DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 E ISO 27002 APLICADA A PROCESO DE GESTIÓN TIC DE LA GOBERNACIÓN DE NARIÑO

WILLIAM ALFREDO INAMPUES VILLA
DANIEL ESTEBAN LARA ROSERO

UNIVERSIDAD DE NARIÑO

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

PASTO

2018

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 E ISO 27002 APLICADA A PROCESO DE GESTIÓN TIC DE LA GOBERNACIÓN DE NARIÑO

WILLIAM ALFREDO INAMPUES VILLA
DANIEL ESTEBAN LARA ROSERO

Proyecto de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Director:
I.S. Esp. FRANCISCO SOLARTE SOLARTE

UNIVERSIDAD DE NARIÑO

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

PASTO

2018

NOTA DE RESPONSABILIDAD

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.

“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 N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma del Director de Tesis

_____
Firma del Jurado

_____
Firma del Jurado

San Juan de Pasto, agosto de 2018.

AGRADECIMIENTOS

En primer lugar, a Dios por habernos guiado por el camino correcto durante estos años de pregrado, por fortalecernos, darnos salud e iluminar nuestras mentes en esos difíciles momentos y por ponernos en la vida a cada una de esas personas incondicionales que contribuyeron al desarrollo de este proyecto.

Agradecer hoy y siempre a nuestros padres y familiares cercanos por el apoyo brindado y por sus consejos diarios que nos dan fortaleza para continuar formándonos integralmente día y día.

Un agradecimiento especial al Ingeniero Francisco Nicolás Solarte Solarte, director del proyecto, por su colaboración y disposición en el desarrollo de este trabajo, ya que, por medio de su orientación, fue posible la consecución de cada uno de los objetivos propuestos y culminación de la investigación.

Y por último al Ingeniero Daniel Álvarez García del Área de Proceso de Gestión TIC de la Gobernación de Nariño por su cooperación y suministro de información, fundamental para cada una de las fases del proyecto.

DEDICATORIA

Dedico este proyecto de grado a Dios que me ha dado la vida y fortaleza para culminarlo.

A mis padres, Manuel Mesías Inampues y Blanca Ligia Villa, quienes han velado por mi bienestar y educación, siendo apoyo incondicional en todo momento, y demás familiares por su ayuda y constante cooperación en el transcurso de la carrera.

A mis profesores, gracias por su tiempo, por su apoyo, así como por la sabiduría que me transmitieron en el desarrollo de mi formación profesional.

WILLIAM ALFREDO INAMPUES VILLA

DEDICATORIA

Dedico este proyecto a Dios, que gracias a el hoy puedo culminar uno de mis proyectos de vida.

A mi mama Rosario Rosero y a mis hermanos a quien les debo mucho, gracias por el apoyo y sacrificio, gracias porque siempre estuvieron presente en el proceso de formación profesional y vida.

A nuestro asesor Francisco Solarte porque gracias a el hoy este proyecto culmino con satisfacción, a nuestros profesores de carrera, a quienes gracias a su formación hoy puedo decir soy un Ingeniero de Sistemas, egresado de la mejor universidad de Colombia. UNIVERSIDA DE NARIÑO.

DANIEL ESTEBAN LARA ROSERO

RESUMEN

El Proyecto de grado correspondió al Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 e ISO 27002 para el Área de Proceso de Gestión TIC de la Gobernación de Nariño. Dicho sistema, contempla una serie de elementos, mecanismo, y lineamientos apropiados para el mejoramiento de la seguridad de la información al interior de la entidad en mención.

La estructura del proyecto, está dada por secciones, la primera de ellas concierne al Marco Referencial el cual consta de marco de antecedentes, contextual, teórico, conceptual y legal que soportan la investigación a desarrollar. Seguidamente se encuentra el aparte del Diseño Metodológico.

La Metodología que se desarrolló por planteamiento relaciona, cuatro fases vitales, a saber:

Fase 1: Diagnostico de la situación actual en materia de seguridad informática en el Área de Proceso de Gestión TIC de la Gobernación de Nariño.
Fase 2: Identificar los activos informáticos, definir y aplicar de la metodología de análisis y gestión del riesgo.
Fase 3: Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO 27001 e ISO 27002.
Fase 4: Definición de alcance, objetivos y política del Sistema de Gestión de Seguridad de la Información para el Área de Proceso de Gestión TIC de la Gobernación de Nariño.

Finalmente, en la sección de resultados y conclusiones se registró el impacto una vez se dio el desarrollo del proyecto de grado, así como los anexos que documentan la misma.

ABSTRACT

The Degree Project corresponds to the Design of an Information Security Management System based on ISO 27001 and ISO 27002 for the ICT Management Process Area of the Government of Nariño. Said system contemplates a series of elements, mechanism, and appropriate guidelines for the improvement of information security within the entity in question.

The structure of the project is given by sections, the first of which concerns the Reference Framework, which consists of a background, contextual, theoretical, conceptual and legal framework that supports the research to be developed. Next is the apart of the Methodological Design.

The Methodology of development that by approach relates, four vital phases, namely:

Phase 1: Diagnosis of the current situation in terms of computer security in the ICT Management Process Area of the Government of Nariño.
Phase 2: Identify the computer assets, define and apply the methodology of risk analysis and management.
Phase 3: Determine and evaluate the applicability of information security controls under ISO 27001 and ISO 27002.
Phase 4: Definition of the scope, objectives and policy of the Information Security Management System for the ICT Management Process Area of the Government of Nariño.

Finally, in the results and conclusions section, the impact is recorded once the development of the degree project occurred, as well as the annexes that document it.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

INTRODUCCIÓN

Existen normas elaboradas por la ISO y la IEC como son la ISO 27001 y la ISO 27002 las cuales describe cómo gestionar la seguridad de la información en una empresa, especifica los requisitos necesarios para establecer, implantar, mejorar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI) la cual establece las estrategias y controles adecuados que aseguren una permanente protección de la información, lo que contribuye a fomentar las actividades de protección de la información en las entidades públicas o privadas, mejorando su seguridad de la información, su imagen y generando confianza frente a terceros.

El empleo de esta norma verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.

El presente proyecto denominado, “Diseño de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001 e ISO 27002 Aplicada al Área de Proceso de Gestión TIC de la Gobernación de Nariño” brindo un apoyo al soporte de los datos que se encuentran registrados en la organización, para ello se implementó un SGSI con estándar ISO 27001 e ISO 27002 para el cuidado de la información el cual brinda confidencialidad, disponibilidad e integridad de los datos para el buen uso de la Información y no divulgación del mismo empezando por las unidades más pequeñas como lo son los procesos hasta llegar a una integración completa de todos los dominios y producir una documentación clara de los hallazgos y las recomendaciones.

El desarrollo de este proyecto se planteó abordando la definición de los activos que necesitan protegerse para el Área de Sistemas de la Gobernación de Nariño, junto con los riesgos, vulnerabilidades, amenazas y controles existentes para cada uno de ellos. Una vez hecho esto, se procedió a definir nuevos controles necesarios para cada uno de los activos, y como resultado se obtuvo un sistema de gestión de seguridad de la información (SGSI), ajustado a las necesidades actuales y que permita gestionar de manera eficiente la información para el Área de Sistemas de la Gobernación de Nariño, asegurando la integridad, confidencialidad y disponibilidad de la misma y con esto la mejora continua de la organización

Planteamiento del problema

Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

El acceso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más difícil salvaguardar la información y sus métodos de transmisión; ya sean estos comunicados verbales, archivos, documentos, base de datos, insuficiencias en las medidas y procedimientos recogidas en los planes de seguridad informática de entidades que no se rigen por los estándares internacionales que norman los sistemas de gestión de seguridad informática tanto en la prevención como recuperación ante desastres o ataques.

El problema radica en que la organización y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. Actualmente existen normas las cuales establecen metodologías de gestión de la seguridad clara y estructurada de la información.

Formulación del problema

¿Cómo el Diseño de un Sistema de Gestión de Seguridad de la Información SGSI basado en la norma ISO 27001 E ISO 27002 ayudará a mejorar la gestión de la seguridad en el Área de Proceso de Gestión TIC de la Gobernación de Nariño?

Justificación

Debido a los riesgos a los que están expuestos los activos de información, el impacto que la interrupción de estos puede causar, es preponderante la definición de una metodología y el uso de herramientas que nos ayuden reducir y mitigar estos riesgos.

Es por ello que se propuso la implementación de un Sistema de gestión de seguridad de información (SGSI) basado en la norma ISO 27001 e ISO 27002 el cual nos brindó los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información, implantar los controles necesarios que ayudaron a salvaguardar los activos de información de los procesos de tecnología, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de Información (SGSI), alineándolo de esta manera a los objetivos estratégicos de la organización.
Mediante el SGSI – Sistema de Gestión de Seguridad de la Información, el Área de Proceso de Gestión TIC de la Gobernación de Nariño consiguió minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permitió identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Como Objetivo general se tuvo mejorar la gestión de la seguridad en los procesos, servicios y sistemas de información mediante el Diseño de un SGSI basado en la Norma ISO 27001 e ISO 27002 para el Área de Proceso de Gestión TIC de la Gobernación de Nariño. En cuanto a los objetivos específicos fueron**:**

Identificar y determinar los activos informáticos del Área de Proceso de Gestión TIC de la Gobernación de Nariño mediante la aplicación de instrumentos de recolección de información para establecer los dominios del estándar ISO 27001 e ISO 27002

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

Verificar la existencia de controles de acuerdo a la norma ISO 27002 que ayude a definir la existencia de políticas y procedimientos de seguridad en el Área de Proceso de Gestión TIC

Diseñar el SGSI para la organización de acuerdo a los resultados de la evaluación realizada anteriormente.

Antecedentes de investigación

Los proyectos sobre el sistema de seguridad de la información son relativamente nuevos, por lo cual no se ha encontrado ninguno en la Gobernación de Nariño, y se tomó como referentes otros proyectos a nivel nacional e internacional que servirán de guía para enfocar mejor la investigación.

Dentro de los antecedentes se tomará en cuenta los siguientes:

El proyecto internacional desarrollado por Christian Miguel Cadme Ruiz y Diego Fabián Duque Pozo para la Universidad Politécnica Salesiana – Sede Cuenca (Ecuador) denominado: "AUDITORÍA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA LA EMPRESA DE ALIMENTOS "ITALIMENTOS CÍA. LTDA"[1]. En la empresa "ITALIMENTOS CÍA. LTDA." Existen vulnerabilidades para acceder a cierta información, para ello se ha realizado una auditoria de seguridad informática basada en un estándar internacional ISO 27001, el cual tiene como objetivo la confidencialidad, disponibilidad e integridad de los datos.

De este proyecto se tomó en cuenta la metodología utilizada para hacer un análisis de riesgos, vulnerabilidades, amenazas y el informe de recomendaciones presentado.

El proyecto desarrollado en la región por parte de José Daniel Guerra y Rafael Llerena, para la Institución Universitaria CESMAG – Sede Pasto denominado: "DIAGNOSTICO DEL ESTADO DE LOS SGSI CON LA APLICACIÓN DE UN SOFTWARE EN LAS INSTITUCIONES DE EDUCACION SUPERIOR DE SAN JUAN DE PASTO"[2]. En este proyecto se desarrolló un software que evalúa el estado de madurez de los sistemas de gestión de la información, en donde se concluye que solo a nivel regional, la Institución Universitaria CESMAG y la Universidad Mariana poseen sistemas de seguridad de información implantados que manejan un buen nivel de madurez. Sin embargo, aún existen muchas mejoras a los controles existentes sobre cada área de seguridad de la información.
De este proyecto se tomará como ejemplo los formatos de reportes que arroja el sistema y también se utilizarán los resultados obtenidos en esa época como parte de una base conceptual para dar nuestras respectivas recomendaciones y así se realizó la implantación del Sistema de Gestión de Seguridad de la Información por parte de los directivos del Área de Proceso de Gestión TIC de la Gobernación de Nariño**.**

Marco contextual

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

[1] CADME, Christian y DUQUE, Diego. Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos CÍA. LTDA.". Tesis previa a la obtención del título de Ingeniero de Sistemas. Cuenca. Ecuador: Universidad politécnica salesiana, 2012.

[2] LLERENA, Rafael y GUERRA, José. Diagnóstico del estado de los SGSI con la aplicación de un software en las instituciones de Educación superior de san juan de Pasto. Tesis previa a la obtención del título de Ingeniero de Sistemas. Pasto. Colombia: Institución universitaria CESMAG, 2009.

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 prebendando 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”

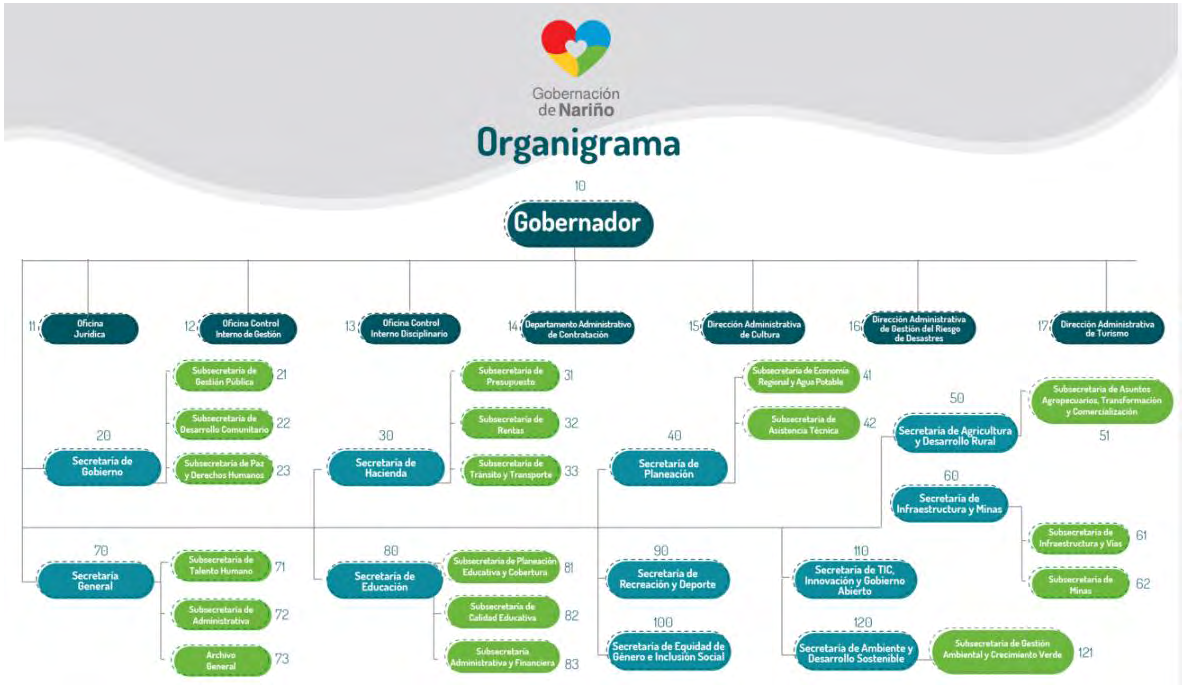
El 3 de octubre de 1588, se fundó el Ministerio de la Pura y Limpia Concepción de Nuestra Señora, contando por aquel entonces con 7 damas, 6 doncellas y 1 viuda. La ceremonia de clausura todavía la recuerda la historia; “El Vicario de Bracamonte puso cerrojo a las puertas y se guardó las llaves a la 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 sirvieron 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 quedó 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 tomó 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.

Figura 1. Estructura Orgánica - Gobernación de Nariño



Fuente: http://xn--nario-rta.gov.co/inicio/index.php/gobernacion/informacion-organizacional/organigrama

El alcance de este proyecto incluye:

- Definición de los activos en el Área de Proceso de Gestión TIC de la Gobernación de Nariño que necesitan protegerse de acuerdo a la norma ISO 27001.

- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en el Área de Proceso de Gestión TIC de la Gobernación de Nariño.
- Verificación de controles de seguridad de la información que se llevaron a cabo en el Área de Proceso de Gestión TIC de la Gobernación de Nariño teniendo en cuenta la norma ISO 27002.
- Estructuración del Sistema de Gestión de Seguridad de la Información para el Área de Proceso de Gestión TIC de la Gobernación de Nariño.

El proyecto contemplo el análisis y evaluación de riesgos de seguridad de la información como herramienta clave para la revisión y evaluación de los controles, que se logró una utilización más eficiente y segura de la información.
Estructura organizacional. "El Área de Proceso de Gestión TIC de la Gobernación de Nariño, en la actualidad solo se encuentra en una sola Área. Así mismo, el área tiene asignado un determinado número de procesos y procedimientos, los cuales cumplen su labor para la Gobernación de Nariño"[3].

En la figura 2 se puede apreciar el esquema jerárquico de la Gobernación de Nariño.

c. Administración portal web. El Portal Web de la Gobernación de Nariño www.narino.gov.co se encuentra administrado bajo plataforma Microsoft en un servidor con sistema operativo Windows Server 2010 SP2 bajo el framework 4.0 de .Net, desarrollado en su gran mayoría en el lenguaje de programación ASP.Net con aplicaciones de Silverlight y Adobe Flash CS3.

En sus contenidos de información se encuentran las secciones de noticias y actualidad de la Gobernación de Nariño, eventos, convocatorias, correo electrónico, boletín de prensa y un menú donde se puede acceder a los principales recursos de la Gobernación de Nariño, como sus diferentes dependencias.

Algunas de las aplicaciones que se conectan a través del Portal Web se encuentran desarrolladas bajo lenguaje de programación PHP y están ubicadas en un servidor APACHE, de igual manera en dicho servidor se encuentran almacenadas las bases de datos de las diferentes aplicaciones manejados bajo los motores de PostgresSQL y MySQL.

Actualmente, el Portal Web de la Gobernación de Nariño se encuentra a cargo de un profesional en Diseño Web quien lo administra personalmente y quien brindan soporte en la actualización del Portal, así como al desarrollo de nuevos sitios.

Procedimientos Administración Portal Web:

[3] AREA DE PROCESO DE GESTION TIC. Proyecto SGSI PGT. Pasto: Gobernación de Nariño. [en línea] Disponible en internet. http://www.narino.gov.co/. [citado febrero de 2018]

- Administración, publicación, montaje y mantenimiento de los sitios Web existentes dentro del Portal de la Gobernación de Nariño.

- Desarrollo de las políticas de seguridad y accesibilidad del Portal.

- Seguimiento, análisis, interpretación y evaluación estadística del tráfico del Portal.

- Gestión y capacitación de los diferentes sistemas de publicación específicos (Gestores de contenidos) para las respectivas dependencias de la Gobernación de Nariño.

- Mantenimiento el diseño Web del Portal de acuerdo con la definición de la estructura del mismo.

- Revisión y control de posibles errores existentes tanto en los links, estética como de contenido de la información.

Participar activa en el desarrollo de los planes estratégicos e informáticos de la Gobernación de Nariño.

d. Área de soporte técnico: "El Área de Soporte Técnico brinda al Área de Proceso de Gestión TIC de la Gobernación de Nariño el soporte y la asistencia técnica en el mantenimiento preventivo y correctivo de los equipos de cómputo y ofimática" [4]. .

Asistencia y soporte técnico: El servicio de soporte técnico tiene como objetivo brindar solución a los problemas que presenten los equipos de cómputo y ofimática en hardware y software. Dentro de este servicio se encuentran tareas tales como; configuración y conexión a la red de datos, instalación y configuración de periféricos como impresoras, cámaras, escáner, unidades ópticas y demás, recuperación y/o creación de copias de seguridad de la información, identificación, diagnóstico y eliminación de virus informáticos, asesorías en el uso del sistema operativo, software ofimático y aplicaciones básicas, así como también ensamblaje de equipos de cómputo, entre otras.

Mantenimiento preventivo: La ejecución el plan de mantenimiento preventivo busca diagnosticar y corregir posibles fallas que estén afectando el normal funcionamiento de los equipos de cómputo.

En el mantenimiento preventivo se realizan las siguientes tareas:

[4] Ibíd.

- Registro en el Sistema (inventario e historial de mantenimientos).
- Limpieza de hardware.
- Revisión, instalación y actualización de Software.
- Comprobación de errores de Disco Duro.
- Optimización del sistema operativo.
- Identificación, diagnóstico y eliminación de virus informáticos.

Funciones personal PGT[5]:

Tabla 1. Funciones – Director del Área de Proceso de Gestión TIC

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Director del Área de Proceso de Gestión TIC**
No. De Cargos:	Uno (1)
Dependencia:	Área de Proceso de Gestión TIC.
Cargo del Jefe Inmediato:	**Gobernador**
II. PROPOSITO PRINCIPAL	
Liderar la política del sector de las TIC's y definir estrategias para definir su acceso, uso y apropiación por parte de la comunidad, las entidades gubernamentales del orden territorial y el sector privado en el Departamento de Nariño, mediante la implementación de la trasparencia por medio del acceso a la información veraz, oportuna y de calidad para todos los ciudadanos, la participación activa de la ciudadanía en la construcción y aprobación conjunta de políticas colectivas que propendan a la realización social de nuestra región, y la colaboración de los diferentes grupos de interés que componen el recurso humano del departamento de Nariño por medio de la gestión, utilización y aplicación adecuada de esta información.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Gestionar el fortalecimiento del Ecosistema Digital en el Departamento de Nariño 2. Fomentar una política de Gobierno Abierto, para modernizar la Administración pública de la Gobernación del Departamento, ampliando el rol del ciudadano para que sea protagonista del proceso del cambio 3. Implementar las posibilidades que ofrecen las TIC a los ciudadanos para que participen de manera activa y directa, en la toma de decisiones del gobierno del departamento. 4. Apoyar en la conciliación de un modelo de democracia conversacional y abierta por medio de un ejercicio continuo de trasparencia de la	

[5] PROCESO DE GESTIÓN TIC. Manual especifico de funciones Pasto: Gobernación de Nariño, 2016.

Continuación tabla 1.

información, aplicación de esta información por parte de diferentes grupos de interés, y participación ciudadana en la construcción de una política pública colectiva.

5. Apoyar y elaborar planes estratégicos, de acción y proyectos de inversión fortalecidos en lineamientos TIC.
6. Buscar mecanismos de sensibilización para la población en general sobre el uso adecuado de las TIC.
7. Propender por la inversión de recursos, por parte de la Gobernación de Nariño que garanticen la sostenibilidad de los proyectos TIC en el ente territorial.
8. Dirigir y coordinar la formulación, adopción, ejecución y control de las políticas, planes generales, programas y proyectos que garanticen el apoyo tecnológico en el fortalecimiento del ecosistema digital.
9. Diseñar e implementar estrategias orientadas a la creación de ambientes favorables para el desarrollo de la industria de tecnologías de la información y las comunicaciones en el ente territorial o en beneficio de este.
10. Formular panes y programas de la secretaria TIC para promover la competitividad de las empresas localizadas en el Departamento de Nariño, a través del uso y apropiación de las tecnologías de la información y la comunicación.
11. Desarrollar programas de capacitación en el manejo de las Tecnologías de la Información y las Comunicaciones para la Comunidad del Departamento de Nariño a través de un programa de inclusión digital que favorezca a todos los sectores de la sociedad.
12. Orientar el desarrollo de todos los proyectos de competitividad, innovación, ciencia y tecnología, en el departamento de Nariño.
13. Gestionar la consecución de proyectos TIC de cooperación técnica y cofinanciación de recursos financieros con el Gobierno Nacional y Organismos Internacionales que generen desarrollo económico en las entidades territoriales regionales.
14. Realizar el análisis de requerimientos para el desarrollo de nuevos aplicativos e implementación de software sobre medida para la articulación total de la Gobernación con las diferentes secretarias, entidades descentralizadas y entidades territoriales y coordinar con las demás dependencias de la Administración Departamental el diseño y puesta en marcha de un sistema de información integral.
15. Crear políticas que permitan preservar, proteger y administrar de forma eficiente la información de la Gobernación de Nariño, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, para

Continuación tabla 1.

asegurar el cumplimiento de las funciones misionales de la entidad apoyadas en el uso adecuado de TIC. 16. Liderar y establecer planes estratégicos de acción para avanzar en el cumplimiento de la estrategia de gobierno en línea y demás políticas de nivel nacional. 17. Elaborar, ejecutar, el plan estratégico de tecnología de la información, ajustando permanente a la normatividad vigente y necesidades de la entidad. 18. Liderar y establecer las políticas de gestión, monitoreo y de control de software y hardware de red. 19. Liderar y establecer las políticas de soporte técnico y mantenimiento de equipos de cómputo de la entidad, para su buen funcionamiento y prevención de daños. 20. Presentar a consideración del Gobernador de Departamento de Nariño los proyectos de Ordenanza y actos administrativos relacionados con las funciones de la secretaria. 21. Ejercer las funciones de dirección, coordinación y control en las materias d su competencia. 22. Asistir a todas las reuniones y eventos que, en materia de TIC, innovación y gobierno Abierto, se programen y donde el señor Gobernador lo hay delegado. 23. Las demás que le sean asignadas por la autoridad competente, de acuerdo con el área de desempeño.

Fuente. ÁREA PROCESO DE GESTIÓN TIC. Manual especifico de funciones. Pasto: Gobernación de Nariño, 2016.

Tabla 2. Funciones – Administrador soporte y servicios tecnológicos

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador soporte y servicios tecnológicos.**
No. De Cargos:	Uno (1)
Dependencia:	Área de Proceso de Gestión TIC
Cargo del Jefe Inmediato:	**Director del Área de Proceso de Gestión TIC**
II. PROPOSITO PRINCIPAL	
Contribuir en la eficiencia e innovación de los procesos y servicios de la infraestructura tecnológica y comunicaciones de la Gobernación de Nariño, a través de la gestión del soporte técnico y el mantenimiento preventivo en los equipos de cómputo de las diferentes dependencias administrativas.	

Continuación tabla 2.

III. DESCRIPCIÓN DE FUNCIONES ESENCIALES
1. Administrar y supervisar los procedimientos; de soporte y asistencia técnica en la solución de los problemas que presenten los equipos de cómputo y ofimática de las dependencias administrativas de la Gobernación de Nariño. 2. Ejecutar los cronogramas y procedimientos del mantenimiento preventivo en los equipos de cómputo de la Gobernación de Nariño. 3. Administrar y controlar el inventario de los equipos de cómputo y de ofimática del Área de Proceso de Gestión TIC. 4. Diseñar e implementar el programa de mantenimiento preventivo en el Área de Proceso de Gestión TIC. 5. Instalar y configurar el hardware y software disponible en el Área de Proceso de Gestión TIC, acorde a las solicitudes de las unidades administrativas. 6. Apoyar el servicio de préstamo de recursos audiovisuales y multimedia. 7. Asesorar cuando se requiera a las diferentes dependencias en la adquisición de equipos de cómputo y ofimática. 8. Brindar asistencia y soporte técnico en las actividades o eventos programados por la Gobernación de Nariño, dentro y fuera de las instalaciones, según sus requerimientos. 9. Presentar informes cuando sean solicitados sobre el estado actual de los equipos de cómputo del Área de Proceso de Gestión TIC. 10. Investigar e implementar sobre nuevas tecnologías en software y hardware. 11. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Gobernación. 12. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 13. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene.

Fuente. ÁREA PROCESO DE GESTION TIC. Manual especifico de funciones. Pasto: Gobernación de Nariño, 2016.

Tabla 3. Funciones – Administrador de red de datos e internet

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador de red de datos e internet**.
No. De Cargos:	Uno (1)
Dependencia:	Área de Proceso de Gestión TIC
Cargo del Jefe Inmediato:	**Director del Área de Proceso de Gestión TIC**
II. PROPOSITO PRINCIPAL	
Asegurar que la red de datos funcione correctamente, dando servicio de internet, intranet a todas las dependencias de la Gobernación de Nariño, permitiendo la adecuada aplicación de las normas y procedimientos vigentes, con el fin de cumplir con las labores pertinentes, Investigación y Proyección Social de la Gobernación de Nariño.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Brindar soporte, operación, gestión y mantenimiento de la red privada e Internet. 2. Realizar la configuración, gestión y mantenimiento de los equipos activos y pasivos de red, además refinamiento del servidor proxy y firewall, según especificaciones técnicas. 3. Realizar la instalación, configuración y mantenimiento de los servidores Proxy, Firewall, DHCP, DNS, FTP, según procedimientos establecidos. 4. Administrar la utilización del ancho de banda, para evitar su uso inadecuado, de acuerdo a lineamientos establecidos. 5. Participar en el desarrollo de los planes estratégicos e informáticos de la Gobernación, dando cumplimiento a la modernización tecnológica. 6. Apoyar en la implementación e investigación sobre nuevas tecnologías en comunicación, telemática e Internet, videoconferencia red de alta velocidad, según metodología planteada. 7. Administrar lógicamente la red inalámbrica de la Gobernación, de conformidad con los lineamientos fijados por el Área de Proceso de Gestión TIC. 8. Apoyar en la administración de sistemas de información y administración de servidores, según requerimientos. 9. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Gobernación. 10. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros.	

Continuación tabla 3.

11. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad.

Fuente. ÁREA DE PROCESO DE GESTIÓN TIC. Manual especifico de funciones. Pasto: Gobernación de Nariño, 2016.

Tabla 4. Funciones - Administrador de sistemas

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador De Sistemas**
No. De Cargos:	Uno (1)
Dependencia:	Área de Proceso de Gestión TIC
Cargo del Jefe Inmediato:	**Director del Área de Proceso de Gestión TIC**
II. PROPOSITO PRINCIPAL	
Mantener actualizada y asegurada la plataforma de infraestructura tecnológica de servidores computacionales, que permiten a la comunicación de la Gobernación de Nariño, una fácil comunicación apoyando la agilidad de los procedimientos de las dependencias de la Gobernación.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Garantizar el aseguramiento lógico y administración de servidores, según metodologías y estándares de seguridad. 2. Administrar el sistema de correo electrónico de la Gobernación de Nariño – Postmaster, según la normativa de la organización. 3. Montaje y Administración de sistemas de Información alojados en los servidores del Área de Proceso de Gestión TIC de la Gobernación de Nariño, según requerimientos de usuarios, recursos disponibles y normatividad establecida. 4. Administrar Bases de Datos, asegurando la confidencialidad, la integridad y la disponibilidad de la información. 5. Apoyar en la implementación e investigación sobre nuevas tecnologías en comunicación, telemática e Internet. 6. Apoyar a la administración del portal web de la Gobernación. 7. Salvaguardar la confidencialidad de la información tanto de los usuarios de la red como de la información de las bases de datos de la Gobernación. 8. Administrar mantener y asegurar el sistema interno de mensajería instantánea, garantizando funcionalidad en el sistema. 9. Participar, de acuerdo a su competencia, en el desarrollo de los planes estratégicos e informáticos de la Gobernación, contribuyendo a la modernización tecnológica. 10. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Gobernación.	

Continuación tabla 4.

11. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 12. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene.

Fuente. ÁREA DE PROCESO DE GESTIÓN TIC. Manual especifico de funciones. Pasto: Gobernación de Nariño, 2016.

Tabla 5. Funciones – Administrador portal web

I. IDENTIFICACIÓN	
Nivel:	Profesional
Denominación del Empleo:	**Administrador Del Portal Web**
No. De Cargos:	Uno (1)
Dependencia:	Área de Proceso de Gestión TIC
Cargo del Jefe Inmediato:	**Director del Área de Proceso de Gestión TIC**
II. PROPOSITO PRINCIPAL	
Asegurar el correcto funcionamiento del Portal Web, en función del intercambio informativo entre la sociedad y grupos de interés, con el fin de cumplir con las labores pertinentes, Investigación y Proyección Social de la Gobernación de Nariño.	
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES	
1. Administrar, actualizar, brindar soporte y mantenimiento al Portal Web de la Gobernación de Nariño conforme a procedimientos establecidos. 2. Desarrollar los sitios web de las unidades administrativas de la Gobernación, realizando su publicación, montaje y mantenimiento, de acuerdo a los requerimientos. 3. Realizar capacitación en el manejo de los sistemas de publicación específicos (gestores de contenidos) a las unidades administrativas de la Gobernación, de acuerdo con prioridades establecidas y requerimientos. 4. Hacer el seguimiento, análisis, interpretación y evaluación estadística del tráfico del Portal Web de la Gobernación, siguiendo especificaciones técnicas. 5. Desarrollar las políticas de seguridad y accesibilidad del portal teniendo en cuenta la normatividad vigente. 6. Investigar e implementar nuevas tendencias tecnológicas referentes al área de su desempeño, según necesidades. 7. Brindar respaldo al área de administración de sistemas, según requerimientos.	

Continuación tabla 5.

8. Participar de acuerdo a su competencia en el desarrollo de los planes informáticos de la Gobernación y modernización tecnológica, según necesidades. 9. Coordinar y supervisar las actividades de todos los integrantes que colaboran en el funcionamiento del Portal Web de la Gobernación, según procedimientos establecidos. 10. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 11. Adelantar, de acuerdo a su competencia y responsabilidad, las actividades relacionadas con el establecimiento, documentación, implementación y mantenimiento del Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de la eficacia, eficiencia y efectividad de los planes, programas, proyectos y procesos en los cuales interviene. 12. Desempeñar las demás funciones que le asigne el superior inmediato de acuerdo con el nivel, la naturaleza, el área de desempeño, y el perfil del empleo.

Fuente. ÁREA DE PROCESO DE GESTIÓN TIC. Manual especifico de funciones. Pasto: Gobernación de Nariño, 2016.

Marco teórico

Seguridad de la información: "Es la protección de los activos de información frente a diferentes amenazas, con el objetivo de preservar su disponibilidad, integridad y confidencialidad que permitan a la organización cumplir con su misión o continuidad del negocio, minimizar el riesgo de materialización de las amenazas potenciales y maximizar el retorno de inversiones y oportunidades" [6] .

Las organizaciones que conocen los riesgos y los problemas que enfrentan relacionados con la seguridad de la información, ya sea por ataque deliberado de personal interno o externo, por un evento natural o un evento industrial, cuentan con personal certificado en prácticas de seguridad informática y gestionan varios recursos para la protección de la información y sistemas, lo que permite que dicha información sean menos vulnerable a ataques que hagan posible su distribución, modificación e incluso su eliminación[7].
Los principios básicos de la seguridad de la información, son los siguientes:

[6] SEGURIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.ean.edu.co/index.php?option=com_content&view=article&id=2597&Itemid=1280. [citado febrero de 2018].

[7] CONFIDENCIALIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html [citado febrero de 2018].

- Disponibilidad: Es la capacidad de accesibilidad a la información cuando se la requiera utilizar. La disponibilidad protege al sistema contra intentos accidentales o intencionados de realizar una eliminación de información no autorizada, denegación del servicio o accesibilidad a la información y de intentos de utilización del sistema o la información para propósitos no autorizados.

- Integridad: Se encarga de garantizar que la información únicamente pueda ser modificada por personal autorizado y de manera controlada y así evitar la pérdida de consistencia. La violación de la integridad se presenta cuando un empleado, programa o proceso (por accidente o intencionalmente) modifica o elimina los datos que hacen parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y dicha modificación sea registrada, asegurando su precisión y confiabilidad.

- Confidencialidad: Aseguramiento de que la información es accesible solo para personal autorizado.

Familia de normas ISO 27000: "La información es uno de los activos más importantes que debe ser manejado eficientemente, para garantizar ventajas dentro de los campos administrativos y académicos competidos en la actualidad, por lo que las organizaciones incrementan su inversión en el uso de diferentes tecnologías para su aseguramiento" [8].

Una adecuada gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y basado en objetivos claros de seguridad. Este proceso es el que conforma un Sistema de Gestión de Seguridad de la Información (SGSI), que podría considerarse por similitud con el Sistema de Calidad para la Seguridad de la Información basado en la norma ISO 9001.

Actualmente existen una serie de normas que proporcionan un marco de gestión para la seguridad de la información, las cuales pueden ser utilizadas por toda organización, cualquiera que sea su naturaleza y propósito. Estas normas son las que componen la serie ISO/IEC 27000 por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), donde se indica como estructurar e implantar un Sistema de Gestión de Seguridad de la Información basado en ISO 27001.

Origen: Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

[8] EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado febrero de 2018].

- BS 5750. Publicada en 1979. Origen de ISO 9001
- BS 7750. Publicada en 1992. Origen de ISO 14001
- BS 8800. Publicada en 1996. Origen de OHSAS 18001

La norma BS 7799 de BSI apareció en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información. La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas. En la segunda parte (BS 7799-2), publicada en 1998, la que estableció los requisitos de un sistema de seguridad de la información para ser certificable por una entidad independiente.
Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin grandes cambios, como ISO 17799 en el año 2000. En 2002, se revisó la segunda parte para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, esta norma se publicó por ISO como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799 que se renombró como ISO 27002:2005 el 1 de Julio de 2007.

En 2006, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

De igual manera, ISO continúa desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001.

Serie 27000: Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO/IEC 27000**: Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación.

- **ISO/IEC 27001:** Publicada el 15 de octubre de 2005. Es la norma principal de la serie y comprende dos secciones. La primera sección contiene los requisitos del Sistema de Gestión de Seguridad de la Información para obtención de certificación.

Las cláusulas metodológicas definidas en el estándar son:

Sistema de Gestión de Seguridad de la Información:

Responsabilidad de la Dirección:

- Compromiso de la Dirección: Se debe proveer evidencia de su compromiso con el proyecto.
- Provisión de recursos

Auditorías Internas a intervalos planificados para determinar:

- Si el SGSI es conforme a ISO 27001
- Si el SGSI es conforme con otros requisitos
- Si el SGSI está implantado y mantenido de forma efectiva
- Si el SGSI funciona según lo esperado

Revisión de la Dirección de forma regular para garantizar:

- Que el alcance sigue siendo adecuado
- Que las mejoras del SGSI han sido debidamente identificadas

Mejora continua del SGSI:

- Deben tomarse acciones correctivas y preventivas
- Tener experiencias propias o de otras organizaciones
- Comunicar acciones y mejoras a todas las partes interesadas
- Asegurar que las mejoras alcanzan los objetivos buscados

La segunda sección correspondiente al Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

Desde el punto de vista de certificación, cualquier exclusión de controles necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables.

- ISO/IEC 27002: “Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios” [9].

[9] ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [citado febrero de 2018].

Figura 2. Dominios ISO 27002

Fuente: Disponible en Internet. http://iso27002.es/

A5 Política de Seguridad

[5.1] Política de seguridad de la información: La Dirección debería establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.

A6 Organización de la Seguridad de la Información

[6.1] Organización interna: Gestionar la seguridad de la información dentro de la Organización. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.

[6.2] Terceros: Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

A7 Gestión de Activos

[7.1] Responsabilidad sobre los activos: Alcanzar y mantener una protección adecuada de los activos de la Organización.

[7.2] Clasificación de la información: Asegurar que se aplica un nivel de protección adecuado a la información.

A8 Seguridad de los Recursos Humanos

[8.1] Seguridad en la definición del trabajo y los recursos: Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

[8.2] Seguridad en el desempeño de las funciones del empleo: Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

[8.3] Finalización o cambio del puesto de trabajo: Garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma organizada.

A9 Seguridad Física y del Entorno

[9.1] Áreas seguras: Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.

[9.2] Seguridad de los equipos: Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

A10 Gestión de las Comunicaciones y Operaciones

[10.1] Procedimientos y responsabilidades de operación: Asegurar la operación correcta y segura de los recursos de tratamiento de información.

[10.2] Supervisión de los servicios contratados a terceros: Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.

[10.3] Planificación y aceptación del sistema: Minimizar el riesgo de fallos en los sistemas.

[10.4] Protección contra software malicioso y código móvil: Proteger la integridad del software y de la información.

[10.5] Gestión interna de soportes y recuperación: Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

[10.6] Gestión de redes: Asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo.

[10.7] Utilización y seguridad de los soportes de información: Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.

[10.8] Intercambio de información y software: Mantener la seguridad de la información y del software que se intercambian dentro de la organización o con cualquier entidad externa.

[10.9] Servicios de comercio electrónico: Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

[10.10] Monitorización: Detectar actividades de procesamiento de la información no autorizadas.

A11 Control de Acceso

[11.1] Requerimientos de negocio para el control de accesos: Controlar los accesos a la información.

[11.2] Gestión de acceso de usuario: Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

[11.3] Responsabilidades del usuario: Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.

[11.4] Control de acceso en red: Impedir el acceso no autorizado a los servicios en red.

[11.5] Control de acceso al sistema operativo: Impedir el acceso no autorizado al sistema operativo de los sistemas.

[11.6] Control de acceso a las aplicaciones: Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.

[11.7] Informática móvil y teletrabajo: Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

[12.1] Requisitos de seguridad de los sistemas: Garantizar que la seguridad es parte integral de los sistemas de información.

[12.2] Seguridad de las aplicaciones del sistema: Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

[12.3] Controles criptográficos: Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

[12.4] Seguridad de los ficheros del sistema: Garantizar la seguridad de los sistemas de ficheros.

[12.5] Seguridad en los procesos de desarrollo y soporte: Mantener la seguridad del software del sistema de aplicaciones y la información.

[12.6] Gestión de las vulnerabilidades técnicas: Reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.

A13 Gestión de los Incidentes de Seguridad

[13.1] Comunicación de eventos y debilidades en la seguridad de la información: Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.
[13.2] Gestión de incidentes y mejoras en la seguridad: Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.

A14 Gestión de la Continuidad del Negocio

[14.1] Aspectos de la gestión de continuidad del negocio: Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

A15 Cumplimiento

[15.1] Conformidad con los requisitos legales: Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.

[15.2] Revisiones de la política de seguridad y de la conformidad técnica: Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la Organización.

[15.3] Consideraciones sobre la auditoría de sistemas: Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde este proceso.

Sistema de Gestión de Seguridad de la Información: "La gestión de la seguridad de la información es necesaria que se realice mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso se puede constituir por el Sistema de Gestión de Seguridad de la Información (SGSI)" [10].

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se instituye ISO 27001, cuyo estándar ha sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar:

- Confidencialidad: Aseguramiento de que la información es accesible solo para personal autorizado.
- Integridad: Se encarga de garantizar que la información únicamente pueda ser modificada por personal autorizado y de manera controlada y así evitar la pérdida de consistencia.
- Disponibilidad: Es la capacidad de accesibilidad a la información y los sistemas de tratamiento de la misma cuando se los requiera utilizar

Este modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en un análisis y evaluación de riesgos y en una medición de la eficacia de estos. Por lo tanto, el SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

La aceptación de este estándar debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización.

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional impulsa que sus usuarios enfaticen la importancia de:

[10] PARÁMETROS FUNDAMENTALES PARA LA IMPLANTACIÓN DE UN SGSI SEGÚN ISO 27001:2005. [en línea] Disponible en internet. http://www.slideshare.net/jhonny14/iso27001-norma-e-implantacion-sgsi. [citado febrero de 2018].

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del Sistema de Seguridad de la Información.
- Mejoramiento continuo en base a la medición del objetivo.

Beneficios de un SGSI:

- Involucrar a la Dirección en la seguridad de la información
- Desarrollar políticas formales de cumplimiento obligatorio
- Conocer realmente de qué activos dispone la organización
- Cumplir con la legislación vigente ligada al proyecto
- Realizar análisis de riesgos para el desarrollo del negocio
- Introducción de contratos de niveles de servicio
- Reforzar la seguridad ligada a personal
- Disponer de planes de contingencias ante incidentes
- Disponer planes de continuidad del negocio y recuperación ante desastres
- Desarrollo de indicadores del desempeño del SGSI
- Disminución de riesgos a niveles aceptables, etc.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, se adopta el ciclo de mejora continua PHVA (Véase Figura 6).

Figura 3. Ciclo PHVA

Fuente: http://www.iso27000.es/sgsi.html

- **Planear**: Establecer el Sistema de Gestión de Seguridad de la Información. Es una fase donde se realiza el análisis y evaluación de riesgos, el Plan de Tratamiento de Riesgos y la definición de las políticas de seguridad.

- **Hacer**: Implementar y operar el Sistema de Gestión de Seguridad de la Información. Es una fase que envuelve la implementación y operación de los controles.
- **Verificar**: Monitorear y revisar el Sistema de Gestión de Seguridad de la Información. Es una fase de medición de resultados, auditoria interna y revisión por parte de la dirección de la organización.
- **Actuar**: Mantener y mejorar el Sistema de Gestión de Seguridad de la Información. Es una fase en la que se llevan a cabo acciones preventivas y correctivas para el Sistema de Gestión de Seguridad de la Información.

Se Llevó a cabo la implantación de un Sistema de Gestión de Seguridad de la Información que comprendió las siguientes etapas:

- Identificar los objetivos del negocio
- Obtener el patrocinio de la alta dirección
- Establecer el alcance (algunos procesos del negocio)
- Diagnóstico / Análisis de brecha (Gap Analysis)

En esta etapa se determinó la brecha con respecto al nivel de madurez de los requerimientos del estándar ISO/IEC 27001:2005, el cual dispone de unas cláusulas cuya finalidad fue establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, en el contexto de los requerimientos de la organización.
El estándar comprendió dos (2) secciones: En la primera se especificó cinco (5) cláusulas, de cumplimiento obligatorio para obtener la certificación, enfocadas a características metodológicas del SGSI. En la segunda, denominada Anexo A, se definieron los controles mínimos para gestionar la seguridad de la información de manera adecuada. Desde el punto de vista de la certificación, cualquier exclusión de controles necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables.

Las cláusulas metodológicas definidas en el estándar fueron:

- Sistema de Gestión de Seguridad de la Información
- Responsabilidad de la Dirección
- Auditorías Internas
- Revisión de la Dirección
- Mejora continua del SGSI.

Los controles del Anexo A están organizados en once (11) dominios, denominados A5 hasta A15:

A5 Política de Seguridad
A6 Organización de la Seguridad de la Información
A7 Gestión de Recursos

A8 Seguridad de los Recursos Humanos
A9 Seguridad Física y del Entorno
A10 Gestión de las Comunicaciones y Operaciones
A11 Control de Acceso
A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
A13 Gestión de los Incidentes de Seguridad
A14 Gestión de la Continuidad del Negocio
A15 Cumplimiento

El diagnóstico se realizó por medio de una serie de entrevistas a los responsables de los temas contemplados en el estándar, las cuales pueden ser complementadas con una revisión documental de los procedimientos y políticas asociadas a la seguridad de la información.

Una vez relevada la información, se procedió a analizar los controles y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala definida por el estándar COBIT, consignada en la **Tabla 6. Escala nivel de madurez COBIT** contenida en el Anexo J – Plantillas y tablas.

- Se asignar recursos y capacitación al equipo

Análisis y evaluación de riesgos de activos de información:

- Se definieron método de análisis y evaluación: En el ámbito empresarial, toda organización, cualquiera que sea su naturaleza y propósito, se crea y se estructura en unas reglas y normas de comportamiento que permitan alcanzar unos objetivos propuestos. Existe un gran número de eventualidades que pueden perjudicar negativamente el cumplimiento de dichos objetivos, ya sean de origen interno o externo, intencionado o deliberado. De igual manera las innumerables medidas de protección contra este tipo de eventos son inabarcables por motivos de costo.
- Por tal razón se hiso necesario definir un proceso para identificar los riesgos más significativos, en oposición a los riesgos de bajo impacto, baja frecuencia o alto costo de control del mismo. Para este proyecto se utiliza la metodología MAGERIT.
- Se preparar un inventario de los activos de información a proteger: En adición al inventario de activos, para la valuación de riesgos son de gran importancia los informes de vulnerabilidades, informes de seguimiento de riesgos y repositorio de incidentes para definir las amenazas y vulnerabilidades de cada activo de información.
- Análisis de riesgos: El análisis de riesgos es la herramienta por medio de la cual se puede identificar, clasificar y valorar los riesgos a los que la organización está expuesta y establecer los controles adecuados para minimizar la probabilidad de

materialización o reducir el impacto de estos hasta un nivel tolerable o aceptable en caso de materializarse.

- Evaluación de riesgos: En la medida en que el riesgo implica una eventual exposición a un impacto para la consecución de los objetivos de una organización, tiene una connotación negativa. No obstante, el riesgo es algo inherente a cualquier actividad y no puede considerarse un factor adverso, sino un factor que conviene conocer y gestionar adecuadamente para que se convierta en una ventaja competitiva para la unidad.

  Un mejor control del riesgo, en la medida en que se transmita a todos los grupos de interés (personal, proveedores, supervisores, etc.) puede proporcionar ventajas competitivas significativas. Esta característica del riesgo tanto como amenaza y como oportunidad se refleja tanto en la cantidad de riesgo que una organización es capaz de gestionar y la cantidad de riesgo que está dispuesta a gestionar para lograr los objetivos propuestos. Con los resultados obtenidos en el análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios. En esta actividad se concluye el Informe de evaluación de riesgos TI, el cual es utilizado para elaborar el Plan de tratamiento de riesgos.

- Gestionar el riesgo y elaborar un Plan de Tratamiento de Riesgos: Elaboración del Plan de Tratamiento de riesgos que contenga una serie de controles y recomendaciones básicas de seguridad para toda la organización que permita disminuir un alto grado de riesgo.
- Establecer la normativa para controlar el riesgo: Establecer las políticas de seguridad de la información que mejor se adapten a la organización.
- Monitorizar la implantación del SGSI: Con base en el informe de riesgos, el plan de seguridad y los informes de estado de la seguridad, se evalúa el avance de la implementación y la eficacia de los controles vigentes. La eficacia se mide a través de pruebas de vulnerabilidades o “ethical hacking”, realizadas en forma coordinada.
- Prepararse para la auditoria de certificación
- Llevar a cabo auditorías internas periódicas.

Estándares y metodologías para el análisis y gestión de riesgos: “La gestión de riesgos de seguridad de la información es tal vez el proceso más significativo para la estructuración, mantenimiento y mejora de un sistema capaz de gestionar adecuadamente la seguridad de la información” [11].

[11] SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [citado marzo de 2018].

Las metodologías de análisis y/o evaluación de riesgos ayudan a las organizaciones a acelerar este proceso. Algunas de las metodologías más utilizadas son:

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

- **COBIT (*Control Objectives for Information and related Technology*): "**Es un modelo de gobierno para administrar el riesgo y controlar las Tecnologías de Información. Mantenido por ISACA (en inglés: *Information Systems Audit and Control Association*) y el IT *Governance Institute*, tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de Tecnologías de Información, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión" [12].

  La estructura del estándar COBIT se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.

  En la actualidad se encuentra la versión 5, la cual proporciona una visión empresarial del Gobierno de Tecnologías de Información que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

- **MAGERIT: "**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" [13].

---

[12] ¿Cuál es el mejor estándar de administración de riesgo para las TI? [en línea] Disponible en internet. http://www.emb.cl/gerencia/articulo.mvc?xid=1301. [citado marzo de 2018].

[13] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. [en línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf. [citado marzo de 2018].

MAGERIT persigue los siguientes objetivos:

Directos:

a) concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
b) ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
c) ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Actualmente se encuentra en la versión 3; durante el periodo transcurrido desde la publicación de la primera versión de MAGERIT (1997), el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

La versión 2 y 3 de MAGERIT se ha estructurado en tres libros: “El Método”, un “Catálogo de Elementos” y una “Guía de Técnicas”.
El método: “Realización del análisis y de la gestión: En la Planificación del Análisis y Gestión de Riesgos se establecen las consideraciones necesarias para arrancar el proyecto, investigando la oportunidad de realizarlo, definiendo los objetivos que ha de cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del proyecto” [14].

Análisis de Riesgos: En el Análisis de riesgos se identifican y valoran los elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.
Elementos del análisis de riesgos: Aquí el Analista de Riesgos es el profesional especialista que maneja seis elementos básicos:

a. Activos: El activo esencial es la información o dato.

b. Amenazas: Determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza.

Las amenazas según MAGERIT pueden ser de 4 tipos como se indica en la **Tabla 7. Tipo de amenazas MAGERIT** contenida en el Anexo J – Plantillas y tablas.

[14] Ibíd.

c. Vulnerabilidades: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

d. Impacto: Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto

e. Riesgo: Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo ya podemos calcular la frecuencia

f. Salvaguardas: Es un mecanismo de protección frente a las amenazas.

Catálogo de elementos: "Ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, escala de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información. Se persiguen dos objetivos[15]:

a. Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
b. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Dicho catálogo está conformado por las siguientes tablas: **Tabla 8. Tipos de activos, Tabla 9. Dimensiones de valoración de un activo**, **Tabla 10. Valoración cualitativa y Tabla 11. Valoración cuantitativa** que pueden consultarse en el Anexo J – Plantillas y tablas.

Muchos Activos de información no son medibles en sentido contable o como 'valor de cambio'; pero no por ello dejan de tener 'valor de uso' para la organización.

Controles: Hay diferentes aspectos en los cuales puede actuar un control para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

[PR] Se requieren procedimientos tanto para la operación de los controles preventivos como para la gestión de incidencias y la recuperación tras las mismas.

[PER] política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe cubrir desde las fases de especificación del puesto de trabajo y selección, hasta la formación continua.

[15] Ibíd.

Guía de técnicas: *"*Proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos" [16].

Es importante resaltar que la notación que se propone en la aplicación de la técnica en ningún caso se considerará obligatoria. Cada organización podrá utilizar la notación que desee, la que suele utilizar o la que ofrecen sus herramientas de desarrollo, respetando las reglas y restricciones específicas de las distintas técnicas.

Técnicas específicas: Se han considerado de especial interés:

a. Uso de tablas para la obtención sencilla de resultados: La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Estimación del impacto: Se puede calcular el impacto con base a tablas sencillas de doble entrada. (Ver **Tabla 12. Estimación del impacto** en el Anexo J – Plantillas y tablas)

Aquellos activos que reciban una calificación de impacto desastroso deberían ser objeto de atención inmediata.

Estimación de la probabilidad: Por otra parte, se modela la probabilidad de ocurrencia de una amenaza por medio de escalas cualitativas. (Ver **Tabla 13. Estimación de la probabilidad** en el Anexo J – Plantillas y tablas)

Estimación del riesgo: La estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

*Riesgo = probabilidad * impacto*

Este proceso de análisis de riesgos normalmente genera un MAPA DE RIESGOS, en el que se ubican los activos de información identificados y los cálculos realizados. (ver **Tabla 14. Mapa de riesgos** en el Anexo J – Plantillas y tablas).

Con los resultados obtenidos con este análisis se procedió a la evaluación. Para cada activo, el proceso concluyo si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios. En esta actividad se concluye el *Informe de evaluación de riesgos TI*, el cual es utilizado para elaborar el *Plan de tratamiento de riesgos*.
El objetivo general del análisis de riesgos, es identificar las causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se

[16] Ibíd.

realiza en una determinada área para así tener suficiente información, optando por un diseño apropiado e implantación de mecanismos de control con el fin de minimizar los efectos de eventos no deseados.

Un minucioso análisis de riesgos; identificar, definir y revisar los controles de seguridad; determinar si se requiere incrementar las medidas de seguridad; y la identificación de los riesgos, los perímetros de seguridad, controles de acceso y los lugares de mayor peligro, pueden hacer el mantenimiento más fácilmente.

b. Técnicas algorítmicas para la obtención de resultados elaborados: Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos.

c. Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información: Los árboles de ataque son una técnica para modelar las diferentes formas de alcanzar un objetivo. El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.
Un árbol de ataque pasa revista a cómo se puede atacar un sistema y por tanto permite identificar qué salvaguardas se necesita desplegar para impedirlo. También permiten estudiar la actividad del atacante y por tanto lo que necesita saber y lo que necesita tener para realizar el ataque; de esta forma es posible refinar las posibilidades de que el ataque se produzca si se sabe a quién pudiera interesar el sistema y/o la información y se cruza esta información con las habilidades que se requieren.

Técnicas generales: Son utilizadas en el desarrollo de un proyecto de análisis y gestión de riesgos. Se han considerado de especial interés:

b. Técnicas gráficas: histogramas, diagramas de Pareto y de tarta:

- Por puntos y líneas: Es la forma más clásica de presentación de resultados. Se limita a usar los ejes cartesianos usando las abscisas para recoger los datos y las ordenadas para mostrar su valor.
- Por barras: Los diagramas de barras disponen los elementos en unas coordenadas cartesianas convencionales: los elementos a considerar en un eje y los valores en el otro eje.
- Gráficos de ‘radar’: Estos gráficos representan las distintas variables o factores del fenómeno en estudio sobre ejes o radios que parten de un centro. Estos radios, tantos como factores, se gradúan para representar sus niveles y posibles umbrales en escala normal o logarítmica, según convenga.

- Diagramas de Pareto: Una gráfica de Pareto es utilizada para separar gráficamente los aspectos más significativos de un problema que el equipo sepa dónde dirigir sus esfuerzos para mejorar. Reducir los problemas más significativos (las barras más largas en una gráfica Pareto) servirá más para una mejora general que reducir los más pequeños.
- Diagramas de tarta: Estos diagramas presentan los datos como fracciones de un círculo, distribuidos los 360º de éste en proporción al valor que es representado en cada sección. La proporción suele ser lineal; rara vez logarítmica.

c. Sesiones de trabajo: entrevistas, reuniones y presentaciones:

- Entrevistas: Las entrevistas son reuniones con una persona o un grupo de personas con el objetivo de obtener cierta información. Las entrevistas se dicen estructuradas cuando se atiene a una serie de preguntas planificadas sin margen para la improvisación. Las entrevistas se dicen libres cuando, existiendo un objetivo claro, no existe un formulario rígido.
- Reuniones: Las reuniones tienen como objetivo obtener información que se encuentra repartida entre varias personas, tomar decisiones estratégicas, tácticas u operativas, transmitir ideas sobre un determinado tema, analizar nuevas necesidades de información, así como comunicar los resultados obtenidos como consecuencia de un estudio.
- Presentaciones: El objetivo de las presentaciones es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda. Se llevan a cabo con el fin de informar sobre el estado de un proyecto en su totalidad o de alguno de los procesos, o exponer uno o varios productos finales de un proceso para su aprobación.

c. Valoraciones Delphi: La técnica Delphi es un instrumento de uso múltiple adecuada para MAGERIT que se utiliza con muy variados objetivos: Identificar problemas, desarrollar estrategias para la solución de problemas, fijando un rango de alternativas posibles, identificar factores de resistencia en el proceso de cambio, establecer previsiones de futuro sobre la evolución de las tendencias que se observan en un determinado campo o sector y contrastar opiniones en un tema abarcando un amplio campo de disciplinas o sectores.

Marco legal

Cada vez que se desee implementar un Sistema de Gestión de Seguridad de la Información, toda organización debe cumplir obligatoriamente con las leyes, normas y decretos aplicables en la consecución de los objetivos y desarrollo de actividades contenidas en un proyecto de este tipo.

“En lo que se refiere específicamente a Seguridad de la Información, algunas de las leyes y normas de la legislación colombiana tomadas de (Seguridad de la Información en Colombia, 2010)” [17]:

DECRETO 1377 DE 2013: “Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012”[18].

LEY ESTATUTARIA 1581 DE 2012: “Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional” **[19]**.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.
- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
- Crea una especial protección a los datos de menores de edad.
- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

---

[17] SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [en línea] Disponible en internet. http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html. [citado abril de 2018].

[18] DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [citado abril de 2018].

[19] LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado abril de 2018].

- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
- Crea el Registro Nacional de Bases de Datos.
- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

DECRETO 2693 DE 2012: "Por el cual se establecen los lineamientos generales de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones" [20].
LEY 1341 DEL 30 DE JULIO DE 2009: "Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones" [21].

LEY 1273 DEL 5 DE ENERO DE 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" [22].
LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008: "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" [23].

LEY 603 DE 2000: "Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales" [24].

---

[20] DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [citado abril de 2018].

[21] LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [citado abril de 2018].

[22] LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado abril de 2018].

[23] LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [citado abril de 2018].

[24] LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado abril de 2018].

Marco conceptual

Enseguida se especifican algunos términos que serán citados y utilizados en el desarrollo del proyecto.

Activos de información: Los activos de información referentes a un nivel tecnológico, son todos los relacionados con los sistemas de información, redes, comunicaciones y la información en sí misma, Por ejemplo, los datos, el hardware, el software, los servicios que se presta, las instalaciones, entre otros.[25]

Vulnerabilidad: Es una situación inherente a los activos, o presente en su entorno, que facilita la materialización de las amenazas y las llevan a la condición de debilidad. Las vulnerabilidades son de diversos tipos como, por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otras.[26]
Amenaza: Es aquella situación que puede ocasionar resultados negativos en las operaciones cotidianas de la Unidad de Informática y Telecomunicaciones, generalmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos físicos o ambientales, entre otros. Las amenazas logran ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos.[27]

Riesgo: Es aquel suceso que dificulta el cumplimiento de un objetivo de manera cuantitativa. Se puede considerar como una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva a dos tipos de consecuencias: Ganancias o pérdidas. Así mismo, el riesgo se plantea solamente como amenaza determinando el grado de exposición o el grado de una perdida (Por ejemplo, el riesgo de que se pierdan los datos por el daño del disco duro, virus informáticos entre otros).

La organización Internacional para la normalización (ISO), define riesgo tecnológico como:

[25] POLÍTICAS DE SEGURIDAD DE ACTIVOS DE INFORMACIÓN. [en línea] Disponible en internet. http://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/calidad/documentos/politicas_sgsi.pdf. [citado mayo de 2018].

[26] METODOLOGIA DE ANALISIS DE RIESGO DE LA EMPRESA LA CASA DE LAS BATERIAS S.A DE C.V. [en línea] Disponible en internet. http://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf. [citado mayo de 2018].

[27] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado mayo de 2018].

“La probabilidad de que una amenaza se materialice, utilizando una vulnerabilidad existente de un activo o un grupo de activos, generándole pérdidas o daños”[28].

Impacto: Es la consecuencia de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financieras, económicas, tecnológicas, físicas, entre otras.[29]

Análisis de Riesgos: Es un instrumento de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos mediante la identificación de sus elementos, lograr establecer el riesgo total y consecutivamente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos.[30]

Probabilidad: Para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada.[31]

Evaluación de Riesgos: Este proceso incluye la medición del potencial de las pérdidas y la probabilidad de la pérdida, categorizando el orden de las prioridades.

Un conjunto de criterios puede ser usado para establecer una prioridad, enfocada en el impacto financiero potencial de las pérdidas, por ejemplo: riesgos críticos, que son todas las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota, riesgos importantes donde las exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones, riesgos no importantes que son las exposiciones a pérdidas que no causan un gran impacto financiero.[32]

SGSI: SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas *de Information Security Management System*. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una

[28] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado mayo de 2018].

[29] Ibíd.

[30] Ibíd.

[31] Ibíd.

[32] Ibíd.

entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.[33]

MAGERIT: La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.[34]

Objetivos de Control y Riesgos: Los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la información es resguardada por los controles de calidad del input, procesamiento, output y software.

Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran la conformidad con las leyes y regulaciones, los estándares contables y de auditoría, y las políticas y procedimientos internos.[35]

Actividades de Control: COBIT y SAC examinan procedimientos de control relativos al sistema automatizado de información de una entidad; COSO discute los procedimientos y actividades de control utilizados en toda la entidad. COBIT clasifica los controles en 32 procesos agrupados naturalmente en cuatro dominios aplicables a cualquier ambiente de procesamiento de información. SAC utiliza cinco esquemas de clasificación diferentes para los procedimientos de control de SI. COSO utiliza solo un esquema de clasificación para los procedimientos de control del sistema de información (SI). La discusión de COSO sobre las actividades de control enfatiza en quién realiza las actividades y en lo operativo más que en los objetivos de informes financieros. COSO también enfatiza la deseabilidad de integrar las actividades de control con la evaluación de riesgos.[36]

---

[33] EL PORTAL DE ISO 27001 EN ESPAÑOL - GLOSARIO. [en línea] Disponible en internet. http://www.iso27000.es/glosario.html. [citado mayo de 2018].

[34] MAGERIT. [en línea] Disponible en internet. https://seguridadinformaticaufps.wikispaces.com/MAGERIT. [citado mayo de 2018].

[35] COMPARACIÓN DE CONTROLES INTERNOS: COBIT, SAC Y COSO. [en línea] Disponible en internet. http://www.netconsul.com/riesgos/cci.pdf. [citado mayo de 2018].

[36] Ibíd.

Linux BackTrack: Es una distribución GNU/Linux en formato Live CD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (*WhiteHat Knoppix*), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu. Incluye una larga lista de herramientas de seguridad aptas para el uso, entre las que destacan numerosos escaneadores de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. Fue incluida en el puesto 7 de la famosa lista "Top 100 Network Security Tools" de 2006. [37]

SQLMAP: Es una herramienta desarrollada en 53ython para realizar inyección de código sql automáticamente. Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web. Una vez que se detecta una o más inyecciones SQL en el host de destino, el usuario puede elegir entre una variedad de opciones entre ellas, enumerar los usuarios, los hashes de contraseñas, los privilegios, las bases de datos o todo el volcado de tablas y/o columnas específicas del DBMS (Sistema de gestión de base de datos), ejecutar su propio SQL SELECT, leer archivos específicos en el sistema de archivos y mucho más.[38]

GOYSCRIPT WEP: Es un script de bash de Linux para poder realizar auditorías de redes WiFi con seguridad WEP (*Wired Equivalent Privacy*). Utilizado para encontrar debilidades en la clave de red de diferentes routers.[39]

1. METODOLOGÍA APLICADA

1.1 Apoyo de la dirección

Uno de los principios fundamentales que se realizó para iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección del Área. No sólo por ser un punto esencial contemplado en la norma sino porque el cambio de cultura y la

[37] BACKTRACK. [en línea] Disponible en internet. http://es.wikipedia.org/wiki/BackTrack. [citado junio de 2018].
[38] SQLMAP – HERRAMIENTA AUTOMÁTICA DE INYECCIÓN SQL. [en línea] Disponible en internet. http://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml. [citado junio de 2018].
[39] GOYSCRIPT (WEP, WPA & WPS). [en línea] Disponible en internet. http://foro.seguridadwireless.net/live-wifislax/goyscriptwep-goyscriptwpa-y-goyscriptwps/. [citado junio de 2018].

concienciación que genera el proceso hacen necesario el impulso constante de la Dirección.

1.2 Plan de recolección de información

Una vez avalado el trabajo por parte de la Dirección, se procedió con la recolección de toda la información necesaria para la consecución del proyecto.

Al final se conformó un inventario de activos actualizado y clasificado para el Área de Proceso de Gestión TIC de la Gobernación de Nariño:

Director del Área de Proceso de Gestión TIC: Inventario conformado por 17 activos de información a proteger, entre los cuales se encuentran los principales servidores que alojan Sistemas de Información, el Portal web de la Gobernación de Nariño, Bases de Datos, aplicaciones, etc. También el personal encargado de la administración del área, la sala de servidores, servicios y demás.

Administración Portal Web: Inventario conformado por 6 activos de información a proteger, entre los que se encuentran el servidor NS1 que lo administra el área de Proceso de Gestión TIC, pero al que también tiene acceso por FTP y SSH la Administradora del Portal web, ya que en este servidor está alojada la página web y demás portales de las diferentes dependencias de la Gobernación de Nariño que son de su responsabilidad. También se listan los equipos de escritorio, sus respectivos Sistemas Operativos y la oficina asignada para llevar a cabo las actividades de esta área.

Área de Soporte Técnico: Un inventario para la parte de Soporte Preventivo y otro inventario para la parte de Soporte Correctivo.

Soporte Preventivo: Inventario conformado por 6 activos de información a proteger, entre los que se encuentran el personal encargado de esta área, el Plan de mantenimiento preventivo de equipos de cómputo, ofimática y telecomunicaciones, etc.

Soporte Correctivo: Inventario conformado por 8 activos de información a proteger, entre los que se encuentran el personal encargado de esta área, el taller de soporte correctivo, la evaporadora de refrigeración para la sala de servidores, el Sistema de Alimentación Ininterrumpida (UPS), etc.

1.3 Análisis y evaluación de riesgos

Existen muchas metodologías de análisis y evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla.

Por lo tanto, la metodología que se utilizó fue MAGERIT ya que estando alineada con los estándares más conocidos para la gestión de riesgos como lo son ISO 27001 e ISO 31000, ofrece un método sistemático para analizar los riesgos derivados del uso de las Tecnologías de Información y Comunicaciones (TIC's), para así implementar los controles adecuados que permitan a una organización mitigarlos.

Esta metodología determino el impacto sobre un activo de información, con la pérdida de confidencialidad, integridad y disponibilidad derivado de la materialización de las amenazas junto con las vulnerabilidades que pueden ser explotadas por esas amenazas, se determina la probabilidad de ocurrencia de dichas amenazas, se calcula el riesgo actual frente a las amenazas, y se determina el riesgo residual, resultante luego de que se implementen los controles.

Es necesario precisar que para efectos de este proyecto se determinó el riesgo residual **esperado**, ya que la implementación del Sistema de Gestión de Seguridad de la Información es decisión y responsabilidad de la Dirección del Área de Proceso de Gestión TIC de la Gobernación de Nariño.

El análisis de riesgos es una aproximación sistemática para determinar el riesgo siguiendo unos pasos:

1.3.1 Definición y valoración de Activos de Información. Por medio de un inventario conformado por los Activos de Información a proteger y cuyas dimensiones de valoración para cada uno de estos son: Confidencialidad, integridad y disponibilidad.

1.3.2 Identificación de amenazas a que están expuestos los activos de información. Aquí se identificaron y evaluaron las amenazas que sufren los activos de información de la unidad. Se realizó la identificación de amenazas basándose en la clasificación de MAGERIT. (Ver **Tabla 7. Tipo de amenazas MAGERIT** en el Anexo J – Plantillas y tablas)

Cada una de las categorías presenta una serie de amenazas. (Ver **Tabla 15. Amenazas MAGERIT** en el Anexo J – Plantillas y tablas)

1.3.3 Identificación de vulnerabilidades existentes para los Activos de Información. Se identificaron las vulnerabilidades que pueden ser explotadas por

las amenazas potenciales por medio de inspección visual, listas de verificación, revisión de la información suministrada y hacking ético.

1.3.4 Estimación del impacto. El objetivo fue conocer el alcance del daño producido en la Unidad 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. (ver **Tabla 12. Estimación del impacto** en el Anexo J – Plantillas y tablas)

1.3.5 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. (ver **Tabla 13. Estimación de la probabilidad** en el Anexo J – Plantillas y tablas)

1.3.6 Estimación del riesgo. La estimación del riesgo fue obtenida por medio de la siguiente ecuación matemática:

Riesgo = probabilidad x impacto

Dicha estimación del riesgo se puede interpretar con mayor facilidad por medio de la utilización de la **Tabla 14. Mapa de riesgos** del el Anexo J – Plantillas y tablas.

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: Se evita el riesgo retirando el activo de información.
- Transferir: Se transfiere el riesgo ejemplo por medio de un seguro.
- Mitigar: Se reduce o mitiga el riesgo por medio de controles.

2. ANÁLISIS DE BRECHA

En esta etapa se determinó la brecha con respecto al nivel de madurez de los requerimientos del estándar ISO/IEC 27001:2005 por medio de la verificación de los controles de seguridad de la información que se llevan a cabo en la Unidad.

Este proceso de diagnóstico junto con el análisis y evaluación de riesgos realizados anteriormente, hace posible la definición de nuevos controles para cada uno de los activos de información que lo requieran según su nivel de riesgo.

Al resultado de esta fase se le conoce como “Informe de análisis de riesgos”, que establece el modo de tratamiento y los controles necesarios para cada uno de los activos de información. Con este informe se elaboró el “Plan de Tratamiento de Riesgos”.

2.1 Gestión de riesgos

2.2.1 Plan de tratamiento de riesgos. Contiene una serie de controles y recomendaciones básicas de seguridad para toda la organización que permitió disminuir un alto grado de riesgo.

2.2.2 Establecer normativa para controlar el riesgo. La información es un activo que tiene valor para el Área de Proceso de Gestión TIC y por consiguiente debe ser protegida y resguardada adecuadamente, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo así, a una mejor gestión de la Gobernación de Nariño.

Por lo tanto, se elaboró una Política de Seguridad de la Información que hiso parte de la cultura organizacional del Área de Proceso de Gestión TIC de la Gobernación de Nariño, lo que implico que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

2.2.3 Plan de implementación. Este plan incorporo los aspectos de la implementación del Sistema de Gestión de Seguridad de la Información, incluyendo estrategias descritas para lograr sus resultados, así como acciones de ejecución de las políticas que se diseñaron.

CONCLUSIONES

La aplicación de la norma ISO/IEC 27001 y 27002 fue útil porque proporcionó los mecanismos necesarios para identificar el nivel de madurez en seguridad de la información del Área de Proceso de Gestión TIC. Al igual que definir las recomendaciones que mejor se adapten a la organización.

La información y documentación solicitada al Área de Proceso de Gestión TIC proporcionó los datos necesarios para desarrollar la etapa de análisis y evaluación de riesgos de esta investigación.

Las herramientas de ethical hacking fueron necesarias en la etapa de identificación de vulnerabilidades puesto que permiten verificar y evaluar la seguridad lógica de los sistemas de información, redes, bases de datos y servidores.

Una vez determinado el nivel de riesgo para cada activo de información del Área de Proceso de Gestión TIC se concluyó que para activos de alto y muy alto valor y con un nivel de riesgo intolerable o extremo, el tratamiento recomendado para mitigación de riesgos es la definición de nuevos controles de tipo preventivo y/o correctivo.

RECOMENDACIONES

Es conveniente que el apoyo por parte de la Dirección de la Organización donde se lleve a cabo un proyecto de este tipo se soporte mediante un documento escrito que especifique los niveles de acceso a la información e instalaciones de procesamiento para facilitar el ingreso y obtención de la documentación.

Para un adecuado manejo del inventario de activos de información, se recomienda organizarlo por áreas o dependencias que conforman el Proceso de Gestión TIC.

Para la identificación de amenazas es importante revisar el Libro II – Catálogo de Elementos de MAGERIT que suministra una serie de tablas donde se indican las amenazas que pueden afectar determinados tipos de activos de información.

Ejecutar una evaluación de las políticas de seguridad de la información semestralmente, que posibilite mantenerse conforme a las necesidades del Área de Proceso de Gestión TIC mediante la aplicación de auditorías internas.

MAGERIT es útil para las organizaciones que inician con la gestión de seguridad de la información, ya que permiten enfocar esfuerzos en los riesgos que pueden ser más críticos.

MAGERIT proporciona un conjunto de amenazas por cada tipo de activos de información que facilitan la identificación de los riesgos y vulnerabilidades que puedan presentarse sobre estos.

BIBLIOGRAFÍA

CADME, Christian y DUQUE, Diego. Auditoría de seguridad informática ISO 27001 para la empresa de alimentos “Italimentos CÍA. LTDA.”. Tesis previa a la obtención del título de Ingeniero de Sistemas. Cuenca. Ecuador: Universidad politécnica salesiana, 2012.

LLERENA, Rafael y GUERRA, José. Diagnóstico del estado de los SGSI con la aplicación de un software en las instituciones de Educación superior de san juan de Pasto. Tesis previa a la obtención del título de Ingeniero de Sistemas. Pasto. Colombia: Institución universitaria CESMAG, 2009.

AREA DE PROCESO DE GESTION TIC. Manual especifico de funciones y competencias laborales. Pasto: Gobernación de Nariño, 2011.

NETGRAFIA

BACKTRACK. [en línea] Disponible en internet. http://es.wikipedia.org/wiki/BackTrack. [citado junio de 2018].

CONFIDENCIALIDAD DE LA INFORMACIÓN. [en línea] Disponible en internet. http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html [citado marzo de 2018].

¿Cuál es el mejor estándar de administración de riesgo para las TI? [en línea] Disponible en internet. http://www.emb.cl/gerencia/articulo.mvc?xid=1301. [citado abril de 2018].

DECRETO 1377 DE 2013. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [citado mayo de 2018].

DECRETO 2693 DE 2012. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198. [citado mayo de 2018].

EL PORTAL DE ISO 27001 EN ESPAÑOL. [en línea] Disponible en internet. http://www.iso27000.es/iso27000.html. [citado marzo de 2018].

ISO 27002. [en línea] Disponible en internet. http://iso27002.es/. [citado marzo de 2018].

LEY 1341 DE 2009. [en línea] Disponible en internet. http://www.mintic.gov.co/portal/604/w3-article-3707.html. [citado mayo de 2018].

LEY ESTATUTARIA 1581 DE 2012. [en línea] Disponible en internet. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [citado mayo de 2018].

LEY 1273 DE 2009. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. [citado mayo de 2018].

LEY ESTATUTARIA 1266 DE 2008. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488. [citado mayo de 2018].

LEY 603 DE 2000. [en línea] Disponible en internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960. [citado junio de 2018].

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. [en línea] Disponible en internet. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_ metodo.pdf. [citado abril de 2018].

PARÁMETROS FUNDAMENTALES PARA LA IMPLANTACIÓN DE UN SGSI SEGÚN ISO 27001:2005. [en línea] Disponible en internet. http://www.slideshare.net/jhonny14/iso27001-norma-e-implantacion-sgsi. [citado marzo de 2018].

SEGURIDAD INFORMÁTICA. [en línea] Disponible en internet. http://seguridadinformaticaufps.wikispaces.com/. [citado abril de 2018].

SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [en línea] Disponible en internet. http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html. [citado mayo de 2018].

ANEXOS

Los anexos del presente proyecto se encuentran almacenados en la carpeta general “ANEXOS” que acompaña este documento.