	Profesional Universitario, Administrador del Sistema de información o Tercero.
10	Seguimiento y control	Realizar seguimiento y control permanente.	Bitácora	Profesional Universitario, Administrador del Sistema de información.
11	Fin del Procedimiento			

Fuente: La presente investigación

1.2.6 Responsables:

Responsable estratégico: Secretaría TIC, Innovación y Gobierno Abierto; Responsable Operativo: Profesional Universitario.

1.2.7 Duración del procedimiento:

Todo el proceso de actualización de software y capacitación no debe tomar más cinco días hábiles.

1.3 PROCEDIMIENTO PARA CAMBIO DE SOFTWARE

Este procedimiento describe el método para determinar y realizar el cambio de software.

1.3.1 Objetivo:

Propender por el adecuado desarrollo de sistemas de información y/o adquisición, para la gestión organizacional. Asegurar que la empresa cuente con las mejores herramientas informáticas para su gestión.

1.3.2 Alcance:

Inicia por la recolección de información y necesidades, termina en el seguimiento y control. Sin estar haciendo erogaciones innecesarias, mantener al día el software de gestión que le sea de mayor utilidad a la empresa.

1.3.3 Definiciones:

Software: Se conoce como un software al equipamiento o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

1.3.4 Condiciones generales:

Cuando se tenga conocimiento de la disponibilidad de un software que mejore la gestión de información en la empresa se procederá a indagar sus bondades y a determinar su adquisición.

1.3.5 Descripción del procedimiento:

El procedimiento para la adquisición de software se realiza cada vez que se tiene conocimiento de la disponibilidad de un buen producto y se procede así:

Tabla 44 Procedimiento Cambio de Software

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
1	Recolección de información y necesidades	Recopilar información o requerimientos de necesidades de las diferentes dependencias de la Gobernación de Nariño.	Registro de necesidades Correos electrónicos	Profesionales Universitarios-Gestores de TICS y/o terceros.
2	Selección de alternativas de solución	Analizar las necesidades y requerimientos, seleccionar alternativas de solución	Registro de necesidades Correos electrónicos Cotizaciones Propuestas	Profesionales Universitarios-Gestores de TICS y/o terceros.
3	Diseño de Alternativa de Solución	Revisar modelos y/o establecer diseño de la alternativa de solución.	Modelos Propuestas Cotizaciones	Profesionales Universitarios-Gestores de TICS y/o terceros.
4	Desarrollo y/o Adquisición del sistema	Programar y/o adquirir el sistema de información	Estudios previos Diseño Actas de avance	Profesionales Universitarios-Gestores de TICS y/o terceros.
5	Construcción de Manuales	Elaboración de manuales técnico y de usuario, Recepción y revisión de manuales a contratista	Manuales técnico y de usuario	Profesionales Universitarios-Gestores de TICS y/o terceros.
6	Implementación del sistema	Implementar prototipo o aplicativo para fase de pilotaje en instancias de prueba. Realización de pruebas de funcionamiento y controles con usuarios.	Contratos Actas de avance	Profesionales Universitarios-Gestores de TICS y/o terceros.
7	Evaluación del Proceso	¿Cumple con los requerimientos establecidos y el proceso es adoptado administrativamente? SI: Ir a actividad 7 NO: Ir a actividad 2	NA	Profesionales Universitarios-Gestores de TICS y/o terceros.
8	Asesoría y Capacitación	Asesoría y Capacitación en el manejo del sistema de información	Manuales de usuario	Profesionales Universitarios-Gestores de TICS y/o terceros.

Tabla 44 (Continuación)

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
9	Implantación del sistema	Poner en funcionamiento el sistema de información	Acta de entrega	Profesionales Universitarios-Gestores de TICS y/o terceros.
10	Actualización de Sistema de información	Administración, mantenimiento y actualización de sistemas de información para corrección de errores o nuevos requerimientos	Requerimientos	Profesionales Universitarios-Gestores de TICS y/o terceros.
11	Fin del Procedimiento			

Fuente: La presente investigación

1.3.6 Responsables:

Responsable estratégico: Profesional Universitario - Secretaría TIC; Responsable Operativo: Profesional Universitario.

1.3.7 Duración del procedimiento:

El tiempo del proceso de adquisición e implementación de software y capacitación depende del producto a ser comprado y sus dimensiones funcionales.

1.4 PROCEDIMIENTO PARA CAMBIO DE HARDWARE

Este procedimiento describe el método para determinar cuándo realizar el cambio de hardware.

1.4.1 Objetivo:

Mantener vigente la plataforma hardware de la empresa acorde con la tecnología de vanguardia que ofrezca mejoras significativas en capacidad de cómputo.

1.4.2 Alcance:

Sin incurrir en gastos innecesarios, disponer del hardware de apoyo a la gestión de la empresa, que cuente con las mejores características técnicas.

1.4.3 Definiciones:

Hardware: Parte física del sistema informático principalmente computadores y periféricos, con todos sus componentes internos que determinan su poder de computo.

1.4.4 Condiciones generales:

Conforme el volumen de información de la empresa crece, la demanda de realización de procesos con esa información, mayor volumen mayor velocidad, la necesidad de contar con comunicaciones más ágiles, etc. Conllevan la necesidad de contar con mayor poder de cómputo, lo cual se evidencia alrededor de cada dos años, lo cual obliga a la renovación paulatina de equipos.

1.4.5 Descripción del procedimiento:

El procedimiento para la adquisición de hardware se realiza periódicamente y se procede de la siguiente forma:

Tabla 45 Procedimiento Cambio de Hardware

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
1	Verificación de las condiciones de los equipos actuales	Verificación de las condiciones de los equipos actuales en la empresa, de la necesidad de incrementar la capacidad de cómputo y de renovación de equipos.	Actas de adquisición de Equipos.	Profesional Universitario y soporte técnico
2	Requerimientos y cotizaciones	Realización de determinación de requerimientos y cotizaciones.	Actas de adquisición de Equipos.	Profesional Universitario y soporte técnico
3	Requerimientos, cotizaciones y costos	Aprobación de identificación de requerimientos cotizaciones y costos.	Actas de adquisición de Equipos.	Profesional Universitario y soporte técnico

Tabla 45 (Continuación)

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	**Descripción de la actividad**	**Documento de trabajo**	**Responsable**
4	cronograma	Planeación del cronograma de adquisición e instalación de equipos y toma de respaldo de la información uno a uno.	Actas de adquisición de Equipos.	Profesional Universitario y soporte técnico
5	Cambio de equipos	Realización del cambio de equipo uno a uno haciendo la restauración de información.	Actas de adquisición de Equipos.	Profesional Universitario y soporte técnico
8	Fin del procedimiento.			

Fuente: La presente investigación

1.4.6 Responsables:

Responsable estratégico: Profesional Universitario - Secretaría TIC; Responsable Operativo: Profesional Universitario.

1.4.7 Duración del procedimiento:

El tiempo del proceso de adquisición e instalación de hardware depende del producto a ser comprado y disponibilidad del proveedor.

ANEXO C Entrevistas y Encuestas

BASE DE ANÁLISIS Y PROCEDIMIENTOS DETALLADOS DE LAS INFORMACIONES RECOPILADAS

En el desarrollo del proyecto se realizaron entrevistas y encuestas para determinar y analizar los incidentes presentados en cuanto a la seguridad de la información, el funcionamiento de los sistemas de información y medidas de políticas de seguridad actualmente por la Gobernación de Nariño.

Entrevista al personal que conforma la secretaria Tic de la Gobernación de Nariño. Se llevó a cabo una serie de entrevistas libres con cada uno de siguientes funcionarios:

- Apoyo en Diseño Grafico
- Contratista
- Soporte Técnico - Secretaría TIC
- Contratista
- Contratista Sistemas
- Contratista Sistemas
- Profesional Universitario
- Profesional Universitario

Por medio de las cuales se indagó acerca de la seguridad de la información, seguridad de la protección y conservación de locales, instalaciones, mobiliaria, equipos, seguridad física, control de acceso (lógico), copias de seguridad, etc. Esto con el fin de obtener un resultado que muestre que sabe el personal de la secretaria

TIC de la Gobernación de Nariño acerca de la Organización en la cual trabaja y la seguridad de la información.

De acuerdo a las preguntas realizadas respecto a la evaluación de Políticas de Seguridad dentro de la Secretaría TIC de la Gobernación de Nariño se obtuvo como resultado que no existen medidas, controles, procedimientos, normas y estándares de seguridad dentro de la secretaria TIC, no existe un documento donde este especificado la relación de las funciones y obligaciones del personal, ni tampoco existen procedimientos de realización de copias de seguridad y de recuperación de datos dentro de la secretaria Tic.

Las siguientes son las preguntas las cuales se contabilizaron para obtener un resultado de cómo el personal de la secretaria Tic de la Gobernación de Nariño sabe acerca de la Organización en la cual trabaja y la seguridad de la información.

Evaluar el funcionamiento administrativo dentro de la secretaria Tic de la Gobernación de Nariño

Tabla 46 Preguntas Secretaría TIC

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
1	¿La Gobernación de Nariño tiene definido la misión, visión, principios y valores de la secretaria Tic?	**4**	**4**
2	¿Está definido el nivel de autoridad dentro de la secretaria Tic?	**6**	**2**
3	¿Se han implementado canales de comunicación efectivos dentro de la secretaria Tic?	**4**	**4**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
5	¿Las condiciones generales de trabajo de los sistemas computacionales de la secretaria Tic son cómodas para el usuario del sistema? (Incluye equipos, infraestructura, dotaciones etc.)	**4**	**4**
6	¿Tiene protección contra la humedad en el ambiente dentro de la secretaria Tic? (Incluye ventilación, calefacción etc.)	**2**	**6**
7	¿Toman medidas para prevenir que los sistemas computacionales y las instalaciones eléctricas, telefónicas dentro de la secretaria Tic tengan contacto con el agua?	**6**	**2**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
8	¿Tienen suficientes suministros de energía dentro de la secretaria Tic? (En cuanto al número de equipos eléctricos utilizados, tienen conexión individual o compartida)	**7**	**1**
9	¿En la secretaria Tic el rendimiento y uso del sistema computacional es adecuado? (Los equipos están en sus óptimas condiciones para su uso)	**6**	**2**
10	¿La configuración, instalaciones y seguridad de los equipos, mobiliario y demás equipos de la secretaria Tic se encuentran de una forma organizada y protegen la información?	**5**	**3**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
11	¿Existen medidas, controles, procedimientos, normas y estándares de seguridad dentro de la secretaria Tic?	**2**	**6**
12	¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal? (Tareas asignadas dentro de la secretaria Tic)	**1**	**7**
13	¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos dentro de la secretaria Tic?	**2**	**6**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
14	¿Existen procedimientos en cuanto a la asignación y distribución de contraseñas para proteger la información dentro de la secretaria Tic?	**6**	**2**
15	¿Existe un período de vida de las contraseñas dentro de la secretaria Tic?	**1**	**7**

Cuestionario Sobre Gestión de Activos Informáticos dentro de la secretaria Tic de la Gobernación de Nariño

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
16	¿Existe un control sobre el acceso físico a las copias de seguridad dentro de la secretaria Tic?	**6**	**2**
17	¿Existe un inventario de los recursos informáticos existentes dentro de la secretaria Tic?	**6**	**2**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
18	¿Las copias de seguridad, o cualquier otro soporte, se almacena fuera de la secretaria Tic?	**2**	**6**
19	¿Existen procedimientos de etiquetado e identificación de los soportes informáticos dentro de la secretaria Tic?	**4**	**4**
20	¿Existen procedimientos para la realización de copias de seguridad dentro de la secretaria Tic?	**7**	**1**
21	¿Existe algún programa que permita gestionar y almacenar claves secretas dentro de la secretaria Tic?	**0**	**8**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
22	¿Las contraseñas de los trabajadores de la secretaria Tic están almacenadas en algún fichero de claves?	**0**	**8**

Cuestionario Sobre Seguridad Relacionada con el Personal dentro de la secretaria Tic de la Gobernación de Nariño

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
23	¿Ha sufrido accidentalmente pérdida de información en su puesto de trabajo dentro de la secretaria Tic?	**3**	**5**
24	En caso de pérdida de información ¿Ha logrado recuperar total o parcialmente la información? ¿Alguna persona ha divulgado información personal o privada dentro de la secretaria Tic?	**4**	**4**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
25	¿Alguna persona ha divulgado información personal o privada dentro de la Secretaria TIC?	**0**	**8**
26	¿Existe un procedimiento o manual que ayude a manejo de la información privada o restringida dentro de la Secretaría TIC?	**3**	**5**
27	¿Separa la información dependiendo de su importancia dentro de la secretaria Tic?	**3**	**5**
28	¿Alguna vez se le ha perdido algún dispositivo de almacenamiento, con información del Proceso de Gestión TIC?	**2**	**6**
29	¿Se ha olvidado de cerrar su sesión de su equipo de trabajo dentro de la secretaria Tic?	**2**	**6**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
30	Cuando está ausente en su puesto de trabajo dentro del Proceso de Gestión TIC ¿Su ordenador se queda prendido?	**5**	**3**
31	¿Ha instalado cualquier tipo de programa en su puesto de trabajo dentro de la Secretaría TIC? (Programa diferente al que se usa con frecuencia en las labores diarias de su puesto de trabajo)	**2**	**6**
32	¿Dentro de la Secretaría TIC en su puesto de trabajo ha intentado ingresar a documentos o archivos y se le ha denegado el acceso?	**2**	**6**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
33	¿Dentro del Proceso de Gestión TIC, al terminar sus labores diarias apaga su computadora?	**5**	**3**
34	¿Dentro de la Secretaría TIC, en caso de ausencia en su puesto de trabajo y este prendido su computador? ¿Cierra usted su sesión?	**5**	**3**
35	¿Dentro de la Secretaría TIC, cuando se instala un programa nuevo? ¿Existe su debida capacitación para su correcto uso?	**4**	**4**
36	Dentro de la Secretaría TIC, por cualquier motivo, ¿Su puesto de trabajo ha sido reemplazado temporalmente por personal interno?	**1**	**7**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
37	¿Dentro de la secretaría TIC, ha sufrido alguna pérdida de información?	**2**	**6**
38	¿Dentro de la Secretaría TIC, ha realizado alguna vez un cambio de clave en su computadora?	**6**	**2**
39	¿Dentro de la Secretaría TIC, ha logrado alguna vez, por su cuenta, arreglar algún error en su computador?	**7**	**1**
40	¿Dentro de la Secretaría TIC, existe un área restringida en alguna carpeta de su computadora? (En cuanto a la información y su nivel de seguridad)	**1**	**7**
41	¿Dentro de la Secretaría TIC, realiza respaldos de su información diariamente en dispositivos de almacenamiento?	**2**	**6**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
42	¿Dentro de la Secretaría TIC, se ha desconectado su computadora por apagones?	**5**	**3**
43	¿Dentro de la Secretaría TIC, se ha perdido información importante o su adelanto de trabajo por causa de apagones?	**1**	**7**
44	¿Dentro de la Secretaría TIC, ha llevado archivos digitales para terminar en su casa por falta de tiempo?	**3**	**5**
45	¿Dentro de la Secretaría TIC, tiene en su ordenador información personal como fotos, videos, música, etc.?	**3**	**5**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
46	¿Cómo trabajador activo de la Secretaría TIC usted separa por categorías los documentos públicos, privados, confidenciales, etc.?	**5**	**3**
47	¿Dentro de la Secretaría TIC, usted comparte su computador con otro compañero de trabajo?	**2**	**6**
48	¿Dentro de la Secretaría TIC, en su puesto de trabajo alguna vez se ha activado advertencias de antivirus?	**3**	**5**
49	Dentro de la Secretaría TIC, ¿Tienen definido sus funciones y obligaciones?	**8**	**0**
50	A parte de usted ¿Alguna otra persona conoce su contraseña de acceso a su computador?	**3**	**5**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
51	Dentro de la secretaría TIC, usted guarda información privada en distintas carpetas? (por medida de seguridad)	**3**	**5**
52	¿Dentro de la secretaría TIC, usted ha intentado ingresar a una página web y se ha bloqueado el acceso?	**7**	**1**
53	¿Dentro de la secretaría TIC, usted ha tenido alguna capacitación del manejo de nuevo software, con el objetivo de informar y mejorar su trabajo diario?	**2**	**6**
54	Dentro de la secretaría TIC, su cuenta de usuario ¿Tiene la misma clave que la de su correo electrónico?	**0**	**8**

Tabla 46 (Continuación)

Nº PREGUNTA	PREGUNTA	Nº RESPUESTAS SI	Nº RESPUESTAS NO
55	¿Dentro de la secretaría TIC, ha rotado alguna vez una memoria para pasar información?	**4**	**4**
56	¿Dentro de la secretaría TIC, usted tiene manuales de todas las aplicaciones en su computador o en físico?	**1**	**7**
57	¿Dentro de la secretaría TIC, su contraseña tiene como caracteres nombres de hijos, esposo, padres, mascotas, etc.?	**0**	**8**
58	¿Dentro de la secretaría TIC, se ha instalado alguna aplicación para el mejor manejo de la información?	**2**	**6**

Fuente: La presente investigación

ISO 27002 PREGUNTAS SEGURIDAD DE LA INFORMACIÓN

A continuación se muestra un cuadro para la lista de chequeo de la estructura de la norma ISO/IEC 27002 donde se describen los dominios, los objetivos de control y posteriormente cada uno de los controles se ha convertido en preguntas, las cuales son de existencia, por lo tanto la respuesta solamente puede ser SI o NO pero también se puede usar otros valores como CUMPLE o NO CUMPLE, y si de pronto puede existir el control pero ha sido implementado parcialmente puedo agregar el otro valor CUMPLE PARCIALMENTE.

En el documento se muestra la estructura de la norma ISO/IEC 27002 con las preguntas asociadas a cada dominio y objetivo de control. Por lo tanto si la respuesta no es evidente, se pueden realizar pruebas que permitan obtener la respuesta.

Tabla 47 Preguntas ISO 27002

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
1	A.5.Políticas de seguridad	A.5.1. Directrices de la Dirección en seguridad de la información	A.5.1.1. Políticas para la seguridad de la información	¿La empresa posee un conjunto de políticas para la seguridad de la información?	5	8	
			A.5.1.2. Revisión de las políticas para seguridad de la información	¿Se cuenta con un plan de revisión y cumplimiento de las políticas de la seguridad de la información?	2	10	
2	A.6. Aspectos organizativos de la SI	A.6.1. Organización interna	A.6.1.1. Roles y responsabilidades para la seguridad de la información	¿Se cuenta con un equipo líder del proceso de seguridad informática?	3	9	
			A.6.1.2. Separación de deberes	¿Se realizan verificaciones a las tareas asignadas al equipo encargado?	3	10	
			A.6.1.3. Contacto con las autoridades	¿Se cuenta con un protocolo de alerta en caso de la presentación de emergencias (robos, pérdidas, personas a las cuales se debe acudir)?	6	9	
			A.6.1.4. Contacto con grupos de interés especial	¿Se realizar asignación de responsabilidades para la seguridad de la información?	4	8	
			A.6.1.5. Seguridad de la información en la gestión de proyectos	¿Existe contacto con las autoridades?	4	6	
		A.6.2. Dispositivos para movilidad y teletrabajo	A.6.2.1. Política para dispositivos móviles	¿La empresa tiene una política de uso de dispositivos para movilidad?	6	8	
			A.6.2.2. Teletrabajo	¿La empresa implementa el teletrabajo?	0	14	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
3	A.7. Seguridad ligada a los recursos humanos	A.7.1. Antes de la contratación	A.7.1.1. Selección	¿Se realiza Investigación de antecedentes?	7	4	
			A.7.1.2. Términos y condiciones del empleo	¿En los acuerdos contractuales en donde se especifiquen las responsabilidades y las de la organización en cuanto a la seguridad la información?	3	5	
		A.7.2. Durante la contratación	A.7.2.1. Responsabilidad de la dirección	¿Se encuentra contratado un profesional específicamente para la realización del tema?	2	7	
			A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	¿la empresa capacita a sus funcionarios en cuanto a la seguridad de la información?	4	12	
			A.7.2.3. Proceso disciplinario	¿Se realizan socializaciones para actualizar a los empleados en los diferentes cambios generados?	9	6	
		A.7.3. Terminación o cambio de puesto de trabajo	A.7.3.1. Terminación o cambio de responsabilidades de empleo	¿Se tienen definidos las responsabilidades y deberes de seguridad de la información una vez el empleado termine su contratación o se le realice un cambio de puesto?	5	4	
4	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.1. Inventario de activos	¿Se cuenta con un inventario de activos actualizado?	4	7	
			A.8.1.2. Propiedad de los activos	¿Se cuenta con un procedimiento para la solicitud de algún equipo faltante y necesario para el desempeño?	12	4	
			A.8.1.3. Uso aceptable de los activos	¿Los funcionarios de la empresa hacen buen uso de los activos informáticos?	6	5	

			A.8.1.4. Devolución de activos	¿Los empleados de la entidad al terminar su contrato hacen devolución de los activos?	14	1	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
		A.8.2. Clasificación de la información	A.8.2.1. Clasificación de la información	¿Se cuenta con un sistema de etiquetado de los equipos para verificar su propiedad?	12	2	
			A.8.2.2. Etiquetado de la información	¿Se tienen implementado un procedimiento para el etiquetado de la información?	8	3	
			A.8.2.3. Manejo de activos	¿Se manejan los activos de acuerdo al procedimiento implementado?	6	3	
5	A.9. Control de Acceso	A.9.1. Requisitos de negocio para el control de accesos	A.9.1.1. Política de control de acceso	¿Se tiene control sobre los accesos a las redes por parte personas internas a la compañía?	7	1	
			A.9.1.2. Política sobre el uso de los servicios de red	¿La empresa posee una política de control de accesos?	5	5	
				¿Se tiene control sobre los accesos a las redes por parte personas externas a la compañía?	6	6	
		A.9.2. Gestión de acceso de usuario	A.9.2.1. Registro y cancelación del registro de usuarios	¿Se lleva un control sobre los usuarios de los sistemas de información?	5	4	
			A.9.2.2. Suministro de acceso a usuarios	¿Se tiene un reporte de los procesos realizados por cada usuario en los Sistemas de información?	1	6	
			A.9.2.3. Gestión de derechos de acceso privilegiado	¿La empresa realiza gestión de altas/bajas en el registro de usuarios?	9	4	

			A.9.2.4. Gestión de información de autenticación secreta de usuarios	¿Cuenta la empresa con un procedimiento que identifique los diferentes niveles de seguridad de acceso a las herramientas o sistemas de información?	4	5	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.9.2.5. Revisión de los derechos de acceso de usuarios	¿Se realiza una revisión periódica de los logs de acceso a las diferentes herramientas o sistemas de información?	2	5	
			A.9.2.6. Retiro o ajuste de los derechos de acceso	¿Se realiza una revisión periódica de los derechos de acceso, realizando de esta manera la eliminación de los usuarios que ya no trabajan en la empresa?	4	2	
		A.9.3. Responsabilidad de los usuarios	A.9.3.1. Uso de la información de autenticación secreta	¿Los usuarios cumplen a cabalidad con el buen uso de la información secreta (No divulgación)?	11	1	
		A.9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1. Restricción de acceso de la información	¿Se cuenta con la decisión de niveles de acceso con relación a cada usuario?	8	2	
			A.9.4.2. Procedimiento de ingreso seguro	¿Se cuenta con la asignación de contraseñas para el acceso a la información?	12	1	
			A.9.4.3. Sistema de gestión de contraseñas	¿Se cuenta con un administrador de la base de datos y el código de aplicaciones?	10	1	
			A.9.4.4. Uso de programas utilitarios privilegiados	¿La empresa hace uso de herramientas de administración de sistemas?	6	3	

			A.9.4.5. Control de acceso a códigos fuente de programas	¿Se tiene definido los roles de las personas que tienen acceso al código fuente y se encuentra esta información en lugares seguros?	3	4	
6	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.1. Política sobre el uso de controles criptográficos	¿Se tiene una política sobre el uso de controles criptográficos para la protección de la información?	0	8	

Tabla 47 (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.10.1.2. Gestión de llaves	¿Se tiene una política con la cual se conoce el uso, protección y tiempo de vida de las llaves criptográficas?	0	8	
7	A.11. Seguridad física y del entorno	A.11.1. Áreas seguras	A.11.1.1 Perímetro de seguridad física	¿Los servidores y puntos de conexión se encuentran ubicados en un lugar seguro?	10	2	
			A.11.1.2. Controles físicos de entrada	¿Las entradas a los lugares prohibidos se encuentran con algún mecanismo de seguridad, por ejemplo biométricos?	4	6	
			A.11.1.3. Seguridad de oficinas, recintos e instalaciones	¿Las oficinas, recintos e instalaciones cuentan con algún tipo de seguridad? Por ejemplo, Vigilantes, cámaras.	5	8	
			A.11.1.4. Protección contra amenazas externas y ambientales	¿El lugar donde se encuentran los servidores cuenta con las medidas de seguridad apropiadas (Extintores, aire acondicionado, entre otros)?	5	8	
			A.11.1.5. Trabajo en áreas seguras	¿Se tiene establecido un procedimiento que indique como	1	9	

				se debe realizar el trabajo en las áreas seguras?			
			A.11.1.6. Áreas de despacho y carga	¿El lugar donde se realiza el despacho y carga de herramientas (computadores, teclados, entre otros), cuenta con medidas de seguridad?	5	8	
		A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	¿La infraestructura eléctrica se encuentra bien instalada y sin riesgos?	7	7	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.11.2.2. Servicios de suministro	¿Los equipos informáticos y accesos de red, están seguros?	5	9	
			A.11.2.3. Seguridad del cableado	¿Se realiza mantenimiento a los equipos periódicamente?	10	4	
			A.11.2.4. Mantenimiento de equipos	¿Se cuenta con puestos de trabajos agradables y seguros?	11	3	
			A.11.2.5. Retiro de activos	¿Cuándo se va a realizar un cambio de algún computador a otro puesto de trabajo, se tiene un conducto regular para realizar dicho proceso?	10	2	
			A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	¿Cuándo un activo es sacado de la empresa, este cuenta con las medidas de seguridad en caso de tener pérdida?	5	5	
			A.11.2.7. Disposición segura o reutilización de equipos	¿Se realiza un backup y limpieza de los equipos de cómputo antes de entregarlo a otra persona?	11	1	

			A.11.2.8. Equipos de usuario desatendidos	¿Los equipos que no tienen personal asignado se les dá una protección adecuada?	4	6	
			A.11.2.9. Política de escritorio limpio y pantalla limpia	¿Se tiene una política de escritorio limpio para los papeles y medios de almacenamiento removibles?	7	7	
8	A.12. Seguridad en las operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Procedimientos de operación documentados	¿Se documentan los procedimientos de operación y se ponen a disposición de los usuarios?	4	5	
			A.12.1.2. Gestión de cambios	¿Se tiene un procedimiento de gestión de cambios en el área de desarrollo de los aplicativos?	3	5	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.12.1.3. Gestión de capacidad	¿Se realiza periódicamente revisión de los recursos, espacio de los diferentes servidores de la empresa?	4	4	
			A.12.1.4. Separación de los ambientes de desarrollo, pruebas y operación	¿Se cuenta con ambientes de desarrollo, pruebas y producción separados?	2	4	
		A.12.2. Protección contra códigos maliciosos	A.12.2.1. Controles contra códigos maliciosos	¿Se cuenta con antivirus activo en todos los equipos de la compañía?	6	6	
				¿Se cuenta con antivirus activo en todos los equipos de la compañía?	6	6	
				¿Se realizan monitoreo en prevención a ataques que se generan al sistema?	4	5	
		A.12.3. Copias de seguridad	A.12.3.1. Respaldo de información	¿Se realizan periódicamente copias de seguridad de la información?	8	2	

		A.12.4. Registro y seguimiento	A.12.4.1. Registro de eventos	¿Se realiza revisión periódica de los logs de las diferentes herramientas con el fin de verificar las fallas y eventos de seguridad de la información?	1	2	
			A.12.4.2. Protección de la información de registro	¿Se tiene un control de acceso no autorizado, con el fin de proteger la información de algún tipo de modificación?	11	1	
			A.12.4.3. Registros del administrador y del operador	¿Las actividades realizadas por los administradores de las diferentes herramientas son monitoreadas?	1	6	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.12.4.4. Sincronización de relojes	¿Los relojes de los equipos de cómputo, servidores y demás sistemas, se encuentran sincronizados?	6	3	
		A.12.5. Control de software operacional	A.12.5.1. Instalación de software en sistemas operativos	¿Se tiene alguna regla que impida a los usuarios finales realizar la instalación de software?	10	2	
		A.12.6. Gestión de la vulnerabilidad técnica	A.12.6.1. Gestión de las vulnerabilidades técnicas	¿Se realizan pruebas de penetración para encontrar vulnerabilidades en los sistemas y así prevenirlas?	1	8	
			A.12.6.2. Restricciones sobre la instalación de software	¿Se tiene un procedimiento definido para las personas de soporte sobre la instalación del software que se puede realizar en los equipos?	6	2	

		A.12.7. Consideraciones sobre auditorias de sistemas de información	A.12.7.1. Información de controles de auditoría de sistemas	¿Los sistemas de información de la entidad, como las Bases de Datos cuentan con un sistema de auditoria activo?	3	5	
9		A.13.1. Gestión de la seguridad de las redes	A.13.1.1. Controles de redes	¿Se tiene un reporte de las transacciones realizadas en las redes de la compañía?	1	5	
			A.13.1.2. Seguridad de los servicios de red	¿En la empresa existen mecanismos de seguridad asociados a servicios de red?	3	5	
			A.13.1.3. Separación en las redes	¿Se tiene algún procedimiento sobre el acceso a las redes?	3	5	
		A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	¿Se cuenta con protocolos de intercambio de información con externos?	2	5	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.13.2.2. Acuerdos sobre transferencia de información	¿Se cuenta con servicio de email dentro del dominio de la compañía?	11	1	
			A.13.2.3. Mensajería electrónica	¿La información contenida en los correos cuenta con mecanismos de seguridad, como por ejemplo antivirus, protección por contraseña?	8	2	
			A.13.2.4. Acuerdos de confidencialidad o de no divulgación	¿Se realiza revisión y actualización de los acuerdos de confidencialidad?	0	7	
10	A.14. Adquisición, desarrollo y	A.14.1. Requisitos de seguridad de los	A.14.1.1. Análisis y especificación de requisitos	Se han implementado protocolos de seguridad en los sistemas de información	4	3	

	mantenimiento de sistemas	sistemas de información	de seguridad de la información				
			A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas	Se cuenta con control de las transacciones realizadas a nivel externo por medio del SI	1	5	
			A.14.1.3. Protección de transacciones de los servicios de las aplicaciones	¿Se realiza la protección de la información involucrada en las transacciones de los servicios de las aplicaciones, por ejemplo certificados digitales?	2	5	
		A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.1. Política de desarrollo seguro	Se cuenta con un procedimiento para la solicitud de desarrollo de software	3	3	
			A.14.2.2. Procedimientos de control de cambios en sistemas	Se lleva un control de las versiones de las aplicaciones desarrolladas	3	3	
			A.14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se cuenta con un protocolo para la aplicación de pruebas a los SI desarrollados	0	6	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.14.2.4. Restricciones en los cambios a los paquetes software	Se cuenta con un procedimiento para la puesta en producción de un desarrollo en SI	0	5	
			A.14.2.5. Principios de construcción de sistemas seguros	Se tienen en cuenta principios de seguridad en un entorno de desarrollo	1	5	
			A.14.2.6. Ambiente de desarrollo seguro	¿El lugar en donde se encuentra el código y las aplicaciones desarrolladas es seguro?	4	1	
			A.14.2.7. Desarrollo contratado externamente	¿Cuenta la empresa con un hosting tercerizado?	7	1	

			A.14.2.8. Pruebas de seguridad de sistemas	¿Se realizan pruebas de funcionalidad a las aplicaciones desarrolladas?	6	1	
			A.14.2.9. Pruebas de aceptación de sistemas	¿Cuándo se realizan actualizaciones a los desarrollos de aplicaciones, se hacen pruebas de aceptación?	3	3	
		A.14.3. Datos de prueba	A.14.3.1. Protección de datos de prueba	¿Cuándo se realizan las pruebas se trabajan con datos falsos?	4	2	
11	A.15. Relación con los proveedores	A.15.1. Seguridad de la información en las relaciones con los proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores	¿Se cuenta con una política de seguridad de la información asociada a terceros?	2	8	
			A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	¿Se tienen establecidos los requisitos y procedimientos de acceso a las instalaciones por parte de terceros?	4	7	
			A.15.1.3. Cadena de suministro de tecnología de información y comunicación	¿Se tiene acuerdos con terceros que incluyan los requisitos para tratar los riesgos de seguridad de la información asociados a la cadena de suministro?	0	8	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
		A.15.2. Gestión de la prestación de servicios con los proveedores	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores	¿Se hace un seguimiento de la prestación del servicio de terceros?	8	1	
			A.15.2.2. Gestión de cambios en los servicios de proveedores	¿Se tiene una gestión de cambios en el suministro de servicios por parte de terceros?	4	5	

12	A.16. Gestión de incidentes en la seguridad de la información	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1. Responsabilidad y procedimientos	¿Se cuenta con un procedimiento para la identificación de un incidente de seguridad de la información?	2	7	
			A.16.1.2. Reporte de eventos de seguridad de la información	¿Se cuenta con un procedimiento para el reporte de un incidente de seguridad de la información?	2	7	
			A.16.1.3. Reporte de debilidades de seguridad de la información	¿Se cuenta con un procedimiento para el trámite de un incidente de seguridad de la información?	1	8	
			A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones de la información	¿Se tiene identificado un responsable para la gestión de los incidentes de seguridad de la información?	4	5	
			A.16.1.5. Respuesta a incidentes de seguridad de la información	¿Los incidentes informáticos son tratados y solucionados a tiempo?	6	1	
			A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	¿Se solicitan evidencias de los incidentes de seguridad de información identificados?	3	5	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
			A.16.1.7. Recolección de evidencia	¿Se tiene definido un procedimiento en donde se especifique como debe realizarse la identificación, recolección, adquisición y preservación de información que es tomada como evidencia?	1	7	

13	A.17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	A.17.1. Continuidad de la seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información	¿Se hace seguimiento a la seguridad de la información?	4	4	
			A.17.1.2. Implementación de la continuidad de la seguridad de la información	¿Se tiene un plan de continuidad?	1	6	
			A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se realiza regularmente la verificación del plan de continuidad?	0	6	
		A.17.2. Redundancias	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información	¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir los requisitos de disponibilidad?	0	5	
14	A.18. Cumplimiento	A.18.1. Cumplimiento de requisitos legales y contractuales	A.18.1.1. Identificación de requisitos legales y contractuales	¿Se realizan auditorías internas para verificar el cumplimiento de la norma?	3	9	
			A.18.1.2. Derechos de propiedad intelectual	¿Se cuenta con mecanismos de protección de la información?	7	7	
			A.18.1.3. Protección de registros	¿Se tiene documentado todo el proceso de seguridad y protección de la información?	3	9	
			A.18.1.4. Privacidad y protección de datos personales	¿Se asegura la privacidad y la protección de la información de datos personales?	7	5	

Tabla 47. (Continuación)

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
14		A.18.2. Revisiones de la seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información	¿Se cumple con las políticas y normas de seguridad?	3	9	

	A.18 Cumplimiento		A.18.2.2. Cumplimiento con las políticas y normas de seguridad	¿Se realizan comités de seguridad con los altos directivos en donde se revisen con regularidad el cumplimiento de las políticas de seguridad en todas las áreas?	3	8	
			A.18.2.3. Revisión del cumplimiento técnico	¿Se realiza revisión periódica de los sistemas con el fin de verificar el cumplimiento de las políticas de seguridad de la información?	3	7	

Fuente: La presente investigación

De las preguntas realizadas a los funcionarios de la Secretaría TIC de la Gobernación de Nariño en base a la norma ISO/IEC 27002 en donde se especifica en su estructura, los dominios de seguridad que deben ser evaluados; dentro de cada dominio se especifica los objetivos y control, y dentro de cada objetivo de control se especifican los controles o actividades de control que se deben verificar, se obtuvieron los siguientes resultados:

Tabla 48. Resultados Obtenidos de la ISO 27002

DOMINIO	Sum - TOTAL SI	Sum - TOTAL NO	DE CUMPLIMIENT	Estado
A.10.	0	16	0	INEXISTENTE
A.11.	113	73	61	DEFINIDO
A.12.	76	67	53	DEFINIDO
A.13.	28	30	48	DEFINIDO
A.14.	38	43	47	DEFINIDO
A.15.	18	29	38	REPETIBLE
A.16.	19	40	32	REPETIBLE
A.17.	5	21	19	INEXISTENTE
A.18.	29	54	35	REPETIBLE
A.5.	7	18	28	REPETIBLE
A.6.	26	64	29	REPETIBLE
A.7.	30	38	44	DEFINIDO
A.8.	62	25	71	GESTIONADO
A.9.	93	50	65	DEFINIDO
Total Result	**544**	**568**		

Fuente: La presente investigación

ANEXO D Informe de Auditoría

INFORME DE AUDITORIA DEL PROCESO REALIZADO EN LA GOBERNACIÓN DE NARIÑO

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento muestra los resultados obtenidos del Diseño de Políticas y Procedimientos de Seguridad Informática y de Información utilizando la norma ISO 27001/2013 y Magerit versión 3.0 para la gestión del riesgo en los activos de información presentes en la Gobernación de Nariño.

La importancia de la realización de este proyecto, contribuirá de manera significativa a la Gobernación de Nariño, para brindar una perspectiva de su funcionamiento y trabajo y así tomar acciones que garanticen la mejora y el cumplimiento de los objetivos gubernamentales.

El proyecto se ha basado principalmente en el estudio del cumplimiento de los requerimientos de la Gobernación, la seguridad física y lógica, al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada; esto con el fin de eliminar o mitigar el riesgo informático y salvaguardar activos de información para la mejora continua de la entidad.

Finalmente se registran los hallazgos y recomendaciones como insumo para las políticas de seguridad informática y de Información acorde a las actividades de la Gobernación de Nariño, para ser aprobadas, difundidas y aplicadas en la misma.

2. OBJETIVO

Conocer el estado actual de la seguridad Informática y de Información en la Gobernación de Nariño, con el fin de determinar los riesgos y vulnerabilidades a los que se encuentra expuesta la entidad y así realizar el Sistema de Gestión de Seguridad de la Información conforme a los requisitos de la norma ISO/IEC 27001:2013.

3. ALCANCE

Determinar a través de los hallazgos encontrados, los controles y las recomendaciones para el diseño del Sistema de Gestión de la Seguridad de la información – SGSI.

4. DICTAMEN

1. Se ha auditado la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño y evaluado el nivel de riesgo presente en los activos informáticos y de información de la misma, con los hallazgos, políticas, recomendaciones y anexos que se adjuntaron.

2. Para la ejecución del proyecto se utilizó la norma ISO 27001/2013 Y Magerit versión 3.0, la cual permitió determinar vulnerabilidades, amenazas y riesgos presentes en los activos de la Secretaría de TIC, con el fin de tomar medidas preventivas y correctivas que ayuden a eliminar los riesgos asociados o en su defecto minimizarlos al máximo.

   En el desarrollo del proyecto se realizó lo siguiente:

   - Entrevistas para obtener información relevante para el proyecto se utilizó la entrevista de modelo conversacional, por ser una técnica eficaz para obtener datos relevantes y significativos, utilizando una entrevista no estructurada con el fin de obtener una opinión personalizada de los Profesionales Universitarios y Especializados quienes son los encargados de la administración de las aplicaciones, base de datos y comunicaciones.
   - Encuestas para determinar vulnerabilidades, conductas y conocimiento que tenían los usuarios de las políticas de seguridad informática, se aplicó una encuesta que fue contestada por 41 personas.
   - Se utilizó la observación para registrar patrones de conducta de los usuarios y del sistema informático.

- Conocer la documentación de procesos y procedimientos de manejo de la información, la documentación de políticas de seguridad y determinar los activos informáticos y sistemas de información que funcionan en la Gobernación de Nariño.
- Realizar el proceso de análisis y evaluación de riesgos identificando mediante pruebas las vulnerabilidades y amenazas de seguridad a que está expuesta la Gobernación de Nariño. ¬ Verificar la existencia de controles de seguridad informática y de información de acuerdo a la norma ISO/IEC 27001 de control interno de seguridad informática.
- Diseñar las nuevas políticas y procedimientos de seguridad informática de acuerdo a los resultados obtenidos del proceso aplicado anteriormente.

3. Este dictamen tiene como fin mejorar la eficiencia gubernamental, minimizar los riesgos asociados a daños y asegurar que se cumplan las funciones misionales de la entidad estableciendo políticas de seguridad y procedimientos de seguridad informática dando cumplimiento a la Estrategia de Gobierno en Línea (GEL) en cuanto al Componente TIC para Seguridad y Privacidad de la información.

4. La Secretaría de TIC presenta un nivel de riesgo medio en sus activos más importantes para los procesos de la misma, aunque a la hora de prestar sus servicios los ofrece normalmente.

5. HALLAZGOS y RECOMENDACIONES

En el presente trabajo de acuerdo a Entrevistas, Encuestas, Observaciones y Revisión documental, se encuentra lo siguiente:

Hallazgo 1:

- Con respecto a la Organización y Administración de la secretaria Tic de la GOBERNACIÓN DE NARIÑO.

  - El área no cuenta con una estructura organizacional
  - Ausencia de manual de funciones para cada puesto de trabajo dentro del área.

Recomendación:

- Establecer una estructura organizacional en la SECRETARÍA DE TIC, INNOVACIÓN Y GOBIERNO ABIERTO DE LA GOBERNACIÓN DE NARIÑO.
- Se establezca un manual de funciones para cada uno de los cargos que desempeña cada empleado en la secretaria Tic.

Hallazgo 2:

- Respecto a la seguridad física y lógica

  - No existe una vigilancia estricta en la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño por personal de seguridad dedicado a este sector

- No existe un puesto o cargo específico para la función de seguridad Informática.
- Falta de alarmas y cámaras de seguridad.

Recomendaciones:

A los efectos de minimizar los riesgos descritos, se sugiere:

- Establecer guardia de seguridad, durante horarios no habilitados para el ingreso a la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño
- Instalar alarmas y cámaras como sugerencia de seguridad.

Hallazgo 3:

- Respecto al plan de prevención y contingencia:

- Ausencia de un Plan de Contingencia debidamente formalizado en la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño.
- No existen normas y procedimientos que indiquen las tareas manuales e informáticas que son necesarias para realizar y recuperar la capacidad de procesamiento ante un eventual problema (desperfectos de equipos, incendios, cortes de energía con más de una hora), y que determinen los niveles de participación y responsabilidades del área de sistemas y de los usuarios.
- Ausencia de un plan de prevención en desastres en la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño.

Recomendaciones:

- Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operatoria normal de la organización y establecer los responsables de cada sistema.
- Efectuar pruebas simuladas en forma periódica a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.

ANEXO E Artículo

Políticas y Procedimientos de Seguridad Informática y de Información para la Gobernación de Nariño.

Argenis Geraldin Fajardo Guerrero, Angela María Timarán Jiménez

Facultad de Ingeniería, Universidad de Nariño, Pasto, Colombia
geralf609@gmail.com angelinamtj@gmail.com

***Resumen*— La Gobernación de Nariño reconoce la importancia de identificar y proteger sus activos informáticos y de información, es por eso que se pretende realizar estudios para determinar amenazas, vulnerabilidades y riesgos presentes en estos activos con el fin de eliminarlos o reducirlos al máximo, garantizando así que los servicios ofrecidos por la entidad sean preservados, seguros y confiables.**

Este proyecto tiene como finalidad diseñar las Políticasy Procedimientos de Seguridad informática y de información basándose en la norma ISO 27001/2013 y Magerit versión 3.0, y constituye una base para garantizar la disponibilidad, integridad, y confidencialidad de la información para la mejora continua de la entidad

***Palabras Clave*— Políticas de seguridad, ISO 27001/2013, Magerit versión 3.0, disponibilidad, integridad, confidencialidad, amenazas, vulnerabilidades y riesgos.**

***Abstract*— The Governorate of Nariño recognizes the importance of identifying and protecting its information and information assets, that is why it is intended to conduct studies to determine threats, vulnerabilities and risks present in these assets in order to eliminate or reduce them to the maximum, thus ensuring that the services offered by the entity are preserved, safe and reliable.**

The purpose of this project is to design IT and Information Security Policies and Procedures based on ISO 27001/2013 and Magerit version 3.0, and constitutes a basis to guarantee the availability, integrity, and confidentiality of information for the continuous improvement of the entity.

***Key Word*— Security politics, ISO 27001/2013, Magerit version 3.0, availability, integrity, confidentiality, threats, vulnerabilities and risks.**

I. INTRODUCCIÓN

La Gobernación de Nariño reconoce la importancia de identificar y proteger sus activos informáticos y de información, así mismo determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, por lo tanto es necesario implementar controles y procedimientos que permitan proteger la continuidad de los niveles de competitividad, de gestión pública, y de conformidad legal necesarios para alcanzar las metas administrativas y del plan departamental de desarrollo Nariño Corazón del mundo 2016-2019.

El presente documento establece las políticas y procedimientos de seguridad informática y de la información definidas por la Gobernación de Nariño. Para la elaboración del mismo, se toman como referencia la norma ISO 27001:2013 y las recomendaciones del entandar ISO 27002: 2013.

Las políticas de seguridad presentes en este documento son de gran importancia para el Sistema de Gestión de Seguridad de la Información SGSI, ya que permiten minimizar los riesgos encontrados en la entidad y garantizar la integridad, confidencialidad y disponibilidad de la información.

II. OBJETIVO

Definir y explicar las políticas y procedimientos de seguridad informática y de información, permitiendo la protección de los activos de la entidad.

III. ALCANCE

Esta Política es de aplicación en el conjunto de Secretarías, Departamentos, subsecretarías, oficinas y dependencias que componen la Gobernación de Nariño, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal de Gobernación, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

IV. DEFINICIONES

- **Confidencialidad:** Los activos de información solo pueden ser accedidos y custodiados por usuarios que cuente con permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que cuenten con los permisos adecuados.
- **Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.
- **Trazabilidad:** Las actuaciones de la entidad pueden ser imputadas exclusivamente a la dicha entidad.
- **Activo:** Son elementos que tienen valor para una organización tales como: datos/información, servicios, aplicaciones (software), equipos (hardware), medios de almacenamiento (físico y electrónico), equipamiento auxiliar, instalaciones y personal.
- **Amenaza:** Es cualquier situación que se puede presentar en la entidad, dañando un activo mediante la presencia de una vulnerabilidad.
- **Vulnerabilidad:** Debilidad de un activo que puede ser aprovechada por una amenaza.
- **Riesgo:** Es el daño que se le puede presentar a un activo cuando se encuentra desprotegido.
- **Análisis de riesgos:** A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Control:** Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

V. COMITÉ PARA LA SEGURIDAD DE LA INFORMACIÓN

La Gobernación de Nariño, proyecta la organización de la Seguridad de la información, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Secretario de Gobierno o Líder GEL
- Secretaria General del Departamento.
- Subsecretaria Talento Humano
- Jefe Oficina de Control Interno de la Gestión
- Jefe Archivo General
- Oficina de Gestión Tecnológica.

Los integrantes del comité deberán revisar y actualizar anualmente la Política de Seguridad de la Información, presentando los proyectos o propuestas al Gobernador del Departamento para su aprobación mediante acto administrativo correspondiente.

L@s Secretari@s, Directores de departamento o Jefes de Dependencias u Oficinas, deben identificar y valorar los activos de información que pertenecen a las respectivas áreas, y deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados y adoptados por el Gobernador.

VI. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

Establecer las políticas y procedimientos de seguridad de información para el uso de Tecnologías de Información y comunicación de la Secretaria de TIC, Innovación y Gobierno Abierto de la

Gobernación de Nariño, donde se denote lo siguiente: Objetivos organizacionales en donde se proteja los activos de información, responsabilidades y los derechos que se deben conocer y cumplir los funcionarios internos y externos, propietarios y administradores de la infraestructura tecnológica para lograr que los recursos tecnológicos de la entidad presten su servicio de manera accesible, confiable y oportuna.

Responsabilidades asignadas: La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Gobernación de Nariño, independiente del tipo de vinculación, el área o dependencia a la cual se encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El Gobernador del Departamento de Nariño aprueba esta Política y es responsable de la aprobación y adopción de las actualizaciones.

El Comité de Seguridad de la Información de la entidad es responsable de revisar, proyectar y proponer a la administración departamental en cabeza del Gobernador, para su aprobación, el documento de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de Información de la Gobernación de Nariño. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Administración Departamental.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la socialización, implementación, seguimiento y control de la política.

Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilidad de mantener de forma integral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Quien ejerza el cargo de Subsecretario de Talento Humano, deberá notificar a todo el personal que se vincule con la Gobernación de Nariño, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación y socialización de la presente Política y de los cambios o actualizaciones que en ella se produzcan a todo el personal, a través de la suscripción de los acuerdos de Confidencialidad y de labores de capacitación continua en materia de seguridad según los lineamientos establecidos por el Comité de Seguridad de la Información de la Entidad.

Los profesionales universitarios y equipo de trabajo de la Oficina de Gestión Tecnológica en coordinación con la Secretaría General del Departamento deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información e infraestructura tecnológica de la Entidad.

El Archivo General del Departamento en colaboración con la oficina de Gestión tecnológica determinara el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Almacén General del Departamento en responsabilidad de los respectivos líderes.

Quien ejerza el cargo de Director@ del Departamento Administrativo de Contratación verificará que los contratos, convenios u otra documentación de la entidad con servidores públicos y con terceros incluya los lineamientos de la Política de Seguridad de la Información de la Entidad.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

La Oficina de Control Interno de la Gestión, es responsable de realizar seguimiento y control periódico sobre información contenida en documentos, sistemas de información y/o actividades vinculadas con la gestión de activos de información. Es responsabilidad de esta área informar sobre el cumplimiento de los lineamientos y medidas de seguridad de la información establecidas por esta Política, y normas adicionales vigentes.

VII. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

A. Organización Interna

Objetivo:

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Gobernación.

Política:

La Secretaría de TIC, Innovación y Gobierno abierto debe conformar el Comité para la Seguridad de la Información conformado por Directores y coordinadores de la Gestión Tecnológica.

Los integrantes del comité deberán revisar y actualizar anualmente la Política de Seguridad de la Información, presentando los proyectos o propuestas al Gobernador del Departamento para su debida aprobación.

VIII. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS.

A. Antes de Asumir el Empleo

Objetivo:

Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Política:

Todos los empleados de la Gobernación de Nariño deberán conocer los términos y las condiciones del contrato laboral haciendo énfasis en los aspectos relativos a la seguridad de la información y se debe verificar que los contratos estén firmados. El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento.

B. Durante la Ejecución del Empleo

Objetivo:

Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Política:

La Secretaría de TIC deberá exigir que los empleados y contratistas cumplan a cabalidad con las políticas de seguridad establecidas por la Gobernación. Para esto debe darles a conocer las políticas y procedimientos pertinentes para su cargo, así mismo capacitara e informara cuando se presenten modificaciones y será estricta en el cumplimiento de las mismas, tomando las medidas disciplinarias o legales del caso, cuando dichas políticas no sean cumplidas por el personal.

IX. POLÍTICA DE GESTIÓN DE ACTIVOS

A. Responsabilidad por los Activos

Objetivo:

Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

Política:

La Gobernación de Nariño deberá implementar reglas para el uso aceptable de los activos informáticos, esto implica la aceptación por parte de los usuarios, de las normas, políticas y estándares establecidos para garantizar la seguridad informática. Este trámite de sebe estandarizar según las normas de calidad, para el cuidado, buen manejo y entrega definitiva de los activos.

B. Clasificación de la Información

Objetivo:

Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la Gobernación.

Política:

Cada una de las dependencias de la Gobernación de Nariño deberá clasificar su información sea física o electrónica, de acuerdo a sus necesidades para compartir o restringir la información, igualmente deben existir procedimientos para el adecuado manejo de todos los activos en la organización.

X. POLÍTICAS SEGURIDAD FÍSICA Y DEL ENTORNO

A. Áreas Seguras

Objetivo:

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Gobernación de Nariño.

Política:

La Secretaría de TIC definirá las áreas restringidas las cuales se identifican porque allí se almacenan, se procesan o utilizan activos de tecnología e informática, activos considerados como críticos con un grado de confidencialidad.

El acceso de personal externo a áreas protegidas se limitará. Este se dará cuando sea necesario y en acompañamiento de personal autorizado. Se debe llevar un registro del ingreso y salida del personal del área protegida, identificando hora, fecha, motivos de ingreso, identificación del personal que ingresa, así como del acompañante autorizado.

Para la seguridad física a oficinas e instalaciones, definirá:

- La ubicación segura de los equipos de soporte como son los equipos, impresoras y escáner.
- El bloqueo de los equipos de cómputo cuando los usuarios están fuera de su sitio de trabajo.
- Control de movimientos para los equipos portátiles
- Control de la utilización de discos duros externos, memorias USB.
- El no consumo de comida y bebidas en la sala de comunicaciones y oficinas.
- Almacenamiento bajo llave de documentos de carácter confidencial y crítico.

La Gobernación dentro de su Dirección administrativa de Gestión del riesgo de desastres deberá establecer las políticas necesarias para proteger al personal como los activos de información en caso de desastres naturales. Para ello deberá demarcar las zonas seguras, así como dotarlas con extintores, igualmente deberá evaluar las condiciones en las que se encuentran estas zonas seguras con el fin de adecuar los diseños en pro de evitar inundaciones y/o riesgos eléctricos.

El trabajo en áreas seguras, se fortalece estableciendo barreras físicas y de acceso a estas áreas, para ello la Gobernación definirá que:

- Ningún funcionario deberá permanecer en un área segura fuera del horario normal de trabajo.
- Los accesos a las zonas restringidas deberán ser controlados y asignados de acuerdo a sus roles y responsabilidades.

Las zonas identificadas como restringidas deberán contar con extintores y equipo que permita controlar incidentes como incendios.

B. Equipos

Objetivo:

Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Política:

Para la protección de los equipos y mantener su vida útil se implementarán los siguientes lineamientos:

- Se establecerán normas para el consumo de alimentos en los puestos de trabajo.
- Se realizará monitoreo permanente al ambiente con el fin de mantener las temperaturas adecuadas a cada uno de los centros de procesamiento.
- Ubicar los equipos de cómputo de tal forma que se impida que la información sea visible por terceros.

Es necesario que los servicios de suministro que soportan todo el procesamiento de información como son el servicio de energía, UPS, equipos de comunicación entre otros se estén monitoreando y realizando mantenimiento preventivo para identificar fallas y corregirlas, y así mitigar los impactos que la no prestación de estos servicios pudiera ocasionar en los servicios de procesamiento con los cuales hoy cuenta la Gobernación.

El cableado estructurado de la Gobernación debe estar diseñado de tal forma que soporte los servicios tecnológicos y de comunicaciones que requiere, su diseño debe estar documentado de tal forma que se identifique la topología, los puntos, la categoría de los cables y la tecnología utilizada. Dentro de esta estructura se debe definir que la alimentación eléctrica debe estar separada del cableado estructurado con el fin de evitar interferencias.

Garantizar la disponibilidad e integridad de todos los componentes Hardware y Software de la entidad mediante un adecuado mantenimiento preventivo y correctivo de tal manera que los procesos normales de la entidad no se vean afectados por fallas en los equipos de cómputo.

El mantenimiento preventivo debe definirse dentro de un cronograma donde se establezca la ubicación del equipo y la clase de mantenimiento que se le hará, si es físico y/o lógico. El personal que realice los mantenimientos debe ser capacitado y autorizado, ya que tiene acceso a información sensible, pública, restringida, la cual debe conservar y proteger mientras realiza estas actividades.

Dentro de las hojas de vida de cada equipo se debe consignar la novedad de mantenimiento realizada de forma detallada, igualmente llevará libro de bitácora para registrar los mantenimientos realizados según cronograma.

Antes de dar de baja un equipo o reasignarlo, se debe eliminar la información sensible que este contenga, con el fin de evitar la pérdida o recuperación de información no autorizada, igualmente se debe desinstalar cualquier software, de tal forma que se evite tener problemas de licenciamiento.

La Gobernación de Nariño deberá adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Desconectar de la red / sistema / servicio los computadores personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo.
- Bloquear las impresoras o protegerlas de alguna manera del uso no autorizado fuera del horario normal de trabajo.

XI. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

A. Procedimientos Operacionales y Responsabilidades

Objetivo:

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Política:

La Gobernación a través de la Secretaria de TIC, documentará y mantendrá actualizados los procedimientos operativos en ésta política, los cuales deben ser solicitados y autorizados por el área que los requiera. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo: Procesamiento y manejo de la información.

Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.

Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

Restricciones en el uso de utilidades del sistema.

Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- Instalación y mantenimiento de las plataformas de procesamiento.
- Monitoreo del procesamiento y las comunicaciones.
- Inicio y finalización de la ejecución de los sistemas.
- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- Uso del correo electrónico.
- Gestión de cambios

La Secretaría de TIC deberá realizar monitoreo y análisis permanente a toda su infraestructura tecnológica de procesamiento de información, con el fin de identificar el estado y la utilización de todos los recursos.

Con esto se busca optimizar los recursos existentes, y apreciar las proyecciones de crecimiento, con el fin de identificar las necesidades y asegurar que la infraestructura esté en las condiciones necesarias para atender la demanda existente y la futura.

B. Protección contra códigos maliciosos

Objetivo:

Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Política:

La secretaria de TIC definirá e implementará controles de detección y prevención para la protección contra software malicioso, además desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado
- Instalar y actualizar periódicamente software de detección y reparación de virus.
- Tener las últimas actualizaciones de seguridad disponibles en los sistemas.

- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Gobernación, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a estos.

C. Copias de Respaldo

Objetivo:

Proteger contra la pérdida de datos

Política:

La Gobernación deberá asegurar que la información de los funcionarios se mantenga protegida contra pérdidas, alteración o divulgación por actos accidentales o malintencionados o por fallas de los equipos y/o redes. Para ello, deberá establecer Políticas para realizar las copias de seguridad a los servidores y bases de datos que soportan los activos de información de la entidad.

Estas Políticas deben ser explicitas en indicar la periodicidad y el tiempo con que se deben realizar las copias, definir los dispositivos de almacenamiento, la identificación que debe llevar cada copia, el lugar de almacenamiento, la responsabilidad de realizar las copias y sus actualizaciones por evolución de tecnología.

D. Registro y Seguimiento

Objetivo:

Registrar eventos y generar evidencia

Política:

Se deben elaborar registros de auditoría que contengan excepciones, fallas y otros eventos relativos a la seguridad de la información.

Los registros de auditoría deberán incluir:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad o ubicación del equipo, si se hubiera dispuesto identificación automática para la misma.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

El propietario de la información o en su defecto quien sea propuesto por el Comité para la Seguridad de la Información, definirá un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

La secretaría de TIC y los propietarios de la información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

La Secretaría de TIC asegurará el registro y la protección de las actividades realizadas por los administradores y operadores en los sistemas, incluyendo según corresponda:

- Tiempos de inicio y cierre del sistema.
- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
- Ejecución de operaciones críticas
- Cambios a información crítica

E. Control se Software Operacional

Objetivo:

Asegurarse de la integridad de los sistemas operacionales.

Política:

Únicamente el personal de la secretaría de TIC deberá realizar los procesos de instalación, desinstalación, actualización y/o modificación de software; ningún usuario que no pertenezca a dicha dependencia está autorizado para realizar ninguna de las anteriores gestiones sobre el software.

Deberá solicitarse a la Secretaria de TIC cualquier requerimiento que implique la modificación o cambio de software y estos deberán ser debidamente documentados por el área encargada con el fin de soportar los cambios realizados.

F. Gestión de Vulnerabilidad Técnica

Objetivo:

Prevenir el aprovechamiento de las vulnerabilidades técnicas

Política:

La Gobernación establecerá un procedimiento para la controlar las vulnerabilidades técnicas de los sistemas de información, el cual deberá:

- Contar con un inventario detallado, clasificado y actualizado de los activos de información.

- Disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas.
- Realizar un análisis detallado a los activos de información para identificar posibles vulnerabilidades con el fin de definir y aplicar las acciones apropiadas que permitan minimizar el impacto de las amenazas sobre la entidad.

Los usuarios de la Gobernación deben abstenerse de instalar cualquier tipo de software en sus computadores, de requerirlo deben solicitarlo a la Secretaria de TIC quien es la responsable de la instalación de los programas en todos los computadores de la Gobernación. Todo software que se instale en los computadores de la Gobernación deberá contar con su respectiva licencia y la instalación solo deberá estar permitida en equipos pertenecientes e la entidad.

G. Consideraciones Sobre Auditorias de Sistemas de Información

Objetivo:

Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos

Política:

La realización de actividades de auditoría que involucren verificaciones de los sistemas en producción, implican una planificación de los requerimientos y tareas, a fin de minimizar el riesgo de interrupción en los procesos de las áreas involucradas en la auditoría.

Para tal efecto se tendrá en cuenta lo siguiente:

- Acordar con el Área que corresponda los requerimientos de auditoría.
- El responsable de auditoría deberá controlar el alcance de las verificaciones.
- Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán las contramedidas necesarias a fin de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
    - Eliminar archivos transitorios.
    - Eliminar entidades ficticias y datos incorporados en archivos maestros.
    - Revertir transacciones.
    - Revocar privilegios otorgados
- Identificar claramente los recursos necesarios para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores.
- Identificar y acordar los requerimientos de procesamiento especial o adicional.
- Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir:
    - Fecha y hora.
    - Puesto de trabajo.
    - Usuario.
    - Tipo de acceso.
    - Identificación de los datos accedidos.
    - Estado previo y posterior.
    - Programa y/o función utilizada.
- Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

XII. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

A. Requisitos de Seguridad de los Sistemas de Información

Objetivo:

Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Política:

La Gobernación deberá implementar una política para incorporar controles de seguridad de la información a los sistemas desarrollados esta y para aquellos que sean adquiridos a terceros, y para las actualizaciones que se realicen a los sistemas ya existentes.

La evaluación de los requerimientos de seguridad debe incluir un análisis costo - beneficio, frente a la implementación de acciones de seguridad en el activo que se quiere proteger y frente al daño potencial que pudiera ocasionar a las actividades realizadas.

Para la información involucrada en los servicios de las aplicaciones que pasan a través de redes públicas, la Gobernación implementará un procedimiento, que incluya la aplicación de las políticas de Seguridad Informática implantadas en la entidad, este procedimiento debe garantizar la protección de la información, la autenticidad y confiabilidad de la

"entidad" con la que se esté haciendo el vínculo comercial.

Para la información involucrada en las transacciones de los servicios de las aplicaciones que pasan a través de redes públicas, la Gobernación aplicará todas las políticas de Seguridad Informática definidas al interior de la entidad, garantizando la integridad de la misma, realizando operaciones en línea bajo los parámetros de integridad, confiabilidad y seguridad, para evitar cualquier posible fraude o intrusión sin autorización a la información vital de la Gobernación.

Para garantizar transacciones por redes telemáticas seguras, es relevante tener en cuenta lo siguiente:

- Utilizar siempre un computador personal con antivirus para acceder a sitios de comercio electrónico y asegurarse de que la dirección que se presenta en el navegador corresponde al sitio que realmente se quiere visitar.
- No utilizar links en páginas de terceros o recibidos vía email y asegurarse de que el sitio tenga una conexión segura, es decir, que los datos transmitidos entre el navegador y el sitio están encriptados.
- Configurar el programa de e-mail para que no ejecute programas automáticamente.
- No realizar transacciones con empresas que solicitan un depósito y no dan la opción de pagar con tarjeta de crédito.
- Realizar transacciones sólo en sitios de instituciones que se consideren confiables, dando preferencia a las empresas grandes y conocidas.
- Nunca digitar la clave o datos personales en emails, aunque se hayan recibido de la empresa.

B. Seguridad en los Procesos de Desarrollo y de Soporte

Objetivo:

Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

Política:

La Gobernación deberá establecer y aplicar controles para el desarrollo interno o externo de los sistemas de información que cumplan con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, cuenta con el nivel de soporte requerido por la entidad.

Para minimizar los riesgos de alteración de los sistemas de información, la Gobernación implementará procedimientos para el control de cambios a los sistemas dentro del ciclo de vida de desarrollo; dichos procedimientos deben incluir:

- Únicamente usuarios autorizados realizaran cambios en las aplicaciones, basándose en las políticas establecidas por la entidad y a las licencias de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del propietario de la información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- La Secretaría de TIC aprobará las tareas necesarias para la gestión de los cambios, antes de que éstas inicien.
- La Secretaría de TIC deberá verificar y garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Las pruebas deben ser realizadas en el ambiente correspondiente y las mismas deben ser aprobadas por parte del usuario final autorizado para tal fin.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Informar a las áreas afectadas antes de la implementación de un cambio que pueda afectar sus operaciones.
- La Secretaría de TIC es la encargada de efectuar la actualización de los datos en el nuevo sistema de información.

La secretaría de TIC de la Gobernación aplicará los principios de desarrollo seguros, documentando y aplicando procesos en la implementación de cualquier sistema de información.

En caso de que la Gobernación requiera del desarrollo de software por parte de terceros, deberá establecer normas y procedimientos que contemplen lo siguiente:

- Acuerdos de licencias, propiedad de código y derechos conferidos.
- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- Una vez finalizado el proyecto software, el contratista entregará a la Gobernación el código fuente, manuales de usuario, documentos de ingeniería de software y cualquier tipo de información relacionada con el mismo.

La Secretaría de TIC de la Gobernación deberá llevar a cabo las pruebas de la funcionalidad durante el desarrollo del sistema, las cuales deberán quedar debidamente documentadas, además deberá establecer los requisitos para poner en producción un sistema nuevo o una actualización a un sistema ya existente. Antes de pasar a ambientes de producción se requiere realizar y documentar las pruebas de funcionamiento en ambientes de pruebas, en compañía de los usuarios que utilizarán la aplicación para conocer que todas las formas a actualizar o poner en producción satisfacen las necesidades expuestas por los usuarios, antes definidas en los requisitos funcionales entregados.

C. Datos de Prueba

Objetivo:

Asegurar la protección de los datos usados para pruebas

Política:

Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente, para ello se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

XIII. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

A. Seguridad de la Información en las relaciones con los Proveedores

Objetivo:

Asegurar la protección de los activos de la Gobernación que sean accesibles a los proveedores.

Política:

La Secretaría de TIC y el propietario de la información, llevarán a cabo y documentarán una evaluación de riesgos a la hora de otorgar acceso a terceras partes a la información de la Gobernación, para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la Seguridad Informática de la Organización.
- Tener estrategias para evitar el mínimo necesario de permisos a otorgar.

Los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, deben quedar claramente estipulados dentro del contrato de prestación de servicios a firmar entre las partes. Dentro de los acuerdos con terceros, se debe incluir:

- Cumplimiento de la Política de Seguridad Informática de la Organización.
- Protección de los activos de la Gobernación, incluyendo:
    - Procedimientos para proteger los bienes de la Organización, abarcando los activos físicos, la información y el software.
    - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por

ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Nivel de servicio esperado y niveles de servicio aceptables.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

- Existencia de Derechos de Propiedad Intelectual.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:

    - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
    - Proceso de autorización de accesos y privilegios de usuarios.

- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

Todos los requisitos de seguridad informática pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la Gobernación, quedando éstos debidamente estipulados en el contrato con el respectivo proveedor.
La Gobernación incluirá en el respectivo contrato los requisitos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos.

B. Gestión de la Prestación de Servicios de Proveedores

Objetivo:

Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

Política:

Cualquier cambio o modificación en los servicios por parte de los proveedores, deberá estar debidamente sustentado y autorizado por la Gobernación, siguiendo las políticas internas de la entidad.

XIV. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

A. Gestión de Incidentes y Mejoras en la Seguridad de la información

Objetivo:

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Política:

La Gobernación establecerá responsabilidades y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Se deben considerar los siguientes ítems:

- ✓ Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:

    - Fallas operativas
    - Código malicioso
    - Intrusiones
    - Fraude informático
    - Error humano
    - Catástrofes naturales

- ✓ Registrar pistas de auditoría y evidencia similar para:
  - Análisis de problemas internos.
  - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
  - Negociación de compensaciones por parte de los proveedores de software y de servicios.

- ✓ Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
  - Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
  - Documentación de todas las acciones de emergencia emprendidas en forma detallada.
  - Comunicación de las acciones de emergencia al personal encargado de restablecer el servicio y revisión de su cumplimiento.
  - Constatación de la integridad de los controles y sistemas de la Gobernación en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del área jurídica de la Gobernación en el tratamiento de incidentes de seguridad ocurridos y sus implicaciones en todos los niveles.

Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como se tenga conocimiento del incidente.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre estos.

La Secretaría de TIC será informada ante la detección de un supuesto incidente o violación de la seguridad, tan pronto como se haya tomado conocimiento. Esta indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Así mismo, mantendrá al Comité de Seguridad de la información al tanto de la ocurrencia de incidentes de seguridad.

La Gobernación evaluará el incidente, y si lo estima pertinente, informará a las autoridades competentes de la ocurrencia del mismo.

Es responsabilidad de los funcionarios informar de cualquier incidente de seguridad del que tenga conocimiento directo o indirecto, con el fin de tomar las acciones para mitigar los posibles impactos del mismo.

Ningún funcionario está autorizado a realizar pruebas para detectar posibles fallas de seguridad; dichas acciones sólo podrán ser realizadas por el personal designado para tal fin.

La Gobernación evaluará los eventos de Seguridad Informática ocurridos en su interior, a fin de valorarlos y clasificarlos o no como incidentes; para realizar la corrección pertinente sobre los hallazgos arrojados en la evaluación de dichos eventos.

La Gobernación proporcionará los recursos suficientes para dar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la misma y que afecten la continuidad de su operación. Además, se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. Así mismo se definirá un proceso para documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías de seguridad, con el fin de identificar aquellos que sean recurrentes o de mayor impacto para la entidad.

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién, dónde, cuándo se halló y quién presenció el hallazgo.
- Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Ante cualquier medida legal que involucre personas ajenas a la Gobernación u otras organizaciones, la entidad deberá contar con asesoría jurídica a fin de no incurrir en violaciones a la ley y a los derechos sobre quien recaiga la acción judicial.

XV. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

A. Continuidad de Seguridad de la Información

Objetivo:

La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la Gobernación.

Política:

La Gobernación determinará los requisitos para la seguridad de la información, y deberá establecer, documentar, implementar y mantener procesos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información en situaciones adversas. Estos controles se verificarán a intervalos regulares con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

B. Redundancias

Objetivo:

Asegurar la disponibilidad de instalaciones de procesamiento de información

Política:

La Gobernación propenderá por la existencia de recursos tecnológicos redundantes que satisfagan los requerimientos de disponibilidad aceptables para la misma.

XVI. POLÍTICAS DE CUMPLIMIENTO

A. Cumplimiento de Requisitos Legales y Contractuales

Objetivo:

Evitar el incumplimiento de las obligaciones legales, estatuarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Política:

Toda información soportada por la infraestructura tecnológica de la Gobernación deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

El almacenamiento de la información de la entidad deberá realizarse interna y/o externamente, esto de acuerdo con la importancia que dicha información tenga para las operaciones de la Gobernación.

En cuanto a los soportes de información físicos, la entidad aplicará los controles que tiene establecidos para tal fin, los cuales se ajustan a la normatividad en esa materia, con el fin de garantizar la conservación de dichos soportes y efectuar una debida destrucción de los mismos, cuando sea necesario.

Es obligación de la Gobernación hacer las gestiones y consultas legales pertinentes para el uso de controles criptográficos, a fin de no incurrir en faltas a la ley, ya sea para el manejo de información dentro o fuera del país.

B. Revisiones de Seguridad de la Información

Objetivo:

Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Política:

Es obligación del Comité para la seguridad de la Información revisar independientemente a intervalos planificados y realizar una evaluación periódica de los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información a fin de evaluar su eficacia y efectividad y tomar las acciones correctivas pertinentes o si es del caso replantear las políticas que no proporcionan los resultados esperados por la Gobernación.

La Secretaria de TIC verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

El resultado de la evaluación debe quedar consignado en un informe técnico para su interpretación por parte de los especialistas.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados.

Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

XVII. PROCEDIMIENTOS DOCUMENTADOS

En este documento se describe algunos de los procedimientos de las políticas establecidas en el anexo A. Un procedimiento es la secuencia de

actividades mediante un método explicando de manera clara y sencilla las indicaciones de los pasos a realizar.

En la Gobernación de Nariño se cuenta con los siguientes procedimientos:

- Procedimiento para copias de seguridad
- Procedimiento para instalación de software
- Procedimiento para actualización de software
- Procedimiento para adquisición de software
- Procedimiento para cambio de hardware
- Procedimiento para Levantamiento de panorama de riesgos
- Procedimiento para Capacitación en gestión de riesgos industriales
- Procedimiento para Evaluación de salud ocupacional
- Procedimiento para Gestión documental física, correspondencia física, trámites empresariales.

1. Procedimiento para Copias de Seguridad

Este procedimiento describe el método para realizar las copias de seguridad de la información de la Gobernación de Nariño.

1. Objetivo

Establecer en la Gobernación la realización de copias de seguridad al principal activo informático, la información para garantizar su disponibilidad integridad y confidencialidad.

2. *Alcance*

Empieza con establecer necesidad de respaldo de la información del equipo y finaliza con el cierre del servicio y verificación del cumplimiento de los lineamientos.

3. *Definiciones*

- **Carpeta:** Parte específica donde se almacenan archivos informáticos en un equipo de cómputo.
- **Frecuencia:** Periodicidad con la cual se realizan copias de respaldo.
- **Copia de respaldo:** Copia de archivos de trabajo en medio digital sobre servidor del sistema de información.

4. *Condiciones Generales*

Bajo ninguna circunstancia debe dejarse de realizar este procedimiento por parte del responsable de mimo o por quien haga sus veces en su ausencia, por lo cual también debe conocer cabalmente este procedimiento.

5. Descripción del procedimiento

El procedimiento de copia de seguridad se base en el respaldo necesario para los datos de la gestión de la empresa. Ver *Tabla 1*.

Tabla 49. Descripción de Actividades de Copias de Seguridad

DESCRIPCIÓN DE ACTIVIDADES				
NO	***ACTIVIDAD***	***DESCRIPCIÓN DE LA ACTIVIDAD***	***DOCUMENTO DE TRABAJO***	***RESPONSABLE***
1	***Establecer la necesidad de respaldar la información***	***El funcionario que requiera que se respalde la información que contiene su equipo computo debe crear una carpeta llamada "User Data" en la carpeta Mis Documentos***	***Carpeta creada***	***Funcionario***
2	***Trasladar la Información Institucional a User Data***	***Trasladar la información institucional que se requiere respaldar a la carpeta "User Data".*** ***La Información a trasladar debe ser solo de uso laboral***	***Información contenida en la carpeta User Data***	***Funcionario***
3	***Solicitar el servicio de***	***Solicitar el servicio de Respaldo***	***Solicitud de respaldo de***	***Personal Secretaría TIC***

DESCRIPCIÓN DE ACTIVIDADES				
NO	***ACTIVIDAD***	***DESCRIPCIÓN DE LA ACTIVIDAD***	***DOCUMENTO DE TRABAJO***	***RESPONSABLE***
	respaldo de la Información	***de información corporativa a la Secretaria TIC indicando el tamaño de la carpeta.***	***información***	
4	***Autorizar el respaldo de la Información***	***Autorizar o denegar la copia de respaldo de la información.***	***Registrar nota de observación con la Autorización y/o denegación dejando la justificación.***	***Personal Secretaría TIC***
5	***No Autoriza el respaldo de la información***	***Se deja nota de negación del servicio y se finaliza el procedimiento.*** ***Si acepta el servicio se continúa con el paso 6.***		***Personal Secretaría TIC***
6	***Realizar copia de respaldo***	***Realizar las copias de respaldo de la información, software e imágenes requeridas.***		***Personal Secretaría TIC***
7	***Verificar la copia de respaldo***	***Revisar que la información de respaldo haya quedado grabada***		***Personal Secretaría TIC***
8	***Fin del procedimiento.***			

Fuente: La presente investigación

6. *Responsables*

Responsable estratégico: Profesional Universitario - Secretaría TIC; Responsable Operativo: Técnico Administrativo**.**

7. Duración del Procedimiento

El tiempo total empleado en este proceso es de alrededor de 30 minutos.

2. Procedimiento para Actualización de Software

Este procedimiento describe el método para actualización de software de la empresa.

1. *Objetivo*

Mantener disponibles y óptimos los sistemas de información que la institución requiere para la toma de decisiones, para el control de las operaciones, el análisis de los problemas y la creación de nuevos servicios y/o trámites. Asegurar que la actualización de software se realice en forma autorizada, previa verificación de calidad de la nueva versión.

2. *Alcance*

Inicia con la conformación de un inventario de sistemas de información y termina con el seguimiento permanente. Mantener actualizado él software de la empresa para que se aprovechen las últimas mejoras en funcionalidad y corrección de errores.

3. *Definiciones*

- **Sistema de información:** Es un sistema de información basado en computadora, que presenta una colección de personas, procedimientos, bases.

4. Condiciones Generales

Cuando se tenga conocimiento de la disponibilidad de una nueva versión del software se procederá a indagar sus bondades y a determinar su adquisición.

5. Descripción del Procedimiento

El procedimiento de actualización de software se realiza cada vez que se tiene conocimiento de que una nueva versión está disponible. *Ver Tabla 2*.

Tabla 50. Descripción de Actividades de Actualización de Software

DESCRIPCIÓN DE ACTIVIDADES				
NO	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	DOCUMENTO DE TRABAJO	RESPONSABLE
1	Inventario	Conformación de inventario de Sistemas de información.	Hoja de vida Sistemas de Información, formulario de seguimiento, plataforma web	Profesional Universitario
2	Administrar sistemas de información	Revisión de contratos, convenios o actos administrativos de adquisición, revisión de manuales de usuario y diccionario de datos.	Documentos soporte	Profesional Universitario
3	Caracterización de usuarios	Creación y/o modificación de usuarios por perfiles y roles, asignar privilegios en el sistema de información.	Designación de responsabilidades Correos Electrónicos	Profesional Universitario
4	Parametrizar el Sistema de Información	Configurar el sistema de Información con datos relevantes y estandarizados en tablas maestras, para la ejecución de procesos.	Oficios, correos electrónicos, solicitudes soportadas, normatividad	Profesional Universitario.
5	Actualización de base de datos.	Revisar, controlar y actualizar de forma constante las bases de datos de acuerdo a los requerimientos de los usuarios del sistema de información.	Oficios, correos electrónicos, solicitudes soportadas, normatividad	Profesional Universitario, Administrador del Sistema de Información.
6	Mantenimiento de Sistemas de Información	Realizar mantenimiento preventivo en los sistemas de información, realizar copias de seguridad periódicas, indexación de base de datos, depuración de errores en datos, consolidación de base de datos.	Copias de Seguridad y bitácora de mantenimiento y backups.	Profesional Universitario, Administrador del Sistema de Información.
7	Actualización de Sistemas de Información	Solicitar actualizaciones a los proveedores de los sistemas de información y/o realizar actualizaciones de acuerdo a los requerimientos realizados por los usuarios, normas o leyes.	Documentos Soporte, requerimientos, normatividad	Profesional Universitario, Administrador del Sistema de Información.

DESCRIPCIÓN DE ACTIVIDADES				
NO	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	DOCUMENTO DE TRABAJO	RESPONSABLE
8	Pruebas de Funcionamiento	Crear instancias para pruebas de funcionamiento cuando se emita una nueva actualización	Acta de creación de instancia-software	Profesional Universitario, Administrador del Sistema de información o Tercero.
9	Implementación de actualización	Instalar actualización para funcionamiento en el sistema de información.	Acta de entrega de actualización	Profesional Universitario, Administrador del Sistema de información o Tercero.
10	Seguimiento y control	Realizar seguimiento y control permanente.	Bitácora	Profesional Universitario, Administrador del Sistema de información.
11	Fin del Procedimiento			

Fuente: La presente investigación

6. Responsables

Responsable estratégico: Secretaría TIC, Innovación y Gobierno Abierto; Responsable Operativo: Profesional Universitario.

7. Duración del Procedimiento

Todo el proceso de actualización de software y capacitación no debe tomar más cinco días hábiles.

C. Procedimiento para Cambio de Software

Este procedimiento describe el método para determinar y realizar el cambio de software.

1. *Objetivo*

Propender por el adecuado desarrollo de sistemas de información y/o adquisición, para la gestión organizacional. Asegurar que la empresa cuente con las mejores herramientas informáticas para su gestión.

2. *Alcance*

Inicia por la recolección de información y necesidades, termina en el seguimiento y control. Sin estar haciendo erogaciones innecesarias, mantener al día el software de gestión que le sea de mayor utilidad a la empresa.

3. *Definiciones*

- **Software:** Se conoce como un software al equipamiento o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

4. *Condiciones Generales*

Cuando se tenga conocimiento de la disponibilidad de un software que mejore la gestión de información en la empresa se procederá a indagar sus bondades y a determinar su adquisición.

5. Descripción del Procedimiento

El procedimiento para la adquisición de software se realiza cada vez que se tiene conocimiento de la disponibilidad de un buen producto y se procede así: *Ver Tabla 3*.

Tabla 51. Descripción de Actividades de Cambio de Software

DESCRIPCIÓN DE ACTIVIDADES				
NO	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	DOCUMENTO DE TRABAJO	RESPONSABLE
1	Recolección de información y necesidades	Recopilar información o requerimientos de necesidades de las diferentes dependencias de la Gobernació	Registro de necesidades Correos electrónicos	Profesionales Universitarios- Gestores de TICS y/o terceros.

DESCRIPCIÓN DE ACTIVIDADES				
NO	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	DOCUMENTO DE TRABAJO	RESPONSABLE
		n de Nariño.		
2	Selección de alternativas de solución	Analizar las necesidades y requerimientos, seleccionar alternativas de solución	Registro de necesidades Correos electrónicos Cotizaciones Propuestas	Profesionales Universitarios- Gestores de TICS y/o terceros.
3	Diseño de Alternativa de Solución	Revisar modelos y/o establecer diseño de la alternativa de solución.	Modelos Propuestas Cotizaciones	Profesionales Universitarios- Gestores de TICS y/o terceros.
4	Desarrollo y/o Adquisición del sistema	Programar y/o adquirir el sistema de información	Estudios previos Diseño Actas de avance	Profesionales Universitarios- Gestores de TICS y/o terceros.
5	Construcción de Manuales	Elaboración de manuales técnico y de usuario, Recepción y revisión de manuales a contratista	Manuales técnico y de usuario	Profesionales Universitarios- Gestores de TICS y/o terceros.
6	Implementación del sistema	Implementar prototipo o aplicativo para fase de pilotaje en instancias de prueba. Realización	Contratos Actas de avance	Profesionales Universitarios- Gestores de TICS y/o terceros.

DESCRIPCIÓN DE ACTIVIDADES				
NO	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	DOCUMENTO DE TRABAJO	RESPONSABLE
		de pruebas de funcionament Fuente: La presente investigación o y controles con usuarios.		
7	Evaluación del Proceso	¿Cumple con los requerimientos establecidos y el proceso es adoptado administrativamente? SI: Ir a actividad 7 NO: Ir a actividad 2	NA	Profesionales Universitarios- Gestores de TICS y/o terceros.
8	Asesoría y Capacitación	Asesoría y Capacitación en el manejo del sistema de información	Manuales de usuario	Profesionales Universitarios- Gestores de TICS y/o terceros.
9	Implantación del sistema	Poner en funcionamiento el sistema de información	Acta de entrega	Profesionales Universitarios- Gestores de TICS y/o terceros.

DESCRIPCIÓN DE ACTIVIDADES				
NO	***ACTIVIDAD***	***DESCRIPCIÓN DE LA ACTIVIDAD***	***DOCUMENTO DE TRABAJO***	***RESPONSABLE***
10	***Actualización de Sistema de información***	***Administración, mantenimiento y actualización de sistemas de información para corrección de errores o nuevos requerimientos***	***Requerimientos***	***Profesionales Universitarios-Gestores de TICS y/o terceros.***
11	***Fin del Procedimiento***			

Fuente: La presente investigación

6. Responsables

Responsable estratégico: Profesional Universitario - Secretaría TIC; Responsable Operativo: Profesional Universitario.

7. Duración del Procedimiento

El tiempo del proceso de adquisición e implementación de software y capacitación depende del producto a ser comprado y sus dimensiones funcionales.

D. Procedimiento para Cambio de Hardware

Este procedimiento describe el método para determinar cuándo realizar el cambio de hardware.

1. *Objetivo*

Mantener vigente la plataforma hardware de la empresa acorde con la tecnología de vanguardia que ofrezca mejoras significativas en capacidad de cómputo.

2. *Alcance*

Sin incurrir en gastos innecesarios, disponer del hardware de apoyo a la gestión de la empresa, que cuente con las mejores características técnicas.

3. *Definiciones*

- **Hardware**: Parte física del sistema informático principalmente computadores y periféricos, con todos sus componentes internos que determinan su poder de computo.

4. Condiciones Generales

Conforme el volumen de información de la empresa crece, la demanda de realización de procesos con esa información, mayor volumen mayor velocidad, la necesidad de contar con comunicaciones más ágiles, etc. Conllevan la necesidad de contar con mayor poder de cómputo, lo cual se evidencia alrededor de cada dos años, lo cual obliga a la renovación paulatina de equipos.

5. Descripción del Procedimiento

El procedimiento para la adquisición de hardware se realiza periódicamente y se procede de la siguiente forma: *Ver Tabla 4*.

Tabla 52. Descripción de Actividades de Cambio de Hardware

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	***Descripción de la actividad***	***Documento de trabajo***	***Responsable***
1	***Verificación de las condiciones de los equipos actuales***	***Verificación de las condiciones de los equipos actuales en la empresa, de la necesidad de incrementar la capacidad de cómputo y de renovación de equipos.***	***Actas de adquisición de Equipos.***	***Profesional Universitario y soporte técnico***
2	***Requerimientos y cotizaciones***	***Realización de determinación de requerimientos y cotizaciones.***	***Actas de adquisición de Equipos.***	***Profesional Universitario y soporte técnico***
3	***Requerimientos, cotizaciones y costos***	***Aprobación de identificación de requerimientos***	***Actas de adquisición de Equipos.***	***Profesional Universitario y soporte técnico***

DESCRIPCIÓN DE ACTIVIDADES				
No	**Actividad**	***Descripción de la actividad***	***Documento de trabajo***	***Responsable***
		cotizaciones y costos.		
4	***cronograma***	***Planeación del cronograma de adquisición e instalación de equipos y toma de respaldo de la información uno a uno.***	***Actas de adquisición de Equipos.***	***Profesional Universitario y soporte técnico***
5	***Cambio de equipos***	***Realización del cambio de equipo uno a uno haciendo la restauración de información.***	***Actas de adquisición de Equipos.***	***Profesional Universitario y soporte técnico***
8	***Fin del procedimiento.***			

Fuente: La presente investigación

6. *Responsables*

Responsable estratégico: Profesional Universitario Secretaría TIC; Responsable Operativo: Profesional Universitario.

7. *Duración del Procedimiento*

El tiempo del proceso de adquisición e instalación de hardware depende del producto a ser comprado y disponibilidad del proveedor

ANEXO F Análisis de Riesgos Para los Principales Activos de la Secretaría de Tic, Innovación y Gobierno Abierto de la Gobernación de Nariño.

ANÁLISIS DE VULNERABILIDADES

En la siguiente tabla se visualiza las vulnerabilidades del activo **Base de datos Proyectos de la Gobernación.**

Tabla 53 Vulnerabilidades Base de Datos Proyectos de la Gobernación

Activo STIC-01		**Base de Datos Proyectos de la Gobernación**	
Administrador		**Profesional Universitario**	
Tipo activo		**Datos/Información**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del Administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información para el manejo del activo.
	E19	Fugas de Información.	La entidad no capacita a los funcionarios sobre la seguridad de la información. Falta de políticas de confidencialidad de información.
Ataques Intencionados	A15	Modificación Deliberada de la información	Carencia de políticas de seguridad de uso de soportes de información externos.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Código fuente Portal Web Gobernación de Nariño, Portales**

Tabla 54 Vulnerabilidades Código fuente Portal Web Gobernación de Nariño

Activo STIC-02		**STIC-02 Código Fuente Portal Web de la Gobernación de Nariño, Portales.**	
Administrador		**Administrador Portal Web**	
Tipo activo		**Datos/información**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	El antivirus no se actualiza diariamente.
	E4	Errores de configuración	No cuenta con una protección segura para ataques al sitio web.
	E19	Fugas de información	Los datos no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.
Ataques intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Correo Electrónico Institucional**

Tabla 55 Vulnerabilidades Correo Electrónico Institucional

Activo STIC-03		**STIC-03 Correo Electrónico Institucional.**	
Administrador		**Administrador Correo**	
Tipo activo		**Servicio**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E1	Errores de los usuarios	El usuario no cuenta con capacitación respecto a la seguridad de la información.
	E2	Errores del administrador	No existe un análisis de seguridad para los correos spam.
	E4	Errores de configuración	No cuenta con una protección segura para ataques al sitio web.
	E19	Fugas de información	Los datos no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.
Ataques intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido
	A13	Repudio	Carencia de mecanismos que controlen el envío y recepción de mensajes.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Servicio Técnico y de Software Equipos de Cómputo**

Tabla 56 Vulnerabilidades Servicio Técnico y de Software Equipos de Cómputo

Activo STIC-04		**STIC-04 Servicio Técnico y de Software Equipos de Cómputo.**	
Administrador		**Soporte Técnico**	
Tipo activo		**Servicio**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información. Falta de planilla de registro para los equipos.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Servicios de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas Gobernación de Nariño.**

Tabla 57 Vulnerabilidades Servicios de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas Gobernación de Nariño.

Activo STIC-05		**STIC-05 Servicios de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas Gobernación de Nariño.**	
Administrador		**Área de Soluciones TI**	
Tipo activo		**Servicio**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información.
	E19	Fugas de información	Los datos de los soportes de información y plataformas no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.**

Tabla 58 Vulnerabilidades Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.

Activo STIC-06		**STIC-06 Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.**	
Administrador		**Soporte Técnico**	
Tipo activo		**Servicio**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información.
	E19	Fugas de información	Los datos de los servidores no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Software Sistema de Backup en el Servidor**

Tabla 59 Vulnerabilidades Software Sistema de Backup en el Servidor

Activo STIC-08	**STIC-08 Software Sistema de Backup en el servidor**		
Administrador	**Soporte Técnico**		
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.
	E19	Fugas de información	Los datos de los sistemas de información no son correctamente protegidos.
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.
	E21	Errores de Mantenimiento/actualización Software	Software no Licenciado Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.

Tabla 59 (Continuación)

Activo STIC-08	**STIC-08 Software Sistema de Backup en el servidor**		
Administrador	**Soporte Técnico**		
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición/Vulnerabilidad**
Ataques intencionados	A5	Suplantación de la identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro de los sistemas para prevenir ataques informáticos.
	A18	Destrucción de información.	Falta de Controles de seguridad dentro de los sistemas, para prevenir ataques informáticos.

Fuente: La presente investigación

En la siguiente tabla de visualiza las vulnerabilidades del activo **Software Portal Web Gobernación de Nariño**

Tabla 60 Vulnerabilidades Software Portal Web Gobernación de Nariño

Activo STIC-09	**STIC-09 Software Portal Web Gobernación de Nariño**		
Administrador	**Administrador Portal Web**		
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Seguridad de la Información.
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.
	E19	Fugas de información	Los datos del software no son correctamente protegidos.
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.
	E21	Errores de Mantenimiento/actualización Software	Falta de planes de actualización de software. Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.

Tabla 60 (Continuación)

Activo STIC-09	**STIC-09 Software Portal Web Gobernación de Nariño**		
Administrador	**Administrador Portal Web**		
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Ataques intencionados	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.

Fuente: La presente investigación

En la siguiente tabla de visualiza las vulnerabilidades del activo **Software SYSMAN**

Tabla 61 Vulnerabilidades Software SYSMAN

Activo STIC-10	**STIC-10 Software SYSMAN**		
Administrador			
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Seguridad de la Información. No se realiza capacitaciones para el manejo del software No se realizan auditorias para verificar la calidad y el funcionamiento del software. No se realiza soporte inmediato frente a fallas del software
	E8	Difusión de Software Dañino.	Hay poca capacitación para los empleados que utilizan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb.
	E19	Fugas de información	La entidad no capacita a los empleados que utilizan software sobre la seguridad de la información.
	E20	Vulnerabilidades de los Programas(Software)	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento. Falta de Políticas de uso de aplicaciones e información.
	E21	Errores de Mantenimiento/actualización Software	Falta de planes de actualización de software. Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.

Tabla 61 (Continuación)

Activo STIC-10		**STIC-10 Software SYSMAN**	
Administrador			
Tipo activo		**Software**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Ataques intencionados	A5	Suplantación de la Identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Software SISCAR**

Tabla 62 Vulnerabilidades Software SISCAR

Activo STIC-11	**STIC-11 Software SISCAR**		
Administrador			
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Seguridad de la Información. No se realizan auditorias para verificar la calidad y el funcionamiento del software.
	E8	Difusión de Software Dañino.	Hay poca capacitación para los empleados que utilizan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb.
	E19	Fugas de información	Los datos del software no son correctamente protegidos. La entidad no capacita a los empleados que utilizan software sobre la seguridad de la información.
	E20	Vulnerabilidades de los Programas(Software)	Falta de Políticas de uso de aplicaciones e información.
	E21	Errores de Mantenimiento/actualización Software	Falta de planes de actualización de software. Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.

Tabla 62 (Continuación)

Activo STIC-11	**STIC-11 Software SISCAR**		
Administrador			
Tipo activo	**Software**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Ataques intencionados	A5	Suplantación de la Identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Computadores de Escritorio**

Tabla 63 Vulnerabilidades Computadores de Escritorio

Activo STIC-13		**STIC-13 Computadores de Escritorio**	
Administrador			
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo
	N2	Daños por agua	Los computadores de escritorio se encuentran ubicados sin ninguna precaución.
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
	I3	Contaminación Mecánica	Consumir alimentos a lado de los equipos.
	I5	Avería de Origen Físico o Lógico	Defectos de fábrica de los equipos.

Tabla 63 (Continuación)

Activo STIC-13	**STIC-13 Computadores de Escritorio**		
Administrador			
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De Origen Industrial	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Espacio ilimitado entre los equipos de escritorio No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.
Erores y Fallos	E2	Errores del Administrador	Sobrecarga de trabajo No existe un protocolo para la instalación de las diferentes aplicaciones.
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los equipos. Falta de controles o Políticas de mantenimiento preventivo y periódico a los computadores de escritorio.
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal
	A11	Acceso no autorizado	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios.
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Computadores Portátiles.**

Tabla 64 Vulnerabilidades Computadores Portátiles

Activo STIC-14	**STIC-14 Computadores Portátiles**		
Administrador			
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo
	N2	Daños por agua	Los computadores portátiles se encuentran ubicados sin ninguna precaución.
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
	I3	Contaminación Mecánica	Consumir alimentos a lado de los equipos.
	I5	Avería de Origen Físico o Lógico	Defectos de fábrica de los equipos.
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS

Tabla 64 (Continuación)

Activo STIC-14	**STIC-14 Computadores Portátiles**		
Administrador			
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De Origen Industrial	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.
Erores y Fallos	E2	Errores del Administrador	Sobrecarga de trabajo No existe un protocolo para la instalación de las diferentes aplicaciones.
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los equipos. Falta de controles o Políticas de mantenimiento preventivo y periódico a los computadores de escritorio.
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal
	A11	Acceso no autorizado	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios.
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Impresoras**

Tabla 65 Vulnerabilidades Impresoras

Activo STIC-15	**STIC-15 Impresoras**		
Administrador			
Tipo activo	**Hardware**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo
	N2	Daños por agua	Las impresoras se encuentran ubicadas sin ninguna precaución.
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.
	I*	Desastres Industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
	I5	Avería de Origen Físico o Lógico	Mala ubicación de las impresoras.
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.

Tabla 65 (Continuación)

Activo STIC-15		**STIC-15 Impresoras**	
Administrador			
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Erores y Fallos	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para las impresoras Falta de controles o Políticas de mantenimiento preventivo y periódico a las impresoras.
	E24	Caída del sistema por agotamiento de recursos.	Falta de papel para impresoras tinta y el tóner.
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Escáner**

Tabla 66 Vulnerabilidades Escáner

Activo STIC-16		**STIC-16 Escáner**	
Administrador			
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo
	N2	Daños por agua	Los escáneres se encuentran ubicados sin ninguna precaución.
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.
	I*	Desastres Industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
	I5	Avería de Origen Físico o Lógico	Mala ubicación de los escáneres.
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.

Tabla 66 (Continuación)

Activo STIC-16		**STIC-16 Escáner**	
Administrador			
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Erores y Fallos	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los escáneres. Falta de controles o Políticas de mantenimiento preventivo y periódico a los escáneres.
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Red Inalámbrica y Local.**

Tabla 67 Vulnerabilidades Red Inalámbrica y Local

Activo STIC-17		**STIC-17 Red Inalámbrica y Local**	
Administrador			
Tipo activo		**Comunicaciones**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De origen Industrial	I8	Fallo de servicios de comunicaciones	Desconexión de un cable de red. Dispositivos de comunicación quemados Dispositivos de comunicación mal configurados.
	E9	Errores de [RE-] Encaminamiento	Falta de medidas de seguridad.
	A5	Suplantación de la Identidad del Usuario.	Falta de Privilegios de acceso a las redes.
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **UPS**

Tabla 68 Vulnerabilidades UPS

Activo STIC-18	**STIC-18 UPS**		
Administrador			
Tipo activo	**Auxiliar**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.

Tabla 68 (Continuación)

Activo STIC-18	**STIC-18 UPS**
Administrador	
Tipo activo	**Auxiliar**

Tipo	ID	Amenaza	Exposición / Vulnerabilidad
De Origen Industrial	I3	Contaminación Mecánica	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad.
	I5	Avería de Origen físico o lógico.	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad. Falta de controles físico y lógicos como el mantenimiento preventivo de hardware.
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.
Errores y Fallos	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de las UPS Falta de controles de mantenimiento preventivo y periódico a las UPS. Falta de plan de Gestión y control de recursos vs requerimientos.
taques intencionados	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.
	A23	Manipulación de los equipos.	Falta de controles para el ingreso a la sala de comunicaciones.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Sala de Comunicaciones.**

Tabla 69 Vulnerabilidades Sala de Comunicaciones

Activo STIC-19		**STIC-19 Sala de Comunicaciones**	
Administrador			
Tipo activo		**Instalaciones**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.

Tabla 69 (Continuación)

Activo STIC-19	**STIC-19 Sala de Comunicaciones**		
Administrador			
Tipo activo	**Instalaciones**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Ataques intencionados	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Secretaría TIC, Innovación y Gobierno Abierto**

Tabla 70 Vulnerabilidades Secretaría TIC, Innovación y Gobierno Abierto

Activo STIC-20	**STIC-20 Secretaría TIC, Innovación y Gobierno Abierto**		
Administrador	-		
Tipo activo	**Instalaciones**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres Naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.

Tabla 70 (Continuación)

Activo STIC-20	**STIC-20 Secretaría TIC, Innovación y Gobierno Abierto**		
Administrador	**-**		
Tipo activo	**Instalaciones**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De Origen Industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.
Ataques intencionados	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la Secretaría TIC..

Fuente: La presente investigación

En la siguiente tabla se visualiza las vulnerabilidades del activo **Personal TIC**

Tabla 71 Vulnerabilidades Personal TIC

Activo STIC-21	**STIC-21 Personal TIC**		
Administrador	_		
Tipo activo	**Personal**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y Fallos	E7	Deficiencias en la Organización,	Falta de capacitación sobre seguridad de la Información. Falta me mecanismos de monitoreo de personal Falta de políticas de uso correcto de telecomunicaciones. Falta de políticas de contratación.
	E19	Fugas de Información	Falta de capacitación sobre seguridad de la Información.
	E28	Indisponibilidad del Personal	Falta de un plan de contingencia en caso de ausencia
Ataques intencionados	A28	Indisponibilidad del Personal	Falta de un plan de contingencia en caso de ausencia
	A29	Extorsión	Falta de Políticas que definan un procedimiento a seguir ante vulnerabilidades de este tipo.
	A30	Ingeniería Social	Falta de capacitación sobre seguridad de la Información. Falta de concientización del personal en las mejores prácticas de seguridad informática.

Fuente: La presente investigación

ESTIMACIÓN DEL IMPACTO

A continuación, se realiza la estimación del impacto para el activo **Base de datos Proyectos de la Gobernación**

Tabla 72 Activo Base de Datos Proyectos de la Gobernación

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 01	Base de Datos proyectos de la Gobernación	D	Uso Interno	Normal	Alta	**Medio**	**3**

Fuente: La presente investigación

Para el caso de la Base de Datos proyectos de la Gobernación con nivel **Medio** y un porcentaje estimado de degradación de **25% - 89%,** puesto que al ser de tipo Dato/Información, las principales amenazas que recaen sobre esta clase de activos son errores del administrador y fugas de información; que afectarían medianamente a la secretaria de TIC, Innovación y Gobierno Abierto.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 2 equivalente a Menor, lo que quiere decir que en caso de materialización de amenaza(s), impacta menormente en la operatividad de los procesos en los que participa este activo de información:

Tabla 73 Estimación del Impacto Base de Datos Proyectos de la Gobernación

IMPACTO		Degradación		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Menor (2): Impacta en la operatividad del proceso.

A continuación, se realiza la estimación del impacto para el activo **Código fuente portal web Gobernación de Nariño, Portales**

Tabla 74 Activo Código Fuente Portal Web de la Gobernación de Nariño, Portales

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 02	Código fuente portal web de la Gobernación de Nariño, Portales	D	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

Fuente: La presente investigación

Para el caso del Código fuente portal web de la Gobernación de Nariño, Portales con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Dato/Información, las principales amenazas que recaen sobre esta clase de activos son errores del administrador, errores de configuración, fugas de información y manipulación de los registros de actividad que lo afectarían

considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 75 Estimación del Impacto Código Fuente Portal Web de la Gobernación de Nariño, Portales

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **Correo electrónico Institucional.**

Tabla 76 Activo Correo Electrónico Institucional

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 03	Correo electrónico institucional	S	Uso Interno	Sensible	Alta	**Alto**	**4**

Fuente: La presente investigación

Para el caso del Correo electrónico institucional con nivel **Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Servicios, las principales amenazas que recaen sobre esta clase de activos son errores de los usuarios, errores del administrador, errores de configuración, fugas de información, manipulación de los registros de actividad y repudio que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 5 equivalente a Mayor, lo que quiere decir que en caso de materialización de amenaza(s), impacta en la operatividad de los procesos en los que participa este activo de información:

Tabla 77 Estimación del Impacto Correo Electrónico Institucional

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Mayor (5): Impacta en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **Servicio técnico y de Software equipos de cómputo.**

Tabla 78 Activo Servicio Técnico y de Software Equipos de Computo

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 04	Servicio técnico y de software equipos de computo	S	Uso Interno	Normal	Alta	**Medio**	**3**

Fuente: La presente investigación

Para el caso del Servicio técnico y de software equipos de cómputo con nivel **Medio** y un porcentaje estimado de degradación de **25% - 89%,** puesto que al ser de tipo Servicios, la principal amenaza que recae sobre esta clase de activos son errores del administrador; que lo afectaría medianamente considerable o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 2 equivalente a Menor, lo que quiere decir que en caso de materialización de amenaza(s), impacta en la operatividad de los procesos en los que participa este activo de información:

Tabla 79 Estimación del Impacto Servicio Técnico y de Software Equipos de Computo

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	**2**	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Menor (2): Impacta en la operatividad del proceso.

A continuación, se realiza la estimación del impacto para el activo **Servicio de administración, desarrollo y soporte de sistemas de información y plataformas Gobernación de Nariño.**

Tabla 80 Activo Servicio de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas Gobernación de Nariño.

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC -05	Servicio de administración, desarrollo y soporte de sistemas de información y plataformas Gobernación de Nariño	S	Uso Interno	sensible	Alta	Alto	4

Fuente: La presente investigación

Para el caso del Servicio de administración, desarrollo y soporte de sistemas de información y plataformas gobernación de Nariño con nivel **Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Servicios, las principales amenazas que recaen sobre esta clase de activos son errores del administrador y fugas de información; que lo afectarían muy considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 5 equivalente a Mayor, lo que quiere decir que en caso de materialización de amenaza(s), impacta en la operatividad de los procesos en los que participa este activo de información:

Tabla 81 Estimación del Impacto Servicio de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas Gobernación de Nariño.

IMPACTO		Degradación		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	**5**
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Mayor (5): Impacta en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **Servicio de administración servidores, máquinas virtuales, dispositivos cisco y mikrotik Gobernación.**

Tabla 82 Activo Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 06	Servicio de administración servidores, máquinas virtuales, dispositivos cisco y mikrotik de la Gobernación	S	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

Fuente: La presente investigación

Para el caso del Servicio de administración servidores, máquinas virtuales, dispositivos cisco y mikrotik de la Gobernación con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Servicios, las principales amenazas que recaen sobre esta clase de activos son errores del administrador y fugas de información; que lo afectarían fuertemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 83 Estimación del Impacto Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **Software Sistema de backup en el servidor.**

Tabla 84 Activo Software Sistema de Backup en el Servidor

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 08	Software sistema de backup en el servidor	SW	confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

Fuente: La presente investigación

Para el caso del Software sistema de backup en el servidor con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Software, las principales amenazas que recaen sobre esta clase de activos son errores del administrador, Difusión de software dañino, fugas de información, vulnerabilidades de los programas, errores de mantenimiento/actualización de software, ataques intencionados como suplantación de la identidad del usuario, Difusión de software dañino, modificación deliberada de la información, y destrucción de información; que lo afectarían fuertemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 85 Estimación del Impacto Software Sistema de Backup en el Servidor

IMPACTO		Degradación		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **Software Portal web Gobernación de Nariño.**

Tabla 86 Activo Software Portal Web Gobernación de Nariño

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 09	Software Portal Web Gobernación de Nariño	SW	Uso público	Sensible	Alta	**Alto**	**4**

Fuente: La presente investigación

Para el caso del Software Portal Web Gobernación de Nariño con nivel **Alto** y un porcentaje estimado de degradación de **25% - 89%,** puesto que al ser de tipo Software, las principales amenazas que recaen sobre esta clase de activos son errores del administrador, Difusión de software dañino, fugas de información,

vulnerabilidades de los programas, errores de mantenimiento/actualización de software, ataques intencionados como suplantación de la identidad del usuario, Difusión de software dañino, modificación deliberada de la información, y destrucción de información; que lo afectarían fuertemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), impacta en la operatividad del macro proceso en el que participa este activo de información:

Tabla 87 Estimación del Impacto Software Portal web Gobernación de Nariño.

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Moderado (3): Impacta en la operatividad del macro proceso.

A continuación, se realiza la estimación del impacto para el activo **Software SYSMAN.**

Tabla 88 Activo Software SYSMAN

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 10	Software SYSMAN	SW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

Fuente: La presente investigación

Para el caso del Software SYSMAN con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Software, las principales amenazas que recaen sobre esta clase de activos son errores del administrador, Difusión de software dañino, fugas de información, vulnerabilidades de los programas, errores de mantenimiento/actualización de software, ataques intencionados como suplantación de la identidad del usuario, Difusión de software dañino, modificación deliberada de la información, y destrucción de información; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 89 Estimación del Impacto Software SYSMAN

IMPACTO		Degradación		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **Software SISCAR.**

Tabla 90 Activo Software SISCAR

ID	ACTIVO	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
			Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 11	Software SISCAR	SW	Confidencial	Sensible	Muy Alta	**Muy Alto**	5

Fuente: La presente investigación

Para el caso del Software SISCAR con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Software, las principales amenazas que recaen sobre esta clase de activos son errores del administrador, Difusión de software dañino, fugas de información, vulnerabilidades de los programas, errores de mantenimiento/actualización de software, ataques intencionados como suplantación de la identidad del usuario, Difusión de software

dañino, modificación deliberada de la información, y destrucción de información; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 91 Estimación del Impacto Software SISCAR

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **COMPUTADORES DE ESCRITORIO.**

Tabla 92 Activo Computadores de Escritorio

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 13	Computadores de Escritorio	10	HW	Uso Interno	Sensible	Alta	**Alto**	4

Fuente: La presente investigación

Para el caso de los Computadores de Escritorio con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores de fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), el impacto es moderado impacta levemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 93 Estimación del Impacto Computadores de Escritorio

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Moderado (3): Impacta en la operatividad del macro proceso.

A continuación, se realiza la estimación del impacto para el activo **COMPUTADORES PORTÁTILES.**

Tabla 94 Activo Computadores Portátiles

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 14	Computadores Portátiles	5	HW	Uso Interno	Sensible	Alta	**Alto**	4

Fuente: La presente investigación

Para el caso de los Computadores de Escritorio con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores de fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), el impacto es moderado impacta levemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 95 Estimación del Impacto Computadores Portátiles

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Moderado (3): Impacta en la operatividad del macro proceso.

A continuación, se realiza la estimación del impacto para el activo **IMPRESORAS.**

Tabla 96 Activo Impresoras

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 15	Impresoras	5	HW	Uso Interno	Normal	Media	**Medio**	3

Fuente: La presente investigación

Para el caso de Impresoras con nivel **Medio** y un porcentaje estimado de degradación de **1% a 24%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla X, el valor del impacto obtenido es 1 equivalente a Insignificante, lo que quiere decir que en caso de materialización de amenaza(s), impacta levemente en la operatividad de los procesos en los que participa este activo de información

Tabla 97 Estimación del Impacto Impresoras

IMPACTO		Degradación		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	**1**	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Insignificante (1): Impacta levemente en la operatividad del proceso

A continuación, se realiza la estimación del impacto para el activo **ESCÁNER.**

Tabla 98 Activo Escáner

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 16	Escáner		HW	Uso Interno	Normal	Media	**Medio**	3

Fuente: La presente investigación

Para el caso de Escáner con nivel **Bajo** y un porcentaje estimado de degradación de **1% a 24%:** puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla X, el valor del impacto obtenido es 1 equivalente a Menor, lo que quiere decir que en caso de materialización de amenaza(s), impacta levemente en la operatividad de los procesos en los que participa este activo de información.

Tabla 99 Estimación del Impacto Escáner

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Insignificante (1): Impacta levemente en la operatividad del proceso

A continuación, se realiza la estimación del impacto para el activo **RED INALÁMBRICA Y LOCAL.**

Tabla 100 Activo Red Inalámbrica y Local

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 17	Red inalámbrica y local		COM	Uso Interno	Normal	Media	**Medio**	3

Fuente: La presente investigación

Para el caso del Red inalámbrica y local con nivel **Medio** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo redes de comunicación, las principales amenazas que recaen sobre esta clase de activos son fallo del servicio de comunicación, errores del administrador, caída del sistema por agotamiento de recursos, corte del suministro eléctrico, condiciones inadecuadas de temperatura y humedad; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 2 equivalente a Menor, lo que quiere decir que en caso de materialización de amenaza(s), impacta menormente en la operatividad de los procesos en los que participa este activo de información:

Tabla 101 Estimación del Impacto Red Inalámbrica y Local

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	**2**	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Menor (2): Impacta en la operatividad del proceso.

A continuación, se realiza la estimación del impacto para el activo **UPS.**

Tabla 102 Activo UPS

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 18	UPS		AUX	Uso interno	Baja	Media Baja	**Bajo**	2

Fuente: La presente investigación

Para el caso de la UPS con nivel **Bajo** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Equipamiento Auxiliar, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, Errores de mantenimiento/actualización de equipos, Manipulación de los equipos.; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 1 equivalente a Menor, lo que quiere decir que en caso de materialización de amenaza(s), impacta levemente en la operatividad de los procesos en los que participa este activo de información.

Tabla 103 Estimación del Impacto UPS

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	**1**	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Insignificante (1): Impacta levemente en la operatividad del proceso

A continuación, se realiza la estimación del impacto para el activo **Sala de Comunicaciones.**

Tabla 104 Activo de Sala de Comunicaciones

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 19	Sala de Comunicaciones	1	L	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

Fuente: La presente investigación

Para el caso de la Sala de Comunicaciones con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Instalaciones, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, acceso no autorizado; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 105 Estimación del Impacto de la Sala de Comunicaciones

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **OFICINA SECRETARIA TIC, INNOVACIÓN Y GOBIERNO ABIERTO.**

Tabla 106 Activo Oficina Secretaria TIC, Innovación y Gobierno Abierto

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 20	Oficina Secretaria TIC, Innovación y Gobierno Abierto		L	Uso Interno	Sensible	Alta	**Alto**	4

Fuente: La presente investigación

Para el caso de la Sala de Comunicaciones con nivel **Alto** y un porcentaje estimado de degradación de **90% - 100%,** puesto que al ser de tipo Instalaciones, las

principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, acceso no autorizado; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 5 equivalente a Mayor, lo que quiere decir que en caso de materialización de amenaza(s), impacta mayormente en la operatividad de los procesos en los que participa este activo de información:

Tabla 107 Estimación del Impacto Oficina Secretaria TIC, Innovación y Gobierno Abierto

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Mayor (5): Impacta en la operatividad de los procesos.

A continuación, se realiza la estimación del impacto para el activo **PERSONAL TIC.**

Tabla 108 Activo Personal TIC

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACIÓN INFORMACIÓN			VALORACIÓN DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
STIC - 21	Personal TIC		P	Uso Interno	Normal	Muy Alta	**Alto**	4

Fuente: La presente investigación

Para el caso del Personal TIC con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Personal, las principales amenazas que recaen sobre esta clase de activos son fugas de información, extorción, ingeniería social; que lo afectarían considerablemente o afectarían a la secretaria de TIC, Innovación y Gobierno Abierto considerablemente.

Al realizar el producto de ambos datos en la tabla, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), el impacto es moderado impacta levemente en la operatividad de los procesos en los que participa este activo de información:

Tabla 109 Estimación del Impacto Personal TIC

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: La presente investigación

Moderado (3): Impacta en la operatividad del macro proceso.

ESTIMACIÓN DE LA PROBABILIDAD

A continuación, se realiza el impacto y la frecuencia de materialización de cada una de las amenazas sobre los principales activos de la Gobernación

Tabla 110 Impacto y Frecuencia Base de Datos Proyectos de la Gobernación

Activo STIC-01	**STIC-01 Base de Datos Proyectos de la Gobernación**	

Administrador					
Degradación	**50%**				
Impacto	**2**	**Menor**			
Tipo activo	**Datos/Información**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del Administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información para el manejo del activo.	Baja	3
	E19	Fugas de Información.	La entidad no capacita a los funcionarios sobre la seguridad de la información. Falta de políticas de confidencialidad de información.	Baja	3
Ataques Intencionados	A15	Modificación Deliberada de la información	Carencia de políticas de seguridad de uso de soportes de información externos.	Baja	3

Fuente: La presente investigación

Tabla 111 Impacto y Frecuencia Código Fuente Portal Web Gobernación de Nariño, Portales.

Activo STIC-02	**STIC-02 Código fuente portal web Gobernación de Nariño, Portales**				
Administrador					
Degradación	**100%**				
Impacto	**8**	**Desastroso**			
Tipo activo	**Datos/Información**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	El antivirus no se actualiza diariamente. El administrador no cuenta con capacitación respecto a la seguridad de la información para el manejo del activo.	Media	4
	E4	Errores de configuración	No cuenta con una protección segura para ataques al sitio web.	Media	4
	E19	Fugas de información	Los datos no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Media	4
Ataques Intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Muy Baja	2

Fuente: La presente investigación

Tabla 112 Impacto y Frecuencia Correo Electrónico Institucional.

Activo STIC-03	**STIC-03 Correo Electrónico Institucional**				
Administrador					
Degradación	**100%**				
Impacto	**5**	**Mayor**			
Tipo activo	**Servicio**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E1	Errores de los usuarios	El usuario no cuenta con capacitación respecto a la seguridad de la información.	Baja	3
	E2	Errores del administrador	No existe un análisis de seguridad para los correos spam.	Media	4
	E4	Errores de configuración	No cuenta con una protección segura para ataques al sitio web.	Media	4
	E19	Fugas de información	Los datos no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Baja	3
Ataques Intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Baja	3
	A13	Repudio	Carencia de mecanismos que controlen el envío y recepción de mensajes.	Baja	3

Fuente: La presente investigación

Tabla 113 Impacto y Frecuencia Servicio Técnico y de Software Equipos de Cómputo

Activo STIC-04	**STIC-04 Servicio Técnico y de Software equipos de cómputo.**				
Administrador					
Degradación	**50%**				
Impacto	**2**	**Menor**			
Tipo activo	**Servicio**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información. Falta de planilla de registro para los equipos.	Baja	3

Fuente: La presente investigación

Tabla 114 Impacto y Frecuencia de Servicios de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas de la Gobernación.

Activo STIC-05	**STIC-05 Servicios de administración, Desarrollo y Soporte de sistemas de información y Plataformas de la Gobernación.**				
Administrador					
Degradación	**100%**				
Impacto	**5**	**Mayor**			
Tipo activo	**Servicio**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información.	Baja	3
	E19	Fugas de información	Los datos de los soportes de información y plataformas no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Baja	3

Fuente: La presente investigación

Tabla 115 Impacto y Frecuencia de Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.

Activo STIC-06	**STIC-06 Servicio de Administración Servidores, Máquinas Virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.**				
Administrador					
Degradación	**100%**				
Impacto	**8**	**Desastroso**			
Tipo activo	**Servicio**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información.	Baja	3
	E19	Fugas de información	Los datos de los servidores no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Baja	3

Fuente: La presente investigación

Tabla 116 Impacto y Frecuencia Sistema de Backup en el Servidor

Activo STIC-08	**STIC-08 Sistema de Backup en el servidor.**				
Administrador					
Degradación	**100%**				
Impacto	**8**	**Desastroso**			
Tipo activo	**Software**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.	Baja	3

Tabla 116 (Continuación)

Activo STIC-08	**STIC-08 Sistema de Backup en el servidor.**				
Degradación	**100 %**				
Impacto	**8**	**Desastroso**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.	Media	4
	E19	Fugas de información	Los datos de los sistemas de información no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.	Media	4
	E21	Errores de Mantenimiento/actualización Software	Software no Licenciado Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Baja	3

Tabla 116 (Continuación)

Tipo activo		Software			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Ataques Intencionados	A5	Suplantación de la identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Muy Baja	2
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del sistema, para prevenir ataques informáticos.	Baja	3
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del sistema, para prevenir ataques informáticos.	Baja	3

Fuente: La presente investigación

Tabla 117 Impacto y Frecuencia Software Portal Web Gobernación de Nariño

Activo STIC-09	**STIC-09 Software Portal Web Gobernación de Nariño.**				
Administrador					
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Software**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.	Baja	3
		Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.	Media	4
	E19	Fugas de información	Los datos de los sistemas de información no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.	Media	4
	E21	Errores de Mantenimiento/actualización Software	Software no Licenciado Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Baja	3

Tabla 117(Continuación)

Activo STIC-09	**STIC-09 Software Portal Web Gobernación de Nariño.**				
Administrador					
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Software**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Ataques Intencionados	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3

Fuente: La presente investigación

Tabla 118 Impacto y Frecuencia Software SYSMAN.

Activo STIC-10	**STIC-10 Software SYSMAN.**				
Administrador					
Degradación	**100%**				
Impacto	**8**	**Desastroso**			
Tipo activo	**Software**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Seguridad de la Información. No se realiza capacitaciones para el manejo del software. No se realizan auditorias para verificar la calidad y el funcionamiento del software. No se realiza soporte inmediato frente a fallas del software.	Media	4
	E8	Difusión de Software Dañino.	Hay poca capacitación para los empleados que utilizan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb.	Baja	3
	E19	Fugas de información	La entidad no capacita a los empleados que utilizan software sobre la seguridad de la información.	Baja	3
	E20	Vulnerabilidades de los Programas(Software)	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento. Falta de Políticas de uso de aplicaciones e información.	Baja	3
	E21	Errores de Mantenimiento/actualización Software	Falta de planes de actualización de software. Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Media	4

Tabla 118 (Continuación)

Activo STIC-10	**STIC-10 Software SYSMAN.**		
Administrador			
Degradación	**100%**		
Impacto	**8**	**Desastroso**	
Tipo activo	**Software**		

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)	
Ataques Intencionados	A5	Suplantación de la Identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Muy Baja	2
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.	Baja	3
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.	Baja	3

Fuente: La presente investigación

Tabla 119 Impacto y Frecuencia Software SISCAR.

Activo STIC-11	**STIC-11 Software SISCAR.**				
Administrador					
Degradación	**100%**				
Impacto	**8**	**Desastroso**			
Tipo activo	**Software**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Seguridad de la Información. No se realizan auditorias para verificar la calidad y el funcionamiento del software.	Baja	3
	E8	Difusión de Software Dañino.	Hay poca capacitación para los empleados que utilizan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb.	Baja	3
	E19	Fugas de información	La entidad no capacita a los empleados que utilizan software sobre la seguridad de la información.	Baja	3
	E20	Vulnerabilidades de los Programas(Software)	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento. Falta de Políticas de uso de aplicaciones e información.	Baja	3
	E21	Errores de Mantenimiento/actualización Software	Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Media	4

Tabla 119 (Continuación)

Tipo Activo	**Software**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Ataques Intencionados	A5	Suplantación de la Identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Muy Baja	2
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.	Baja	3
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software para prevenir ataques informáticos.	Baja	3

Fuente: La presente investigación

Tabla 120 Impacto y Frecuencia Computadores de Escritorio

Activo STIC-13	**STIC-13 Computadores de Escritorio**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Baja	3
	N2	Daños por agua	Los computadores de escritorio se encuentran ubicados sin ninguna precaución.	Bajo	3
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Baja	3
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Baja	3
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3
	I3	Contaminación Mecanica	Consumir alimentos a lado de los equipos.	Baja	3
	I5	Avería de Origen Físico o Lógico	Defectos de fábrica de los equipos.	Muy Baja	2
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Espacio ilimitado entre los equipos de escritorio No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3

Tabla 120 (Continuación)

Activo STIC-13	**STIC-13 Computadores de Escritorio**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del Administrador	Sobrecarga de trabajo No existe un protocolo para la instalación de las diferentes aplicaciones.	Baja	3
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los equipos. Falta de controles o Políticas de mantenimiento preventivo y periódico a los computadores de escritorio.	Baja	3
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3
	A11	Acceso no autorizado	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios.	Baja	3
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Baja	3

Fuente: La presente investigación

Tabla 121 Impacto y Frecuencia Computadores Portátiles

Activo STIC-14	**STIC-14 Computadores Portátiles**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Baja	3
	N2	Daños por agua	Los computadores de escritorio se encuentran ubicados sin ninguna precaución.	Bajo	3
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Baja	3
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Baja	3
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3
	I3	Contaminación Mecanica	Consumir alimentos a lado de los equipos.	Baja	3
	I5	Avería de Origen Físico o Lógico	Defectos de fábrica de los equipos.	Muy Baja	2
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Espacio ilimitado entre los equipos de escritorio No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3

Tabla 121 (Continuación)

Activo STIC-14	**STIC-14 Computadores Portátiles**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E2	Errores del Administrador	Sobrecarga de trabajo No existe un protocolo para la instalación de las diferentes aplicaciones.	Baja	3
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los equipos. Falta de controles o Políticas de mantenimiento preventivo y periódico a los computadores de escritorio.	Baja	3
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3
	A11	Acceso no autorizado	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios.	Baja	3
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Baja	3

Fuente: La presente investigación

Tabla 122 Impacto y Frecuencia Impresoras

Activo STIC-15	**STIC-15 Impresoras**				
Administrador	**Soporte Técnico**				
Degradación	**1%**				
Impacto	**1**	**Insignificante**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Muy baja	2
	N2	Daños por agua	Las impresoras se encuentran ubicadas sin ninguna precaución.	Raro	1
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Muy baja	2
	I*	Desastres Industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2
	I5	Avería de Origen Físico o Lógico	Mala ubicación de las impresoras.	Media	4
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3
Errores y fallos	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para las impresoras Falta de controles o Políticas de mantenimiento preventivo y periódico a las impresoras.	Baja	3

Tabla 122 (Continuación)

Activo STIC-15	**STIC-15 Impresoras**				
Administrador	**Soporte Técnico**				
Degradación	**1%**				
Impacto	**1**	**Insignificante**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3

Fuente: La presente investigación

Tabla 123 Impacto y Frecuencia Escáner

Activo STIC-16	**STIC-16 Escáner**				
Administrador	**Soporte Técnico**				
Degradación	**1%**				
Impacto	**1**	**Insignificante**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Muy baja	2
	N2	Daños por agua	Las impresoras se encuentran ubicadas sin ninguna precaución.	Raro	1
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Muy baja	2
	I*	Desastres Industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2
	I5	Avería de Origen Físico o Lógico	Mala ubicación de los escáneres.	Baja	3
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3
Errores y fallos	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para las impresoras Falta de controles o Políticas de mantenimiento preventivo y periódico a las impresoras.	Baja	3

Tabla 123 (Continuación)

Activo STIC-16	**STIC-16 Escáner**				
Administrador	**Soporte Técnico**				
Degradación	**1%**				
Impacto	**1**	**Insignificante**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3
Ataques intencionados	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3

Fuente: La presente investigación

Tabla 124 Impacto y Frecuencia Red Inalámbrica y Local

Activo STIC-17	**STIC-17 Red Inalámbrica y Local**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**2**	**Menor**			
Tipo activo	**Comunicaciones**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
De origen industrial	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3
	I8	Fallo de servicios de comunicaciones	Desconexión de un cable de red. Dispositivos de comunicación quemados Dispositivos de comunicación mal configurados.	Baja	3
Errores y Fallos	E9	Errores de [RE-] Encaminamiento	Falta de Privilegios de acceso a las redes.	Muy baja	2
Ataques intencionados	A5	Suplantación de la Identidad del Usuario.	Falta de Privilegios de acceso a las redes.	Muy baja	2

Fuente: La presente investigación

Tabla 125 Impacto y Frecuencia UPS

Activo STIC-18	**STIC-18 UPS**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**1**	**Insignificante**			
Tipo activo	**Auxiliar**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Muy baja	2
	I3	Contaminación Mecánica	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad.	Baja	3
	I5	Avería de Origen físico o lógico.	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad. Falta de controles físico y lógicos como el mantenimiento preventivo de hardware.	Baja	3

Tabla 125 (Continuación)

Activo STIC-18	**STIC-18 UPS**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**1**	**Insignificante**			
Tipo activo	**Auxiliar**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja	3
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de las UPS Falta de controles de mantenimiento preventivo y periódico a las UPS. Falta de plan de Gestión y control de recursos vs requerimientos.	Baja	3
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3
	A23	Manipulación de los equipos.	Falta de controles para el ingreso a la sala de comunicaciones.	Baja	3

Fuente: La presente investigación

Tabla 126 Impacto y Frecuencia Sala de Comunicaciones

Activo STIC-19	**STIC-19 Sala de Comunicaciones**			
Administrador	**Soporte Técnico**			
Degradación	**100%**			
Impacto	**8**	**Desastroso**		
Tipo activo	**Instalaciones**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Baja	3
Ataques intencionados	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Media	4

Fuente: La presente investigación

Tabla 127 Impacto y Frecuencia Secretaría TIC, Innovación y Gobierno Abierto

Activo STIC-20		**STIC-20 Secretaría TIC, Innovación y Gobierno Abierto**			
Administrador		**Soporte Técnico**			
Degradación		**100%**			
Impacto		**5**	**Mayor**		
Tipo activo		**Instalaciones**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2
De origen industrial	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Baja	3
Ataques	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3

Fuente: La presente investigación

Tabla 128 Impacto y Frecuencia Personal TIC

Activo STIC-21	**STIC-21 Personal TIC**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Personal**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y Fallos	E7	Deficiencias en la Organización,	Falta de capacitación sobre seguridad de la Información. Falta me mecanismos de monitoreo de personal Falta de políticas de uso correcto de telecomunicaciones. Falta de políticas de contratación.	Baja	3
	E19	Fugas de Información	Falta de capacitación sobre seguridad de la Información.	Baja	3
	E28	Indisponibilidad del Personal	Falta de un plan de contingencia en caso de ausencia	Muy baja	2
Ataques Intencionados	A28	Indisponibilidad del Personal	Falta de un plan de contingencia en caso de ausencia	Muy baja	2
	A29	Extorsión	Falta de Políticas que definan un procedimiento a seguir ante vulnerabilidades de este tipo.	Baja	3
	A30	Ingeniería Social	Falta de capacitación sobre seguridad de la Información. Falta de concientización del personal en las mejores prácticas de seguridad informática.	Baja	3

Fuente: La presente investigación

ESTIMACIÓN DEL RIESGO

A continuación, se realiza la estimación del riesgo para cada uno de los principales activos de la Secretaría de TIC.

Tabla 129 Estimación del Riesgo Base de Datos Proyectos de la Gobernación.

Activo STIC-01		**STIC-01 Base de Datos Proyectos de la Gobernación**							
Administrador									
Degradación		**50%**							
Impacto		**2**	**Menor**						
Tipo activo		**Datos/Información**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							2	Tolerable	
				Frecuencia (F)		R		NR	
Errores y Fallos	E2	Errores del Administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información para el manejo del activo.	Baja	3	6	2	Tolerable	
	E19	Fugas de Información.	La entidad no capacita a los funcionarios sobre la seguridad de la información. Falta de políticas de confidencialidad de información.	Baja	3	6	2	Tolerable	
Ataques Intencionados	A15	Modificación Deliberada de la información	Carencia de políticas de seguridad de uso de soportes de información externos.	Baja	3	6	2	Tolerable	

Fuente: La presente investigación

Tabla 130 Estimación del Riesgo Código Fuente Portal Web Gobernación de Nariño, Portales.

Activo STIC-02	**STIC-02 Código fuente portal web Gobernación de Nariño, Portales.**

Administrador									
Degradación		**100%**							
Impacto		**3**	**Moderado**						
Tipo activo		**Datos/Información**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
								4	Extremo
				Frecuencia (F)		**R**		**NR**	
Errores y Fallos	E2	Errores del administrador	El antivirus no se actualiza diariamente. Los funcionarios no tienen conocimiento sobre la seguridad de la información.	Media	4	32	4	extremo	
	E4	Errores de configuración	No cuenta con una protección segura para ataques al sitio web.	Media	4	32	4	extremo	
	E19	Fugas de información	Los datos no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Media	4	32	4	extremo	
Ataques Intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Muy Baja	2	16	4	extremo	

Fuente: La presente investigación

Tabla 131 Estimación del Riesgo Correo Electrónico Institucional.

Activo STIC-03	**STIC-03 Correo Electrónico Institucional**	

Administrador								
Degradación		**100%**						
Impacto		**5**	**Mayor**					
Tipo activo		**Servicio**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**		**NR**
Errores y Fallos	E1	Errores de los usuarios	El usuario no cuenta con capacitación respecto a la seguridad de la información.	Baja	3	15	4	extremo
	E2	Errores del administrador	No existe un análisis de seguridad para los correos spam.	Media	4	20	4	extremo
	E4	Errores de configuración	No cuenta con una protección segura para ataques al sitio web.	Media	4	20	4	extremo
	E19	Fugas de información	Los datos no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Baja	3	15	4	extremo
Ataques Intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Baja	3	24	4	extremo
	A13	Repudio	Carencia de mecanismos que controlen el envío y recepción de mensajes.	Baja	3	15	4	extremo

Fuente: La presente investigación

Tabla 132 Estimación del Riesgo Servicio Técnico y de Software Equipos de Cómputo

Activo STIC-04	**STIC-04 Servicio Técnico y de Software equipos de Cómputo**

Administrador									
Degradación	**50%**								
Impacto	**2**	**Menor**							
Tipo activo	**Datos/Información**								
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
				Frecuencia (F)		**R**	2	**NR**	
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información. Falta de planilla de registro para los equipos.	Baja	3	6	2	Tolerable	

Fuente: La presente investigación

Tabla 133 Estimación del Riesgo Servicios de Administración, Desarrollo y Soporte de Sistemas de Información y Plataformas de la Gobernación.

Activo STIC-05	**STIC-05 Servicios de Administración, Desarrollo y Soporte de sistemas de información y plataformas de la Gobernación.**								
Degradación	**100%**								
Impacto	**5**	**Mayor**							
Tipo activo	**Datos/Información**								
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
						4	extremo		
				Frecuencia (F)		**R**	**NR**		
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información	Media	4	20	4	extremo	
	E19	Fugas de información	Los datos de los soportes de información y plataformas no son correctamente protegidos.	Baja	3	15	4	extremo	

Fuente: La presente investigación

Tabla 134 Estimación del Riesgo Servicios de Administración Servidores, Máquinas virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.

Activo STIC-06	**STIC-06 Servicios de Administración servidores, Máquinas virtuales, Dispositivos Cisco y Mikrotik de la Gobernación.**
Administrador	

Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Servicios**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
				Frecuencia (F)		**R**	4 **NR**	
Errores y Fallos	E2	Errores del administrador	El administrador no cuenta con capacitación respecto a la seguridad de la información	Baja	3	24	4	extremo
	E19	Fugas de información	Los datos de los servidores no son correctamente protegidos. La entidad no capacita a los funcionarios sobre la seguridad de la información.	Baja	3	24	4	extremo

Tabla 135 Estimación del Riesgo Software Sistema de Backup en el Servidor

Activo STIC-08	**STIC-08 Software Sistema de Backup en el servidor**
Administrador	

Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Software**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**		**NR**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.	Baja	3	24	4	extremo
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.	Media	4	32	4	extremo
	E19	Fugas de información	Los datos de los sistemas de información no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3	24	4	extremo
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.	Media	4	32	4	extremo

Tabla 135 (Continuación)

Activo STIC-08	**STIC-08 Software Sistema de Backup en el servidor**
Administrador	

Degradación		**100%**						
Impacto		**8**	**Desastroso**					
Tipo activo		**Software**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		R		NR
Ataques Intencionados	A5	Suplantación de la identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Muy Baja	2	16	4	extremo
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3	24	4	extremo
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3	24	4	extremo
	A18	Destrucción de información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3	24	4	extremo

Fuente: La presente investigación

Tabla 136 Estimación del Riesgo Software Portal Web Gobernación de Nariño.

Activo STIC-09	**STIC-09 Software Portal web Gobernación de Nariño.**
Administrador	

Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Software**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							3	Intolerable
				Frecuencia (F)		**R**		**NR**
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información.	Baja	3	9	3	Intolerable
	E8	Difusión de Software Dañino.	Uso de Software No Licenciado en la Entidad. Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb. No se descargan los parches de seguridad con regularidad.	Media	4	12	3	Intolerable
	E19	Fugas de información	Los datos de los sistemas de información no son correctamente protegidos. La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3	9	3	Intolerable
	E20	Vulnerabilidades de los Programas(Software)	Falta de claves criptográficas No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento.	Media	4	12	3	Intolerable
	E21	Errores de Mantenimiento/actualización Software	Falta de planes de actualización Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Media	4	12	3	Intolerable

Tabla 136 (Continuación)

Activo STIC-09	**STIC-09 Software Portal web Gobernación de Nariño.**

Administrador									
Degradación	**50%**								
Impacto	**3**	**Moderado**							
Tipo activo	**Software**								
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
				Frecuencia (F)		**R**		**NR**	
							3	Intolerable	
Ataques Intencionados	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3	9	3	Intolerable	
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3	9	3	Intolerable	
	A18	Destrucción de información.	Falta de Controles de seguridad dentro de la plataforma web, para prevenir ataques informáticos.	Baja	3	9	3	Intolerable	

Fuente: La presente investigación

Tabla 137 Estimación del Riesgo Software SYSMAN.

Activo STIC-10	**STIC-10 Software SYSMAN**	

Administrador										
Degradación	**100%**									
Impacto	**8**	**Desastroso**								
Tipo activo	**Software**									

Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
				Frecuencia (F)	R	4	Extremo	NR
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Seguridad de la Información. No se realiza capacitaciones para el manejo del software. No se realizan auditorias para verificar la calidad y el funcionamiento del software. No se realiza soporte inmediato frente a fallas del software	Media	4	32	4	extremo
	E8	Difusión de Software Dañino.	Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb.	Baja	3	24	4	extremo
	E19	Fugas de información	La entidad no capacita a los empleados que utilizan software sobre la seguridad de la información.	Baja	3	24	4	extremo
	E20	Vulnerabilidades de los Programas(Software)	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento. Falta de Políticas de uso de aplicaciones e información.	Baja	3	24	4	extremo
	E21	Errores de Mantenimiento/actualización Software	Falta de planes de actualización de software. Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Media	4	32	4	extremo

Tabla 137 (Continuación)

Activo STIC-10	**STIC-10 Software SYSMAN**
Administrador	

Degradación	**100%**									
Impacto	**8**	**Desastroso**								
Tipo activo	**Software**									
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**						
						4	Extremo			
				Frecuencia (F)	R	NR				
Ataques Intencionados	A5	Suplantación de la Identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	24	4	extremo		
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3	24	4	extremo		
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3	24	4	extremo		
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3	24	4	extremo		

Fuente: La presente investigación

Tabla 138 Estimación del Riesgo Software SISCAR.

Activo STIC-11	**STIC-11 Software SISCAR.**	
Administrador		

Degradación		**100%**						
Impacto		**8**	**Desastroso**					
Tipo activo		**Software**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
				Frecuencia (F)		R		NR
							4	extremo
Errores y Fallos	E2	Errores del administrador	Falta de Políticas de Confidencialidad de la Información. No se realizan auditorias para verificar la calidad y el funcionamiento del software.	Baja	3	24	4	extremo
	E8	Difusión de Software Dañino.	Hay poca capacitación para los empleados que manejan software de la organización. El antivirus no se actualiza diariamente. Falta de restricción de puertos usb.	Baja	3	24	4	extremo
	E19	Fugas de información	La entidad no capacita a los empleados que desarrollan software sobre la seguridad de la información.	Baja	3	24	4	extremo
	E20	Vulnerabilidades de los Programas(Software)	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento. Falta de Políticas de uso de aplicaciones e información.	Baja	3	24	4	extremo
	E21	Errores de Mantenimiento/actualización Software	Falta de documentación cuando hay cambio o actualización en los sistemas de información en producción.	Media	4	32	4	extremo

Tabla 138 (Continuación)

Activo STIC-11	**STIC-11 Software SISCAR.**

Administrador										
Degradación		**100%**								
Impacto		**8**	**Desastroso**							
Tipo activo		**Software**								
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**						
				Frecuencia (F)		**R**		**NR**		
							4	extremo		
Ataques Intencionados	A5	Suplantación de la Identidad del Usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	24	4	extremo		
	A8	Difusión de Software dañino	No existe un procedimiento para la actualización de software. Falta de Políticas de protección a los equipos.	Baja	3	24	4	extremo		
	A15	Modificación deliberada de la información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3	24	4	extremo		
	A18	Destrucción de información.	Falta de Controles de seguridad dentro del software, para prevenir ataques informáticos.	Baja	3	24	4	extremo		

Fuente: La presente investigación

Tabla 139 Estimación del Riesgo Computadores de Escritorio

Activo STIC-13		**STIC-13 Computadores de Escritorio**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							2.9	Intolerable
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Baja	3	9	3	Intolerable
	N2	Daños por agua	Los computadores de escritorio se encuentran ubicados sin ninguna precaución.	Baja	3	9	3	Intolerable
Ataques Intencionados	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Baja	3	9	3	Intolerable
	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Baja	3	9	3	Intolerable
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable
	I3	Contaminación Mecanica	Consumir alimentos a lado de los equipos.	Baja	3	9	3	Intolerable

Tabla 139 (Continuación)

Activo STIC-13	**STIC-13 Computadores de Escritorio**							
Administrador	**Soporte Técnico**							
Degradación	**50%**							
Impacto	**3**	**Moderado**						
Tipo activo	**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							2.9	Intolerable
				Frecuencia (F)		**R**	**NR**	
	I5	Avería de Origen Físico o Lógico	Defectos de fábrica de los equipos.	Muy Baja	2	6	2	Tolerable
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3	9	3	Intolerable
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Espacio ilimitado entre los equipos de escritorio No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3	9	3	Intolerable
	E2	Errores del Administrador	Sobrecarga de trabajo No existe un protocolo para la instalación de las diferentes aplicaciones.	Baja	3	9	3	Intolerable
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los equipos. Falta de controles o Políticas de mantenimiento preventivo y periódico a los computadores de escritorio.	Baja	3	9	3	Intolerable
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3	9	3	Intolerable
	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3	9	3	Intolerable

Tabla 139 (Continuación)

Activo STIC-13		**STIC-13 Computadores de Escritorio**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							2.9	Intolerable
				Frecuencia (F)		**R**	**NR**	
	A11	Acceso no autorizado	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios.	Baja	3	9	3	Intolerable
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Baja	3	9	3	Intolerable

Fuente: La presente investigación

Tabla 140 Estimación del Riesgo Computadores Portátiles

Activo STIC-14		**STIC-14 Computadores Portátiles**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							2.9	Intolerable
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Baja	3	9	3	Intolerable

Tabla 140 (Continuación)

Activo STIC-14		**STIC-14 Computadores Portátiles**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							2.9	Intolerable
				Frecuencia (F)		**R**	**NR**	
	N2	Daños por agua	Los computadores de escritorio se encuentran ubicados sin ninguna precaución.	Baja	3	9	3	Intolerable
Ataques Intencionados	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Baja	3	9	3	Intolerable
	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Baja	3	9	3	Intolerable
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable
	I3	Contaminación Mecánica	Consumir alimentos a lado de los equipos.	Baja	3	9	3	Intolerable
	I5	Avería de Origen Físico o Lógico	Defectos de fábrica de los equipos.	Muy Baja	2	6	2	Tolerable

Tabla 140 (Continuación)

Activo STIC-14		**STIC-14 Computadores Portátiles**							
Administrador		**Soporte Técnico**							
Degradación		**50%**							
Impacto		**3**	**Moderado**						
Tipo activo		**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							2.9	Intolerable	
				Frecuencia (F)		**R**	**NR**		
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3	9	3	Intolerable	
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. Espacio ilimitado entre los equipos de escritorio No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3	9	3	Intolerable	
	E2	Errores del Administrador	Sobrecarga de trabajo No existe un protocolo para la instalación de las diferentes aplicaciones.	Baja	3	9	3	Intolerable	
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para los equipos. Falta de controles o Políticas de mantenimiento preventivo y periódico a los computadores de escritorio.	Baja	3	9	3	Intolerable	
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3	9	3	Intolerable	
	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3	9	3	Intolerable	

Tabla 140 (Continuación)

Activo STIC-14		**STIC-14 Computadores Portátiles**							
Administrador		**Soporte Técnico**							
Degradación		**50%**							
Impacto		**3**	**Moderado**						
Tipo activo		**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							2.9	Intolerable	
				Frecuencia (F)		**R**	**NR**		
	A11	Acceso no autorizado	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios.	Baja	3	9	3	Intolerable	
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de control de acceso a la sala de comunicaciones. Falta de personal suficiente para vigilancia interna.	Baja	3	9	3	Intolerable	

Fuente: La presente investigación

Tabla 141 Estimación del Riesgo Impresoras

Activo STIC-15		**STIC-15 Impresoras**							
Administrador		**Soporte Técnico**							
Degradación		**1%**							
Impacto		**1**	**Insignificante**						
Tipo activo		**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							1.6	Tolerable	
				Frecuencia (F)		**R**	**NR**		
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Muy baja	2	2	1	Aceptable	

Tabla 141 (Continuación)

Activo STIC-15	**STIC-15 Impresoras**		
Administrador	**Soporte Técnico**		
Degradación	**1%**		
Impacto	**1**	**Insignificante**	
Tipo activo	**Hardware**		

Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							1.6	Tolerable
				Frecuencia (F)		**R**	**NR**	
	N2	Daños por agua	Las impresoras se encuentran ubicadas sin ninguna precaución.	Raro	1	1	1	Aceptable
Ataques Intencionados	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	2	1	Aceptable
	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Muy baja	2	2	1	Aceptable
	I*	Desastres Industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2	2	1	Aceptable
	I5	Avería de Origen Físico o Lógico	Mala ubicación de las impresoras.	Media	4	4	2	Tolerable
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3	3	2	Tolerable

Tabla 141 (Continuación)

Activo STIC-15		**STIC-15 Impresoras**						
Administrador		**Soporte Técnico**						
Degradación		**1%**						
Impacto		**1**	**Insignificante**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							1.6	Tolerable
				Frecuencia (F)		**R**	**NR**	
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3	3	2	Tolerable
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para las impresoras Falta de controles o Políticas de mantenimiento preventivo y periódico a las impresoras.	Baja	3	3	2	Tolerable
	E24	Caída del sistema por agotamiento de recursos.	Falta de papel para impresoras tinta y el tóner.	Baja	3	3	2	Tolerable
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3	3	2	Tolerable
	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3	3	2	Tolerable
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3	3	2	Tolerable

Fuente: La presente investigación

Tabla 142 Estimación del Riesgo Escáner

Activo STIC-16		**STIC-16 Escáner**						
Administrador		**Soporte Técnico**						
Degradación		**1%**						
Impacto		**1**	**Insignificante**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							1.6	Tolerable
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo	Muy baja	2	2	1	Aceptable
	N2	Daños por agua	Las impresoras se encuentran ubicadas sin ninguna precaución.	Raro	1	1	1	Aceptable
Ataques Intencionados	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	2	1	Aceptable
	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de alarmas de Humo.	Muy baja	2	2	1	Aceptable
	I*	Desastres Industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2	2	1	Aceptable
	I5	Avería de Origen Físico o Lógico	Mala ubicación de los escáneres.	Baja	3	3	2	Tolerable

Tabla 142 (Continuación)

Activo STIC-16		**STIC-16 Escáner**						
Administrador		**Soporte Técnico**						
Degradación		**1%**						
Impacto		**1**	**Insignificante**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							1.6	Tolerable
				Frecuencia (F)		**R**	**NR**	
	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3	3	2	Tolerable
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3	3	2	Tolerable
	E23	Errores de mantenimiento/actualización de equipos	No existen bitácoras de registro para las impresoras Falta de controles o Políticas de mantenimiento preventivo y periódico a las impresoras.	Baja	3	3	2	Tolerable
	E25	Pérdida de equipos/robo	No existen cámaras de seguridad en la oficina de Secretaria de TIC, innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3	3	2	Tolerable
	A7	Uso no previsto	Falta de mecanismos de monitoreo del personal	Baja	3	3	2	Tolerable
	A25	Robo	No existen cámaras de seguridad en la secretaria de TIC, Innovación y Gobierno Abierto. Falta de personal suficiente para vigilancia interna.	Baja	3	3	2	Tolerable

Fuente: La presente investigación

Tabla 143 Estimación del Riesgo Red Inalámbrica y Local

Activo STIC-17		**STIC-17 Red Inalámbrica y Local**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**2**	**Menor**					
Tipo activo		**Comunicaciones**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							2	Tolerable
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	I6	Corte del suministro eléctrico	Funcionamiento no confiable de las UPS	Baja	3	6	2	Tolerable
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad. No cuentan con aire acondicionado en la oficina de Secretaria de TIC, Innovación y Gobierno abierto.	Baja	3	6	2	Tolerable
Ataques Intencionados	I8	Fallo de servicios de comunicaciones	Desconexión de un cable de red. Dispositivos de comunicación quemados Dispositivos de comunicación mal configurados.	Baja	3	6	2	Tolerable
	E9	Errores de [RE-] Encaminamiento	Falta de Privilegios de acceso a las redes.	Muy baja	2	4	2	Tolerable
	A5	Suplantación de la Identidad del Usuario.	Falta de Privilegios de acceso a las redes.	Muy baja	2	4	2	Tolerable

Fuente: La presente investigación

Tabla 144 Estimación del Riesgo UPS

Activo STIC-18		**STIC-18 UPS**							
Administrador		**Soporte Técnico**							
Degradación		**50%**							
Impacto		**1**	**Insignificante**						
Tipo activo		**Auxiliar**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							1.6	Tolerable	
				Frecuencia (F)		R	NR		
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2	2	1	Aceptable	
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	1	1	Aceptable	
Ataques Intencionados	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2	2	1	Aceptable	
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal. Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones.	Muy baja	2	2	1	Aceptable	

Tabla 144 (Continuación)

Activo STIC-18	**STIC-18 UPS**		
Administrador	**Soporte Técnico**		
Degradación	**50%**		
Impacto	**1**	**Insignificante**	
Tipo activo	**Auxiliar**		

Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							1.6	Tolerable
				Frecuencia (F)		**R**	**NR**	
	I3	Contaminación Mecánica	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad.	Baja	3	3	2	Tolerable
	I5	Avería de Origen físico o lógico.	En la sala de comunicaciones se realiza con poca frecuencia una limpieza para el polvo y/o suciedad. Falta de controles físico y lógicos como el mantenimiento preventivo de hardware.	Baja	3	3	2	Tolerable
	I7	Condiciones Inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja	3	3	2	Tolerable
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida de las UPS Falta de controles de mantenimiento preventivo y periódico a las UPS. Falta de plan de Gestión y control de recursos vs requerimientos.	Baja	3	3	2	Tolerable
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3	3	2	Tolerable
	A23	Manipulación de los equipos.	Falta de controles para el ingreso a la sala de comunicaciones.	Baja	3	3	2	Tolerable

Fuente: La presente investigación

Tabla 145 Estimación del Riesgo Sala de Comunicaciones

Activo STIC-19	**STIC-19 Sala de Comunicaciones**							
Administrador	**Soporte Técnico**							
Degradació	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Instalaciones**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2	16	4	Extremo
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	16	4	Extremo
Ataques Intencionados	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2	16	4	Extremo
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Baja	3	24	4	Extremo

Tabla 145 (Continuación)

Activo STIC-19	**STIC-19 Sala de Comunicaciones**							
Administrador	**Soporte Técnico**							
Degradación	**100%**							
Impacto	**8**	**Desastroso**						
Tipo activo	**Instalaciones**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Media	4	32	4	Extremo

Fuente: La presente investigación

Tabla 146 Estimación del Riesgo Secretaría TIC, Innovación y Gobierno Abierto

Activo STIC-20	**STIC-20 Secretaría TIC, Innovación y Gobierno Abierto**							
Administrador	**Soporte Técnico**							
Degradación	**100%**							
Impacto	**5**	**Mayor**						
Tipo activo	**Instalaciones**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							3,4	Intolerable
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	N1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo	Muy baja	2	10	3	Intolerable
	N8	Desastres Naturales Fenómeno de Origen Volcánico	La secretaria de TIC se encuentra en zona media de riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Muy baja	2	10	3	Intolerable

Tabla 146 (Continuación)

Activo STIC-20		**STIC-20 Secretaría TIC, Innovación y Gobierno Abierto**							
Administrador		**Soporte Técnico**							
Degradación		**100%**							
Impacto		**5**	**Mayor**						
Tipo activo		**Instalaciones**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							3,4	Intolerable	
				Frecuencia (F)		**R**	**NR**		
Ataques Intencionados	I1	Fuego	Falta de un sistema de alarma contra incendios. Falta de extintor en la sala de comunicaciones Falta de alarmas de Humo.	Muy baja	2	10	3	Intolerable	
	I*	Desastres Industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal Disposición desordenada de cableado eléctrico y de comunicaciones puede ocasionar un accidente a todo aquel funcionario que ingrese a la sala de comunicaciones y también corto circuito.	Baja	3	15	4	Extremo	
	A11	Acceso no autorizado	Falta de protocolos de seguridad, cualquier persona puede ingresar a la sala de comunicaciones.	Baja	3	15	4	Extremo	

Fuente: La presente investigación

Tabla 147 Estimación del Riesgo Personal TIC

Activo STIC-21		**STIC-21 Personal TIC**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Personal**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							3	Intolerable
				Frecuencia (F)		**R**	**NR**	
Errores y Fallos	E7	Deficiencias en la Organización,	Falta de capacitación sobre seguridad de la Información. Falta me mecanismos de monitoreo de personal Falta de políticas de uso correcto de telecomunicaciones. Falta de políticas de contratación.	Baja	3	9	3	Intolerable
	E19	Fugas de Información	Falta de capacitación sobre seguridad de la Información.	Baja	3	9	3	Intolerable
Ataques Intencionados	E28	Indisponibilidad del Personal	Falta de un plan de contingencia en caso de ausencia	Muy baja	2	6	2	Tolerable
	A28	Indisponibilidad del Personal	Falta de un plan de contingencia en caso de ausencia	Muy baja	2	6	2	Tolerable
	A29	Extorsión	Falta de Políticas que definan un procedimiento a seguir ante vulnerabilidades de este tipo.	Baja	3	9	3	Intolerable
	A30	Ingeniería Social	Falta de capacitación sobre seguridad de la Información. Falta de concientización del personal en las mejores prácticas de seguridad informática.	Baja	3	9	3	Intolerable

Fuente: La presente investigación