FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DEL INTERIOR

AUTOR

MATTHAEUS LEONARDO MARTEN ALAVA

AÑO

2019

FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DEL INTERIOR

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información

Profesor Guía

Msc. Iván Patricio Ortiz Garcés

Autor

Matthaeus Leonardo Marten Alava

Año

2019

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo Propuesta metodológica para la gestión de riesgos de la infraestructura tecnológica del Ministerio del Interior, a través de reuniones periódicas con el estudiante Matthaeus Leonardo Marten Alava, en el semestre 201920, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Iván Patricio Ortiz Garcés
Magister en Redes de Comunicaciones
C.C.:0602356776

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Propuesta metodológica para la gestión de riesgos de la infraestructura tecnológica del Ministerio del Interior, del Matthaeus Leonardo Marten Alava, en el semestre 201920, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

William Eduardo Villegas Chiliquinga
Magister en Redes de Comunicaciones
C.C.: 1715338263

DECLARACIÓN DE AUDITORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

Matthaeus Leonardo Marten Alava

C.C.:1719058933

AGRADECIMIENTO

Agradezco principalmente a Dios, por darme la oportunidad de estudiar y por brindarme las herramientas necesarias, también doy gracias mis padres por
nunca dejarme solo y ayudarme a cumplir mis objetivos.

DEDICATORIA

Quiero dedicar este trabajo especialmente a mi mamá Prissilla, mi papá Leonardo y a mis dos lindas hermanas Heliana y Ananda, son lo más importante que tengo y siempre son mi motivación para cumplir mis metas, espero siempre hacerlos sentir orgullosos.

RESUMEN

El principal objetivo del trabajo de investigación es realizar una propuesta metodológica para gestionar los riesgos tecnológicos en el Ministerio del Interior entidad del estado ecuatoriano. Esta nace de la necesidad de cumplir con las obligaciones que cuentan las instituciones públicas con la Secretaria Nacional de Administración Pública, misma que exige que se establezca una metodología de gestión de riesgos que cumpla con parámetros establecidos y que permita aplicar las técnicas de control de forma adecuada.

Para cumplir el objetivo principal se realizará una evaluación de los diferentes estándares internacionales de control de riesgo tecnológico y a su vez revisar los requerimientos que solicitan las entidades reguladoras nacionales, con la finalidad de realizar una comparación entre los estándares.

Posteriormente se realizará un levantamiento de información sobre los activos de la institución y de los posibles riesgos que pueda afectar infraestructura tecnológica del Ministerio del Interior, mismo que nos permitirá identificar, analizar y priorizar según corresponda los diferentes eventos.

Por último, teniendo en cuenta el estudio realizado se elaborará una propuesta que permita plantear soluciones, controlar, mitigar y evaluar los riegos.

ABSTRACT

The main goal of this investigation is to implement a risk management methodology for the technological infrastructure of the Ministerio del Interior of Ecuadorian government. This necessity was born from the necessity to fulfill obligations that each public institution has with the Ministerio de Telecomunicaciones MINTEL which demands that they should have a risk management methodology that has their own established parameters that allow to apply the appropriate control techniques.

To help accomplish the main goal there will be an evaluation of the different controls of technological risk standards and evaluate the national requirements that the publics institutions must have, for this it will be a comparison between the standards.

To obtain the results wanted a study of the possibly risks of the technological infrastructure of the Ministerio del Interior is needed to be able to identify, analyze y prioritize the different events as they appropriate.

Ultimately, based on the studies a tender that help to find possible solutions, control, mitigate and evaluate risks.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Cada vez que se realizar cualquier actividad en la vida esta provoca un posible riesgo, en el área de las tecnologías de información ocurre lo mismo, por ejemplo, esto ocurre con los procesos tecnológicos, la infraestructura de red, hasta los activos de la empresa, ya que estos pueden estar expuestos a posibles peligros informáticos, por este motivo las entidades buscan métodos de control de riesgos que les ayude a mitigar casi en su totalidad las posibles vulnerabilidades que puedan presentar.

Es de suma importancia tener en cuenta que cada año la tecnología realiza avances importantes que rápidamente suelen ser adaptadas por las empresas alrededor del mundo, por lo tanto, esto provoca que las entidades busquen una forma segura de acoplarse a estas mejoras y que a su vez garanticen su eficiencia y el cuidado de su información.

También ocurren los casos en que solventan ciertas necesidades con soluciones tecnológicas las cuales permiten mejorar diferentes procesos, esto provoca que tecnología se vuelva una parte fundamental de una organización para que sea exitosa, pero al mismo tiempo abre una posibilidad de que se sufra un ataque informático, es decir, motivo por el cual es importante mantener las estrategias de seguridad actualizadas, así también como las técnicas de control para evitar se dañe la integridad de la información.

Para las entidades públicas estas requieren cumplir ciertos parámetros marcados por el Secretaria Nacional de Administración Pública y por el Ministerio de la Política, este último que regula a las carteras del estado utilizando el Esquema Gubernamental de Seguridad de la Información EGSI el cual nos indica que: “la evolución de las tecnologías de la Información y comunicación han obligado al

gobierno tomar en cuenta métodos de protección a la información con la finalidad de crear confianza en el ciudadano ecuatoriano, todo con el fin de mitigar las vulnerabilidades informáticas". (Secretaría nacional de Gestión de la Política, 2017)

Como se mencionó anteriormente la seguridad informática toma un rol importante en las entidades de Administración Pública que dependen de la Función Ejecutiva, por lo tanto, se recomienda: acoger políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad la seguridad de la información que se genera". (Secretaría nacional de Gestión de la Política, 2017)

Unos de los principales estándares internacionales como son: la ISO 27005:2012 Técnicas de seguridad para control de riesgo de la información, la ISO 31000: 2012 Gestión de Riesgos, y también en el caso de las normativas nacionales se toma en cuenta la propuesta por el Gobierno Electrónico del Ecuador y su Esquema Gubernamental de Seguridad de la Información EGSI forman parte de la metodología a proponer.

En el caso del Ministerio del Interior no se cuenta con un método actualizado que informe sobre los activos y los posibles riesgos, esto resulta muy preocupante ya que es una entidad importante del estado esta requiere realizar un estudio de cuales son las medidas a tomar para prevenir o cuidarse de los posibles riesgos tecnológicos.

Por lo tanto, el propósito de este documento es solventar esta necesidad realizando una propuesta acoplada a las necesidades de la cartera de estado antes mencionada y mejorar su gestión de seguridad informática de manera positiva.

1.1. Alcance

El presente estudio busca realizar un levantamiento de información sobre los posibles riesgos tecnológicos que pueda presentar el Ministerio del Interior, y establecer una metodología que permita gestionar los posibles riesgos de manera adecuada en base a estándares internacionales y normativas nacionales.

Para logar lo esperado se realizará un análisis de cada estándar para determinar cuál es el mejor para utilizar en el Ministerio del Interior, para definir cuáles son las técnicas que pueden ser aplicadas para los diferentes casos con los que se puedan presentar, también se establecerán prioridades sobre los activos y que procedimiento se debe tomar para atender alguna incidencia.

1.2. Justificación

El Ministerio del Interior es una de las entidades del estado más importantes debido a los diferentes procesos que maneja a nivel nacional, motivo por el cual requieren contar con una metodología de gestión de riesgos tecnológicos acoplada a sus necesidades y que sea funcional permita garantizar los diferentes servicios como son:

- El sistema de antecedentes penales.
- Reclutamiento de Policías
- Registro de Empresas de seguridad
- Sistema SISALEM Sistema integral de sustancias catalogadas sujetas a fiscalización para empresas.

Estos servicios son muy importantes para la ciudadanía y para el trabajo en conjunto con otras entidades como es el caso con la Policía Nacional.

La implementación de estrategias para la gestión de riesgos nos permitirá de alguna manera minimiza el impacto que pueden causar las posibles falencias de seguridad que puedan afectar la confidencialidad, disponibilidad, integridad de la información.

1.3. Objetivo General

Realizar una propuesta metodológica que permita gestionar los riesgos tecnológicos con los que cuenta el Ministerio del Interior del Ecuador, basada en diferentes estándares internacionales como nacionales.

1.4. Objetivos Específicos

- Desarrollar una metodología de riesgos que se encuentran alineadas a las normas de la secretaria nacional de Administración pública.
- Identificar los activos tecnológicos de la Coordinación General de las Tecnologías de Información del Ministerio del Interior y los posibles riesgos que puedan enfrentar.
- Obtener un mapa de riesgos para identificar y priorizar el cuidado de los activos que puedan provocar una paralización de las actividades institucionales.

2. MARCO TEÓRICO

2.1. Seguridad de la Información

Se define a la seguridad de la información como la capacidad de garantizar que los posibles riesgos que afecten a la seguridad de la información sean minimizados, conocidos, asumidos y gestionados, por la organización esto se presenta de una forma documentada, estructurada, repetible, sistemática, adaptada y eficiente a los cambios que puedan producir los riesgos, los avances tecnológicos y el medio de la misma empresa. (ISO International Organization for Standardization, 2014)

Para garantizar los valores antes mencionados se tiene que implementar un sistema de gestión de seguridad de información SGSI, el cual cuida la información, es importante indicar que se denomina información a todo lo grupo de datos organizados que tenga valor para una entidad, esto sin importar la forma que la información se almacenada o transmitida, de la fecha de emisión o de su origen. (ISO International Organization for Standardization, 2014)

Los principales pilares que permiten tener confianza sobre el uso de las tecnologías de la información son:

- Integridad: Permite asegurar la veracidad de los datos, es decir que sean correctos y que no hayan sufrido ninguna alteración en el trayecto de origen a su destino.
- Confidencialidad: Este pilar garantiza de que solo personal autorizado pueda tener acceso a la información.
- Disponibilidad: Certificar que la entidad tenga la posibilidad de acceder al uso de un recurso o de un servicio cuando desee únicamente para el personal que este autorizado.
- Autenticación: Asegurar de la legitimidad del usuario es decir que el usuario mediante una identificación demuestre ser quien dice ser, para de esta forma asegurar que los procesos sean fidedignos. (Hidalgo, Tupiza, & Sánchez, 2017)

2.2. Clasificación de las amenazas en la seguridad informática

Las amenazas informáticas se pueden definir como cualquier evento o situación que afecta a una entidad, e impide que esta pueda desarrollar sus actividades de forma normal, también, se puede decir que estas buscan provocar un mal o un peligro que les permita tomar ventaja de las posibles vulnerabilidades que presenta una organización. Por lo tanto, se puede decir tanto las amenazas y las vulnerabilidades

funcionan de manera conjunta, debido a que en el caso de que no existan vulnerabilidades, las amenazas no pueden surgir efecto dañino a una entidad. (Tarazona, 2007) Las amenazas se clasifican de la siguiente manera:

2.2.1. Amenazas Humanas y posibles ataques

Son las que provienen de personas que las provocan de manera intencionada o no, estas provocan grandes daños tomando ventaja de posibles fallos que pueden presentar los sistemas. En caso de las personas que cuenta con experiencia en el área de las tecnologías tenemos este tipo de atacantes:

- **Hacker:** Es aquel que busca aprender para mejorar su nivel de conocimiento sobre la seguridad de la información, su principal característica es la curiosidad, el objetivo de este es no dañar la información de las entidades sino buscar posibles fallos y de esa manera satisfacer su curiosidad.
- **Cracker:** Persona que cuenta con igual o mejor conocimiento que un hacker, sin embargo, tiene intenciones maliciosas, es decir busca hacer daño a su víctima por algún fin de su propio interés. (Barrientos, 2012)

Es importante considerar que no necesariamente se necesita ser un hacker para efectuar una acción que afecte a los sistemas de información, esto puede ocurrir por desconocimiento o por diversión, entre otros.

Tipos de ataques

Para que los ataques se efectúen se necesita aplicar estrategias o métodos que permitan obtener información, a continuación, se numeraran algunos de los ataques más comunes:

- **Ingeniería Social:** El individuo utiliza su capacidad para comunicarse con las personas para obtener información importante de una empresa, de un

terminal o de una persona, para esto puede utilizar varias estrategias que permitan confundir a las personas, haciéndose pasar por personal técnico, empleado de la compañía o cual quiere otro rol que genere confianza a la persona.

- **Trashing:** Se basa en buscar cualquier tipo de información valiosa, como en el caso de que los usuarios anoten alguna clave de acceso para recordarla y botarla en algún lugar sin tomar cuidado, este papel puede caer en las manos de la persona equivocada. (Barrientos, 2012)
- **Robo:** Pueden ingresar a robar la información directamente en los terminales y guardarla en un dispositivo de almacenamiento. (Barrientos, 2012)
- **Personal Interno:** Es uno de los ataques con menos probabilidad sin embargo puede ocurrir por un abuso de confianza por parte del personal interno, se supone que no debería pasar, pero tiene una pequeña posibilidad.
- **Ex Empleado:** Para este caso suelen ser personas con algún tipo de resentimiento contra la empresa que lo contrato y abusa de su conocimiento sobre las seguridades e ingresa a dañar algún sistema. (Barrientos, 2012)
- **Ingeniería social inversa:** El atacante ofrece ayuda a los usuarios sobre algún inconveniente y este aprovecha la oportunidad para obtener información necesaria para realizar un daño a la persona.

2.2.2. Amenazas Lógicas

Las amenazas de tipo lógicas se pueden encontrar en una gran variedad de programas, los cuales se instalan o ingresan al sistema de alguna manera con una finalidad de tipo maliciosa o también pueden ocurrir con en el caso que se presente un error de compilación de un programa o bug. Las principales amenazas de tipo lógicas son las siguientes:

- **Adware:** Este tipo de amenaza despliega publicidad como ventanas emergentes que parecen en las pantallas principales de los ordenadores. (Barrientos, 2012)

- **Bombas Lógicas:** Fragmento de código de un programa que no se utiliza y no realiza ninguna función hasta el momento en que son activadas, la función de este código no está relacionada con el programa y generalmente su realiza un ataque perjudicial. (Barrientos, 2012)
- **Caballos de Troya:** Se denominan a aquellos programas que se hacen pasar por programas buenos no maliciosos, cuando en realidad son programas malignos. Un ejemplo de este tipo de amenaza ocurre cuando se descarga un programa normal que el usuario desea utilizar, sin embargo, este al ser descargado resulta ser un troyano que un programa que captura todo lo que escribe el usuario en el teclado, esta información puede resultar valiosa para el atacante. (Barrientos, 2012)
- **Gusanos:** Son aquellos que se propagan utilizando las redes y buscan encontrar alguna vulnerabilidad o falla en el sistema operativo de los terminales, para explotar estas falencias y de esa manera realizar alguna acción maliciosa. (Barrientos, 2012)
- **Programa maligno Malware:** Como la palabra lo dice se trata de un Software o archivo de tipo malicioso, su objetivo es insertar gusanos, virus, troyanos o spyware, los cuales buscan conseguir información de una PC o del usuario. (Barrientos, 2012)
- **Phishing:** Consiste en utilizar ingeniería social que les permite obtener información de forma fraudulenta, esto puede ocurrir cuando el atacante también conocido como phisher, se hace pasar por otra persona o empresa, utilizando medio electrónicos haciéndose pasar por personal oficial de la empresa. (Barrientos, 2012)
- **Spam:** Son aquellos mensajes que no se desean recibir y llegan de forma masiva, generalmente llegan a los correos electrónicos, pero también pueden llegar por mensajes de texto a teléfonos móviles. (Barrientos, 2012)
- **Virus:** Son aquellos programas tienen como propósito afectar el funcionamiento de los computadores y en algunos de los casos alterar información, su método de propagación puede ser por el intercambio de

archivos, el intercambio de dispositivos de almacenamiento o por abrir archivos maliciosos, en la mayoría de los casos se activan solos sin intervención de ningún otro usuario. (Barrientos, 2012)

- **Ataques de Autentificación:** Este tipo de ataque se realiza tomando el usuario y contraseña de la víctima o ingresando a sesiones ya establecidas para ingresar al sistema, es decir, el objetivo de este ataque es engañar al sistema. Uno de los ejemplos de este tipo de ataque son Spoofing-Looping, IP Splicing-Hijacking o Net floding. (Barrientos, 2012)
- **Denia lof Service (DoS):** Su principal objetivo es saturar los recursos de la víctima para de esa manera inhabilitar los servicios que brinda. (Barrientos, 2012)
- **Ataques de Modificación de Daño:** Es el tipo de ataque que sin autorización modifica el software o los datos instalados en el sistema de la víctima. De este tipo de ataque tenemos como ejemplo: ataques por vulnerabilidad en los navegadores, ataques mediante JavaScrip, ataques mediante active x entre otros. (Barrientos, 2012)

2.2.3. Amenazas Físicas

La amenaza de forma física son las ocasionadas por el hombre como por la naturaleza del medio físico donde se encuentran los centros computacionales de las organizaciones o entidades. A continuación, tenemos las principales amenazas de forma física:

- **Incendios:** Este tipo de amenaza puede ocurrir por fallas en las instalaciones eléctricas, por el mal uso de combustibles o por la mala manipulación de sustancias peligrosas. Es de suma importancia prevenir los incendios ya que estos pueden causar daños irreparables debido a la facilidad que tiene para destruir los bienes físicos y con esto los archivos que encuentran

almacenados. Se recomienda tomar siempre cuidado con este tipo de amenaza y tener métodos contra incendios y controlar que no ingresen personal no autorizado. (Barrientos, 2012)

- **Inundaciones:** Puede ocurrir en un ambiente que no cuento con respectivo drenaje ni tampoco con una protección adecuada, ya que esto puede provocar que en el momento que ocurra una invasión masiva de agua y no tenga forma de soportar los centros de cómputo causando que estos sean sumergidos en agua y con esto dañar su funcionamiento. (Barrientos, 2012)
- **Terremotos:** Es un fenómeno físico que provoca que la superficie terrestre se sacuda estos pueden llegar a ser tan intensos como aquellos que desploman por completo una estructura de un edificio o leves que no causan ningún efecto. (Barrientos, 2012)
- **Instalaciones eléctricas:** Debido a que se trabajan con elementos que funcionan por medio de electricidad es importante tener en cuenta que se debe tener control sobre los aspectos electrónicos como son: contar con aire acondicionado por el calentamiento de los dispositivos, evitas los picos eléctricos, los ruidos electromagnéticos, un cableado estructurado eficiente, pisos de placas extraíbles y evitar fuertes emisiones electromagnéticas. (Barrientos, 2012)

Estos aspectos son de suma importancia y se deben tomar sus respectivos métodos de control para evitar que ocurran, por lo tanto, tienen que formar para de la metodología de prevención de riesgos y con esto prevenir los posibles daños de la información.

2.3. Normativas Nacionales.

En el Ecuador no se cuenta con una normativa netamente nacional, es decir, nos basamos en las normativas Internacionales más utilizadas como son ISO27000 y el ISO31000 todas gestionadas y acopladas a nuestro entorno por el INEN (Servicio

Ecuatoriano de Normalización). Adicionalmente, la Secretaria Nacional de Gestión de la Política propone ciertos parámetros que tienen que cumplir las instituciones públicas y esto se lo define en el EGSI (Esquema Gubernamental de la Seguridad de la Información).

2.3.1. Esquema Gubernamental de Seguridad de la Información EGSI

El gobierno ecuatoriano por medio de la Secretaria Nacional de Administración pública considera que las TIC son herramientas imprescindibles para el desempeño de institucional e interinstitucional, por lo tanto, es de suma importancia contar con una gestión de seguridad informática que trabaje de forma eficaz y eficiente, motivo por el cual se emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación. (Secretaría nacional de Gestión de la Política, 2017)

La comisión antes mencionada realizo su respectivo análisis de la gestión de Seguridad de la Información en las Instituciones Públicas, determinando que es una necesidad aplicar normas y procedimientos para fomentar la seguridad de la información, e incorporar la cultura y procesos institucionales la gestión permanente de la misma. (Secretaría nacional de Gestión de la Política, 2017)

El EGSI está basado en la norma técnica INEN ISO/IEC 27002 para la Gestión de la Seguridad de la Información dirigido directamente para las Instituciones de la Administración Pública Central.

Consiste en establecer un grupo de indicaciones y que estas sean prioridad para la Gestión de la Seguridad de la Información, que garanticen la seguridad y confianza, y generar una metodología de mejora constante para las entidades de la

administración pública Central, Institucional y dependiente de la función ejecutiva (APCID). (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018)

Este esquema gubernamental realiza la evaluación de la siguiente manera:

- Fase 1: Implementación de 126 hitos prioritarios
- Fase 2: Implementación de hitos no prioritarios.
- Evaluación EGSI: Implementación de fase 1 y fase 2.

Para la calificación de estas fases se utilizarán tres parámetros los cuales son:

- Documentación: Políticas, normas que hayan sido formalmente constituidas.
- Implementación: Emplear lo definido en la documentación.
- Verificables: Mostrar cualquier tipo de evidencia de la gestión como Informes, diagramas de red, reportes, etc.

Un estudio realizado por el mismo MINTEL demuestra la realidad actual de todas las entidades dependientes del estado, de lo cual se obtuvo la siguiente gráfica, mostrando la realidad de nuestro país en relación con la seguridad de la información:

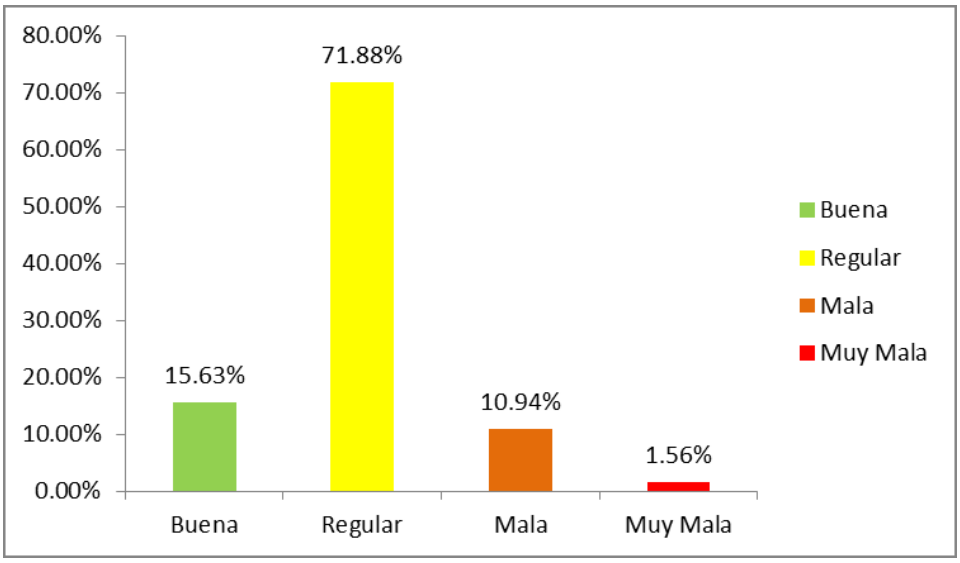

Figura 1. Evaluación de EGSI hasta agosto 2018

Tomada de Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018

Teniendo en cuenta que se tratan de entidades del estado es preocupante los resultados mostrados en la figura 1, ya que más de la mitad tienen una calificación regular, es un problema que llama mucho la intención ya que manejan información delicada del país y tiene que ser una prioridad el resguardar la información de estas entidades.

2.3.2. Marco penal de la seguridad de la información

Para el Ecuador se cuenta la Ley de Comercio Electrónico escrita en el Registro Oficial 557 del 17 de abril del 2002, la cual realizo cambios en el Código Penal, para dar lugar a las infracciones informáticas como son:

- Acceso no autorizado a la información.
- Adulteración de la información.
- Falsificación informática.
- Fraude informático.
- Daños Informáticos.
- Violaciones de derecho a la intimidad.

Posteriormente en agosto 2014, se realizó la creación del COIP (Código Orgánico Integral Penal) el cual amplio la clasificación de los ciberdelitos en el país, según la Fiscalía General del Estado las denuncias reportadas por delitos informáticos en los últimos 4 años luego de las reformas del COIP fueron las siguientes:

La información de la figura 2 es valiosa para comprender en qué estado se encuentra la gestión de seguridad de la información y el uso adecuado de las TIC. Sin embargo, el EGSI está orientado a cuidar la información de las entidades públicas, por lo tanto, a continuación, tendremos las secciones que conforman el Esquema Gubernamental de Seguridad Informática.

FGE
FISCALÍA GENERAL DEL ESTADO
ECUADOR

NOTICIAS DEL DELITO

Art. COIP	DELITOS	PENAS	*2014	2015	2016	2017	**2018	TOTAL
234	ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES	3 a 5 años	54	142	145	221	108	**670**
190	APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	1 a 3 años	507	1283	1049	966	535	**4340**
232	ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS	3 a 5 años	49	78	76	88	50	**341**
173	CONTACTO CON FINALIDAD SEXUAL CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	3 a 5 años	21	80	108	160	81	**450**
230	INTERCEPTACIÓN ILEGAL DE DATOS	3 a 5 años	38	55	83	64	15	**255**
174	OFERTA DE SERVICIOS SEXUALES CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	7 a 10 años		6	9	12	7	**34**
229	REVELACIÓN ILEGAL DE BASE DE DATOS	3 a 5 años	30	24	24	22	21	**121**
* Vigencia del COIP 10 de Agosto 2014. ** Información enero - abril 2018.		TOTALES	699	1668	1494	1533	817	6211

Figura 2. Delitos Informáticos desde 2014 hasta 2018
Tomada de Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018

2.3.3. Política de Seguridad de la Información

Con el paso del tiempo el avance de las tecnologías de la información a tomado un protagonismo primordial en todas las entidades tanto públicas como privadas, motivo por el cual requieren un cuidado minucioso que permita disminuir los riesgos

que conllevan la utilización de soluciones informáticas. En esta sección trataremos brevemente cuales son las obligaciones de las carteras de estado con uno de los entes reguladores de la seguridad de la información como es la Secretaria Nacional de Gestión de la Política.

2.3.3.1. Documento de la Política de seguridad de la información

Consiste en "Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera". (Secretaría nacional de Gestión de la Política, 2017)

Adicionalmente aclara de que las políticas son dependientes de cada institución ya que cada institución realiza diferente tipo de actividades, sin embargo, tienen que estas políticas tienen que estar apagadas a la constitución, leyes y demás normativas legales.

2.3.3.2. Controles y Revisión de la Política

Para garantizar la vigencia de la política de seguridad de la información en la institución, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológica, económico, entre otros. (Secretaría Nacional de Gestión de la Política, 2017)

El documento indica que todo tipo de control adicional al Esquema Gubernamental de la Seguridad de la Información que se desee implementar en las instituciones públicas tiene que ser informado a la Secretaria Nacional de la Gestión de la Política, de igual manera en el caso que exista una excepción y no se pueda aplicar alguna de las directrices del EGSI, tiene que ser comunicado y justificado técnicamente a la cartera de estado antes mencionada el motivo por el cual no se aplica dichas directrices.

2.3.4. Organización de la seguridad de la información

Para que la implementación de técnicas o métodos de control de seguridad de la información es importante contar con una estructura, la cual establezca cuales son los roles y las responsabilidades que tienen los principales responsables en la seguridad informática.

2.3.4.1. Compromiso de la máxima autoridad de la institución con la gestión de seguridad de la información.

Cada institución pública cuenta con una máxima autoridad, misma que cumple el rol de controlar y de supervisar todos los aspectos relacionados a la institución que representa. En la mayoría de los casos estas autoridades suelen delegar responsabilidades a sus funcionarios, sin embargo, es importante destacar que obligación de este representante tomar en cuenta los compromisos que se detallan a continuación.

- Efectuar acompañamiento del estado actual de la aplicación de las normas en el documento.
- Promover la difusión, capacitación y consentimiento del contenido del documento.

- Establecer el Comité de Gestión de la seguridad de la Información y establecer integrantes.
- El comité de la seguridad de la información buscara involucrar a todos los directivos de la institución, adicionalmente tiene que contar con reuniones periódicas las cuales deberán ser justificadas por actas de reuniones.

2.3.4.2. Coordinación de la gestión de la seguridad de la Información

La máxima autoridad de la institución delegara de forma directa a la responsabilidad de organizar, asignar funciones y supervisar al comité de la gestión de seguridad, motivo por el cual requiere cumplir con las siguientes funciones:

- Precisar y conservar la política y reglamentos institucionales particulares en materia de seguridad de la información y encargarse de la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, también el cumplimiento de los empleados de la entidad.
- Dar seguimiento a alguna alteración relevante de los riesgos que afecten a los recursos de información con relación a las amenazas más importantes.
- Obtener información y supervisar la exploración y monitoreo de los incidentes referentes a la seguridad
- Acoger las iniciativas primarias que aumentan la seguridad de la información, según las responsabilidades que tiene cada área involucrada en la gestión de riesgo.
- Acordar y aprobar metodologías y procesos específicos, en base al EGSI relativos a la seguridad de la información.
- Estimar y organizar la puesta en funcionamiento de controles específicos para la seguridad de la información en el caso de nuevas tecnologías o servicios.

- Impulsar la propagación y el soporte a la seguridad de la información dentro de la entidad.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
- Por medio de un documento digital o físico se debe asignar responsables de la información de cada área que conforma la institución.
- Coordinar el abastecimiento constante de recursos económicos, humanos y tecnológicos para la gestión de la seguridad de la información.
- Nombrar de manera formal un funcionario como el Oficial de Seguridad (el funcionario de no debe pertenecer al área de tecnologías) de la Información el cual tendrá la responsabilidad de ser Coordinador de la CSI, por lo que es el encargado en rendir cuentas a la máxima autoridad.
- Designar un funcionario responsable de la seguridad de la información que pertenezca al área de tecnologías de la información y que trabaje en conjunto con el director del área de tecnologías. (Secretaría nacional de Gestión de la Política, 2017)

2.3.4.3. Asignación de responsabilidades de la seguridad de la información

Una vez creado el comité de la seguridad de la información es primordial que se asigne un representante de la Coordinación de Servicios y Componentes de TI el cual estará involucrado directamente con las funciones relacionadas con el EGSI, contara con el cargo de Oficial de la seguridad de la información y sus funciones principales son:

- Establecer procedimientos que permitan administrar y controlar los incidentes de seguridad.

- Implantar y documentar controles para la prevención del acceso no autorizado a información o sistemas, garantizar la integridad de los datos y la disponibilidad de los servicios de la institución.
- Revisar el cumplimiento de los métodos de control de la seguridad información.
- Realizar la coordinación con otras entidades del estado para posibles eventos de seguridad que involucren a ambas entidades.
- Responsable en definir cuantas reuniones sean necesarias para que el comité de seguridad de la información pueda tratar temas importantes, que requieran un tratamiento más detallado (Secretaría nacional de Gestión de la Política, 2017)

Para concluir podemos definir al EGSI como un documento dirigido exclusivamente para las instituciones públicas, está basado en la norma técnica ecuatoriana INE ISO/IEC 27002 para Gestión de Seguridad de la Información, y tiene como objetivo priorizar ciertas directrices, comenzar un proceso que permita realizar controles para mejoras continuas y por último mejorar en general la seguridad de la información en las entidades del estado, y a su vez la confianza de los servidores públicos. (Secretaría nacional de Gestión de la Política, 2017)

2.4. Normativas Internacionales

2.4.1. ISO27001

Esta normativa propone una solución que permite identificar y evaluar todo tipo de amenaza que puedan poner a la información de una organización en peligro, para lograr este objetivo proponen crear un Sistema de Gestión de Seguridad de la información. Otra de sus facetas es plantear estrategias y controles que sean apegadas a las necesidades de la empresa y que permitan disminuir los riesgos de la empresa, su forma de operación se divide en 4 pasos importantes los cuales son:

planificar, hacer, verificar y actuar. Cada uno de estos pasos cuentan con posibles actividades que se clasifican de la siguiente manera en la figura 3. (ISOTools, 2016)

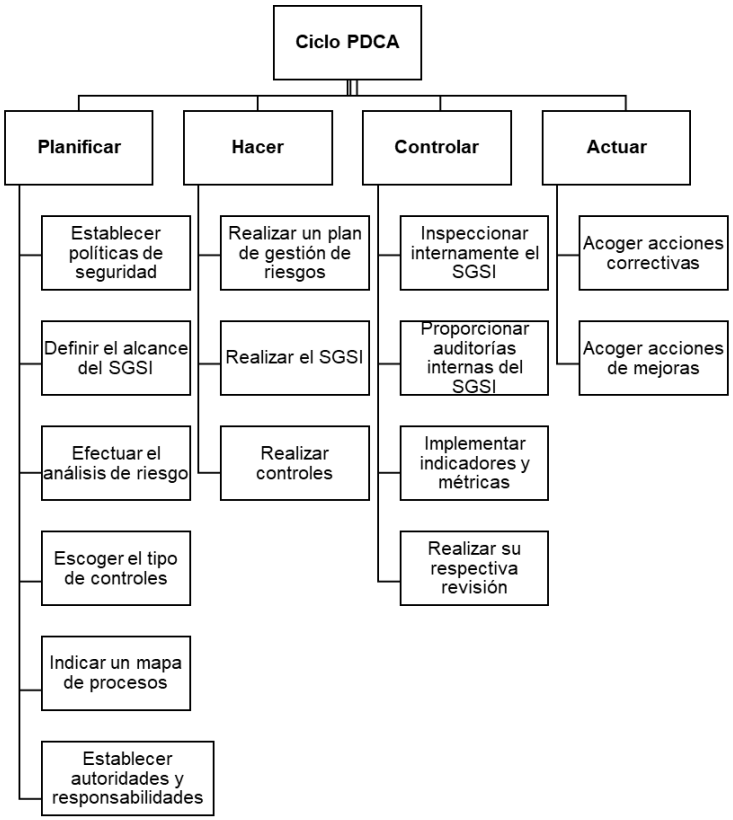

Figura 3. Ciclo PCA para el Sistema de gestión de seguridad informática.

Como se explicó anteriormente uno de los principales objetivos de la ISO 27001 es crear un SGSI y el propósito de este sistema es que se protejan de los posibles riesgos y que se los puede conocer con anticipación, que se puedan aplicar herramientas de gestión y que por último estos sean mitigados, utilizando documentación, estrategias sistemáticas y que también sean estructuradas.

2.4.1.1. Fases de Sistema de Gestión de la Seguridad de la Información

Las fases para elaborar el SGSI son las siguientes:

- **Análisis y evaluación de riesgos**

El principal objetivo de esta fase es calcular el impacto que provocaría el fallo, para esto se tiene que analizar si este fallo afecta la integridad, confidencialidad o integridad de la información, otro de los aspectos a tomar en cuenta es la probabilidad real de ocurrencia, y por último que tipos de consecuencias pueden provocar estos daños. (ISOTools, 2016)

Los pasos por seguir sugerido por el estándar ISO 27001 son los siguientes:

  - Recompilar y ordenar información.
  - Reconocimiento, categorización y apreciación de los grupos activos
  - Reconocimiento y categorización de las amenazas
  - Reconocimiento y evaluación de vulnerabilidades.
  - Reconocimiento y apreciación de los impactos de los riesgos.
  - Valoración y análisis de riesgo.

- **Aplicación de controles**

Para esta sección su principal objetivo es que cada riesgo quede cubierto con algún tipo de control para esto el estándar en su versión del año 2013 cuenta con 113 puntos de control los cuales se dividen en: políticas de seguridad de la información y controles operacionales. (ISOTools, 2016) Depende de cada empresa emplear los controles propuestos por el estándar.

- **Creación de una estrategia para tratar los riesgos.**

Después de que se realiza el análisis del control de riesgo se tiene que tener establecer una estrategia de mejora la cual permitirá que se realice una comparación de las distintas consecuencias de cada riesgo, para esto se necesita

evaluar la criticidad de cada uno de ellos la cual nos permite tener un análisis de las amenazas. Las tres formas de tratar un riesgo son:

- **Mitigar:** Consiste en implantar medidas preventivas con la finalidad de disminuir la probabilidad de ocurrencia o el impacto del fallo.
- **Eliminar:** En el caso de un riesgo critico que pueda alterar todo el funcionamiento de la organización, se tiene que invertir todos los medios para eliminarlo por completo.
- **Trasladarlo:** Esta estrategia permite que se contrate un seguro que garantice que a pesar de los posibles riesgos y se evite una pérdida económica, este trato es importante ya que se tiene que estar listo para cualquier eventualidad que perjudique a la empresa.

Es responsabilidad de la empresa determinar qué tipo de controles necesitan aplicar para cada proceso todo con la finalidad de asegurar la información de la empresa (clasificación de controles en tabla 1, es importante tomar en cuenta que los controles de tipo preventivo son mejores que los de tipo correctivos. Los rangos de control se clasifican de la siguiente manera.

Tabla 1.

Tipos de rango de control de riesgos

Tipos de control de riegos		
Tipo	**Medias de control**	**Periodicidad**
Rango 1	Ninguna	No cuenta
Rango 2	Pocas medidas de seguridad	No cuenta
Rango 3	Controles establecidos	Poco concurrida

Rango 4	Controles establecidos	Concurrencia normal
Rango 5	Controles establecidos	Alta concurrencia

Los controles se realizan de forma periódica y cuenta con un método de mejora continua, el cual permite evaluar la efectividad de los controles aplicados, es decir, se puede determinar si se necesita cambiar el rango del riesgo o si se necesita realizar algún cambio a la metodología utilizada para mitigar los riesgos.

- **Alcance de la gestión**

El alcance nos permite planificar de forma correcta como se va a desarrollar el SGSI, por lo que requiere realizar un levantamiento de información que nos permite determinar: las áreas principales de una empresa que generalmente son aquellas que sus funciones son consideradas fundamentales para cumplir el objetivo principal de una empresa, posteriormente se evaluarán las áreas que vienen en segundo lugar, es decir, aquellas que no manejan información tan crítica pero requieren de un control mínimo y por ultimo las áreas que no cuentan con información delicada y no requieren de una metodología de control. (ISOTools, 2016)

- **Contexto de organización**

El contexto de una organización nos permite determinar cuáles son los contextos internos y los contextos externos en el que se encuentra la empresa, el estándar ISO27001 no cuenta con una metodología específica para determinar el contexto organizacional, sin embargo, se sugiere el método más utilizado para este tipo de estudio y es el análisis FODA el cual consiste en enlistar sus fortalezas, oportunidades, debilidades y amenazas.

- **Partes relacionadas**

Parte del análisis de una organización está definir a las posibles partes relacionadas con la empresa, se requiere identificar quienes están involucrados y cuáles son los roles que cumplen. Se sugiere tener en cuenta estos posibles participantes:

  - Proveedores de servicios de información y el área de tecnologías de la información y la comunicación.
  - Clientes directos.
  - Área de seguridad y jurídicas que están involucrados con los procesos legales.
  - Sociedad en general.

- **Establecer y control de objetivos**

Los objetivos son el principal motivo de la creación del sistema de seguridad de la información porque establecen un punto donde desea llegar, estos objetivos tienen que contar con indicadores para realizar un seguimiento continuo, adicionalmente se recomienda que los objetivos planteados sean medibles y que sean informados a cada uno de los empleados sobre las medidas que se van tomar y que comprendan que es un trabajo en conjunto que requiere de la ayuda de todos para obtener resultados exitosos.

- **Creación de documentación**

Esta sección es de suma importancia para conseguir la certificación ISO, ya que consiste en presentar los parámetros antes establecidos de forma ordenada y en os formatos como: documentos en papel, archivos de texto, hojas de cálculos, archivos de audio y video. Esta documentación tiene que contar con un marco referencial fundamental.

“El organismo ISO exige que se aplique un método sistemático y también contar con una redacción de los procedimientos para su gestión”. (ISOTools, 2016)

- **Auditorías internas y revisión de autoridades**

Básicamente esta sección busca asegurarse de que el funcionamiento de SGSI se encuentra en optimo estado, por lo que se sugiere realizar auditorías cada cierto tiempo. Generalmente se realizan dos auditorías internas:

  - **Gestión:** se realiza un control de la dirección que toma la empresa y el contexto de esta.
  - **Controles:** depende de los tipos de controles sean aplicados por la entidad, hay que recordad que la normativa cuenta con 113 controles sin embargo no todos deben ser aplicados por la empresa, la forma de realizar la auditoria es revisando estos controles de manera anual.

Para obtener una auditoria exitosa se requiere realizar un seguimiento de la auditorias anteriores las cuales permiten revisar como va evolucionando la aplicación de las medidas de control de seguridad, cada auditoria tiene que contar con un alcance ya que de esta manera se puede evidenciar la mejoras o en el caso de que el método utilizado no sea el óptimo se podrá evidenciar los problemas y aplicar nuevos procedimientos.

2.4.2. ISO31000

El estándar ISO 31000 está relacionado directamente con la gestión de riesgos por que su objetivo es ayudar a establecer una estrategia que permita combatir contra las amenazas internas o externas que impidan cumplir con los principales objetivos de la compañía.

La aplicación de las posibles soluciones puede ser aplicadas en cualquier empresa y pueden tratar cualquier tipo de riesgo sin importar el tipo de industria que sea.
Uno de los factores que toma en cuenta el presente estudio son los posibles comportamientos humanos y los factores culturales, por lo que es fundamental realizar diferentes tipos de controles a los diferentes niveles de la organización, por lo tanto, se tiene que establecer a la gestión de riesgos como parte primordial de la gobernanza y el liderazgo de una compañía. (ISO International Organization for Standardization, 2019)

La gestión de riesgos se base tres partes importantes como son los principios de creación y protección del valor, marco referencial de liderazgo y compromiso, por último, tenemos los procesos de tratamiento de riesgo.

2.4.2.1. Principios para la gestión de riesgos

Para contar una gestión de riesgos eficiente se requiere contar con estos elementos, elementos demostrados en la figura 4:

- **Integrada:** Se determinar que la gestión de riesgo tiene que ser integral con todas las actividades de la organización.
- **Estructurada y exhaustiva:** Permite contar con una gestión de riesgo coherente y comparables.
- **Adaptada:** La gestión de riesgo y el marco de referencia tienen que adaptarse tanto a los objetivos de la empresa como los contexto externo e interno.
- **Inclusiva:** Contar con el apoyo de todas las áreas involucradas ayuda a contar con una gestión de riesgos apropiada ya que se toma en cuenta los conocimientos y las necesidades de cada área.

- **Dinámica:** Dentro de una organización pueden ocurrir cambios en su entorno por lo tanto la gestión de riesgos debe anticipar, examinar, averiguar y responder a cualquier tipo de cambio de manera oportuna.
- **Mejor Información disponibles:** Se requiere información oportuna entendible, que este a disponibilidad de todas las áreas de la organización y adicionalmente contar con un repertorio histórico, actual y de las posibles proyecciones de cada entrada.
- **Factores humanos y culturales:** Estos factores influyen directamente en todos los niveles y etapas de la gestión de riesgo.
- **Mejora continua:** Al tratarse de un proceso que funciona de forma continua esto provoca que se adquiera aprendizaje y experiencia a lo largo del tiempo.

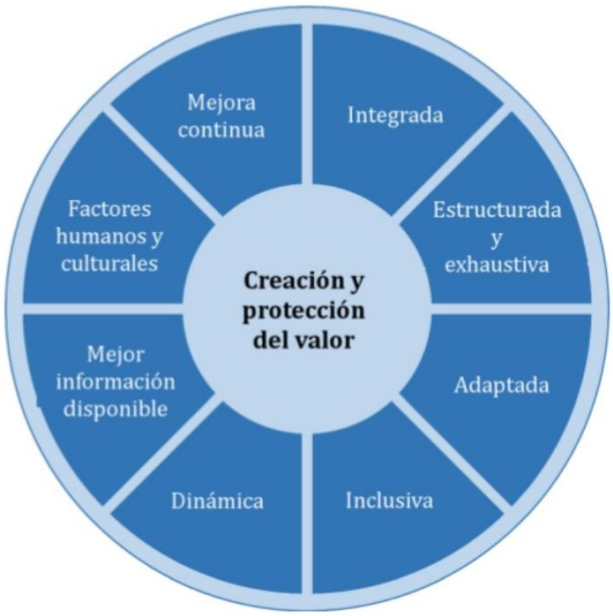

Figura 4. Principios según ISO 31000

Tomada de ISO International Organization for Standardization, 2019

2.4.2.2. Marco de referencia de la gestión de riesgos

Se encarga de apoyar a las entidades en implementar gestión de riesgos sobre todas las actividades involucradas y que tengan funciones significativas de una empresa. El estándar asegura que, si se realiza una integración exitosa con la gobernanza de la organización, motivo por el cual es fundamental contar con el apoyo de las altas direcciones de las entidades". (ISO International Organization for Standardization, 2019)

Como se muestra en la figura 5 el marco referencial tiene los siguientes componentes:

Figura 5. Marco de referencia según ISO 31000
Tomada de ISO International Organization for Standardization, 2019

- **Liderazgo y compromiso:** El objetivo del liderazgo y compromiso es integrar la gestión de riesgo en todas las actividades de la empresa para lograr esto necesitan liderazgo y compromiso de los participantes. Una de las actividades que pueden emplear son las siguientes:
    - Adaptar todos los parámetros del marco de referencia.

  - Publicar políticas que establezcan un plan de acción para la gestión del riesgo.
  - Establecer medios necesarios para la gestión de riesgos.
  - Tener una conjugación de los objetivos y la cultura de la entidad con su sistema de gestión de riesgos.
  - Establecer métricas y clasificadores de riesgo, los cuales permitirán desarrollar las diferentes estrategias a seguir.
  - Establecer un programa de seguimiento sobre los riesgos.
  - Se tiene que confirmar que los riesgos estén acoplados a los objetivos de la organización.
- **Integración:** Se define como un proceso dinámico, que se adapta las necesidades y la cultura de la entidad, su objetivo principal es que la gestión de riesgo no debería estar separada del propósito de la empresa. Por lo que se puede determinar que busca crear una integración entre todas las áreas de una organización, sin importar cuales sean sus actividades, si bien contamos con áreas que tienen finalidades diferentes, todas tienen que estar preocupadas y pendientes en realizar la gestión de riesgos.
- **Diseño:** Para completar un diseño eficiente de la gestión de riesgo se recomienda tener en cuenta los siguientes puntos:
  - Comprender la organización y el contexto de esta.
  - Creación del compromiso para la gestión de riesgos.
  - Atribución de responsabilidades, autoridades, roles y obligaciones para rendir cuentas en la organización.
  - Atribuir recursos para la gestión de riesgos.
  - Establecer métodos para consultas del personal involucrado y promover la comunicación interna con el personal.
- **Implementación:** Consiste en incluir la gestión de riesgos en todas las actividades, decisiones importantes o cambios de contextos sean internos o externos que realiza la organización, esto garantizara el cuidado de la información.

- **Valoración:** Para esta sección se recomienda realizar estudios de forma constante para determinar si los resultados obtenidos son los esperados, adicionalmente nos permite determinar si el marco de regencia es idóneo y ayuda a cumplir los objetivos de la empresa o requiere que se realice algún tipo de cambio.
- **Mejora:** El marco de referencia tiene que estar actualizándose de manera continua para identificar brechas u oportunidades de mejoras esto permitirá que la organización optimizar su marco de referencia de forma idónea, adecuada y con eficacia.

2.4.2.3. Proceso de gestión de riesgos

Para la gestión de riesgos se necesitan aplicar un sistema de políticas y procedimientos, establecer un contexto relacionado con la empresa, sistema de seguimiento para mejoras, repaso a las actividades de comunicación y consultas, programa de evaluación, registro e informe de riesgo, estructura presentada por la figura 6.

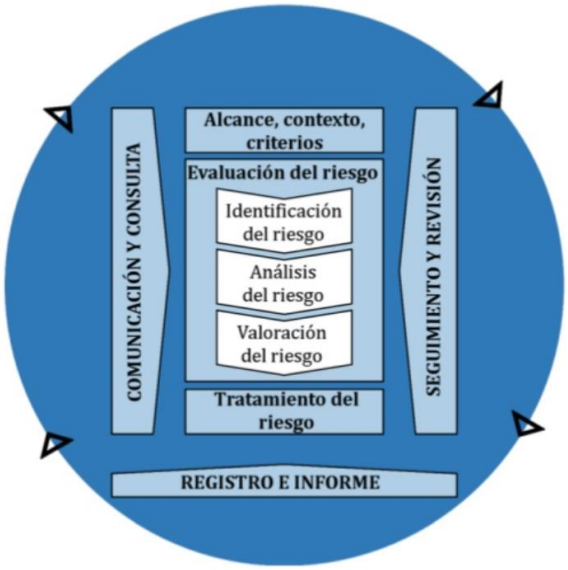

Figura 6. Proceso gestión de riesgos según ISO 31000

Tomada de ISO International Organization for Standardization, 2019

Se recomienda que el proceso de la gestión de riesgos este integrado en todas las actividades de las empresas, debido a que ayudan a cumplir objetivos y permite mejor la seguridad de la empresa.

2.4.2.3.1. Comunicación y consulta.

El principal objetivo de la comunicación es apoyar con conocimiento a las secciones interesadas de la entidad sobre los riesgos y cuáles son los motivos por los cuales se toman ciertas acciones específicas para combatirlos. En el caso de la consulta busca conseguir una retroalimentación o información relevante que mejorará los controles de seguridad. Se sugiere contar con una coordinación intermediaria que organice el intercambio de información y que garantice la confidencialidad de la información brindada y la privacidad de las personas. (ISO International Organization for Standardization, 2019)

Las aspiraciones de aplicar la consulta y comunicación sobre la gestión de riesgos son los siguientes:

- Juntar las áreas más experimentadas para el desarrollo de la gestión del riesgo.
- Respetar y valorar los diversos comentarios o criterios al momento de valorar la importancia de cada riesgo.
- Brindar la información necesaria al momento que se realizan los controles o al momento de tomar una decisión.
- Crear un interés sobre la importancia de los riesgos a todos los involucrados en la entidad.

2.4.2.3.2. Alcance, contexto y criterios.

- **Alcance:** Consiste en definir hasta qué punto llegara la gestión de riesgo, a que niveles se van a aplicar, y que tipo de relación tendrán con los objetivos principales de la entidad.
- **Contexto:** Define un entorno en el que se desea aplicar las medidas de riesgo, generalmente es en el que opera la organización, para lograrlo se necesita analizar el ámbito externo e interno.

  Uno de los resultados que se espera obtener al realizar el análisis del contexto es que exista una relación directa entre la gestión de riesgos y los objetivos principales de la empresa.
- **Criterios:** Busca establecer los tipos de riesgos y el valor que tiene cada uno de los riesgos teniendo en cuenta las obligaciones de la entidad, así como los reflejando los valores, objetivos y recursos. Recordamos que los criterios de riesgo se definen al principio del proceso de la gestión de riesgo, estos criterios no son definitivos y pueden ser actualizados conforme se avanza con el estudio de los riesgos.

2.4.2.3.3. Evaluación del riesgo.

Es el proceso de valora al riesgo, por lo que requiere los diferentes puntos de vista de las partes involucradas, también se requiere la mejor información disponible, es decir, que sea apropiada, pertinente y actualizada. (ISO International Organization for Standardization, 2019)

Los procesos que se realizan en la evaluación de riesgo son:

- **Identificar:** Busca encontrar, certificar y especificar los posibles riesgos que puedan afectar a las entidades y no permitan cumplir sus objetivos.
- **Analizar:** Descifrar las características principales del riesgo, sus posibles consecuencias, probabilidad de ocurrir, eventos, escenarios. El análisis nos

permitirá apreciar que puede haber casos de riesgos que tengan varias causas y consecuencias.

- **Valorar:** Consiste en ayudar la toma de decisiones, realizando una comparación entre los resultados que se obtuvieron en el análisis de riesgos y la identificación de los riesgos, el cual permitirá apreciar si se están tomando las medidas correctivas necesarias o se requiere de otro tipo de control.

2.4.2.3.4. Tratamiento del riesgo.

Consiste en estrategias implementadas para ocuparse de los riesgos, para obtener este resultado se realiza los siguientes procesos

- Exponer y elegir alternativas para el tratamiento del riesgo.
- Planear y poner en funcionamiento el tratamiento del riesgo.
- Valorar la efectividad del tratamiento.
- Resolver si el riesgo es mínimo o aceptable.
- En caso de que no se aceptable se debe crear otro tratamiento adicional.

2.4.2.3.5. Seguimiento revisión.

Debido a que pueden ocurrir ciertos cambios en la gestión de los riesgos se tiene que realizar una revisión continua y con regularidad, para asegurarnos que el diseño implementado funciona de forma eficaz para de esta manera garantizar una calidad en el tratamiento de incidentes.

Se recomienda realizar este tipo de revisiones en todas las etapas del proceso, brindando una retroalimentación y análisis de los resultados obtenidos. (ISO International Organization for Standardization, 2019)

2.4.2.3.6. Registro e informe.

Todo el proceso de gestión de riesgo tiene como resultado toda la información documentada de forma clara el cual nos permitirá informar sobre las actividades, los resultados obtenidos, brindar información para la tomar decisiones y perfeccionar las estrategias para la gestión de riesgo y por último servir como documento que permita realizar una interacción con el personal interesado y también con el personal que tiene como obligación presentar resultados sobre las gestiones de riesgos.

2.4.3. MARGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información creada por el Portal de Administración electrónica del Gobierno de España, pretende poner en funcionamiento el proceso de gestión de riesgo en un contexto de trabajo para que las instituciones gubernamentales empleen decisiones teniendo en cuenta los riesgos que pueden significar el uso de tecnologías de información. (Centro Criptológico Nacional, 2016)

A diferencia de las guías informales, aproximaciones metódicas y herramientas de soporte, es que estas metodologías buscan únicamente determinar si un sistema es seguro o no, sin tomar en cuenta la complejidad de los casos que pueden tener varios elementos que pueden influenciar y agravar la gestión de riesgos, por lo que son soluciones que no son minuciosas y dejan una mucha incertidumbre, esto hace que no sean de confianza total. Por lo tanto, MARGERIT busca ser una mitología que reduzca la incertidumbre y garantice un mejor servicio. (Centro Criptológico Nacional, 2016) Los objetivos principales de este sistema son:

- Crear conciencia sobre las autoridades de las empresas sobre la importancia de la gestión de riesgos y de la necesidad de gestionarlos.
- Presentar un procedimiento sistemático para analizar los riesgos que implican el uso de tecnologías de información y comunicaciones.
- Encontrar y organizar un tratamiento adecuado para contener los riesgos.

El informe de esta metodología utiliza los siguientes puntos:

- **Modelo de valor:** Identificación de la importancia que representan los activos para la entidad y también de la relación entre ellos.
- **Mapa de riesgos:** Relación de las amenazas que se exponen a los activos
- **Declaración de aplicabilidad:** Consiste en establecer si las medidas de seguridad que se aplican son compatibles con los riesgos o no tienen ningún tipo de relación.
- **Evaluación de salvaguardas:** Estudia la efectividad de las salvaguardas aplicadas a los riesgos.
- **Estado de riesgo:** Análisis de las posibles consecuencias después de que se aplicó las salvaguardas antes indicadas.
- **Informe de insuficiencias:** Investigación sobre posibles vulnerabilidades en el sistema, estas se pueden encontrar en posibles salvaguardas que parecen como oportunas sin embargo cuentan con alguna debilidad.
- **Cumplimiento de normativa:** Satisfacción de gestión de los riesgos, se sugiere tener un registro de satisfacción según un formato establecido por esta metodología.
- **Plan de seguridad:** Programa que permite concretar la metodología creada por la organización.

2.5. Información del Ministerio del Interior

Con la finalidad de conceptualizar de mejor manera el contexto de la entidad a estudiar es importante resaltar la misión, visión y los objetivos de la entidad, en este caso el presente trabajo de titulación está relacionado con el Ministerio del Interior del Ecuador, motivo por el cual se presenta la información a continuación.

2.5.1. Descripción del Ministerio del Interior

Ministerio del Interior es una identidad perteneciente al estado ecuatoriano que tiene como finalidad brindar servicios a la ciudadanía de Seguridad Ciudadana y Convivencia Social Pacífica el Ministerio del Interior ha considerado como los valores que permitan transmitir la identidad, compromiso y códigos de comportamiento de funcionarios y empleados, a los siguientes:

2.5.2. Valores del Ministerio del Interior

- Honestidad: Demostrar una conducta recta, honrada que lleva a observar normas y compromisos, así como actuar con la verdad, lo que denota sinceridad y correspondencia entre lo que hace, lo que piensa, lo que dice o que ha dicho. Exige actuar teniendo en cuenta siempre que los fines públicos excluyen cualquier comportamiento que atente directamente contra el interés colectivo.
- Transparencia: Demostrar continuamente los resultados de nuestra gestión pública sin omitir detalle alguno.
- Justicia: Reconocer los derechos que le asisten a cada persona, dando a cada uno lo que es suyo. Rectitud en el actuar ante los demás según sus méritos y dignidad personal- La justicia en tanto valor institucional pretende la equidad y el dar a cada uno según sus méritos aquello que pretenda.
- Respeto: Reconocer, aceptar y valorar las cualidades del prójimo y sus derechos. Implica reconocer en sí y en los demás la condición humana y sus obligaciones.
- Servicio: Brindar la información y atención oportuna de forma amable, eficaz y eficiente a las personas que necesitan de nuestra ayuda y colaboración.
- Compromiso: Actuar con disposición y atención oportuna de forma amable, eficaz y eficiente a las personas que necesitan de nuestra ayuda y colaboración. (Ministerio del Interior, 2019)

2.5.3. Misión y Visión del Ministerio del Interior

Misión:

"Garantizar la seguridad ciudadana y convivencia social pacífica en el marco del respeto a los derechos fundamentales, la democracia y la participación ciudadana con una visión integral que sitúa al ser humano en su diversidad como sujeto central para alcanzar el Buen Vivir". (Ministerio del Interior, 2019)

Visión:

"Ser la institución rectora y co-ejecutora de la política integral de seguridad ciudadana y convivencia social pacífica en el marco del respeto a los derechos, libertades fundamentales y participación ciudadana promoviendo la convivencia y apropiación pacífica de espacios públicos para reducir el delito y erradicar la violencia, garantizando la construcción de una sociedad democrática". (Ministerio del Interior, 2019)

2.5.4. Objetivos Estratégicos del Ministerio del Interior

Los objetivos estratégicos son información provechosa y son pilares al momento de realizar la gestión de riesgos, debido a que todas las estrategias que se apliquen tienen que resguardar el cumplimiento de estos objetivos.

- Incrementar los mecanismos de prevención y protección oportuna al ciudadano ante los riesgos, amenazas y efectos de la inseguridad ciudadana.
- Incrementar las estrategias de permitan anticipar, identificar y neutralizar riesgos y amenazas, actuales o futuras, que afectan la seguridad ciudadana.
- Reducir todos los tipos de conflictividad social que afectan la convivencia pacífica e impacten negativamente sobre la cohesión social.

- Incrementar y fortalecer las capacidades del Estado, en términos de gobernanza, transparencia y calidad de servicio, para hacer frente a los riesgos y amenazas que afecten la seguridad ciudadana.
- Incrementar la eficiencia institucional del Ministerio del Interior.
- Incrementar el desarrollo del talento humano del Ministerio de Interior.
- Incrementar el uso eficiente del presupuesto en el Ministerio del Interior.

3. Análisis de Metodología de gestión de riesgos para el Ministerio del Interior.

Este capítulo busca especificar una estrategia que permita realizar la gestión de riesgos informáticos en el Ministerio del Interior basándonos en requerimientos planteados por el MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información) y por la Secretaría nacional de Gestión de la Política, en el caso de MINTEL presenta el documento de plan de la Sociedad de la información plantea una encuesta realizada por la empresa Deloitte el cual presenta la estadística realizada a 50 empresas internacionales y nacionales, que se desenvuelven en las áreas de salud, financieros, energía y recursos renovables, de lo cual se tomaron en cuenta temas como las brechas de seguridad, componente humano, capacitación, sensibilización entre otros tipos de incidentes, de cual se obtuvo los siguientes resultados", resultados del estudio se puede apreciar en la figura 7. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018):

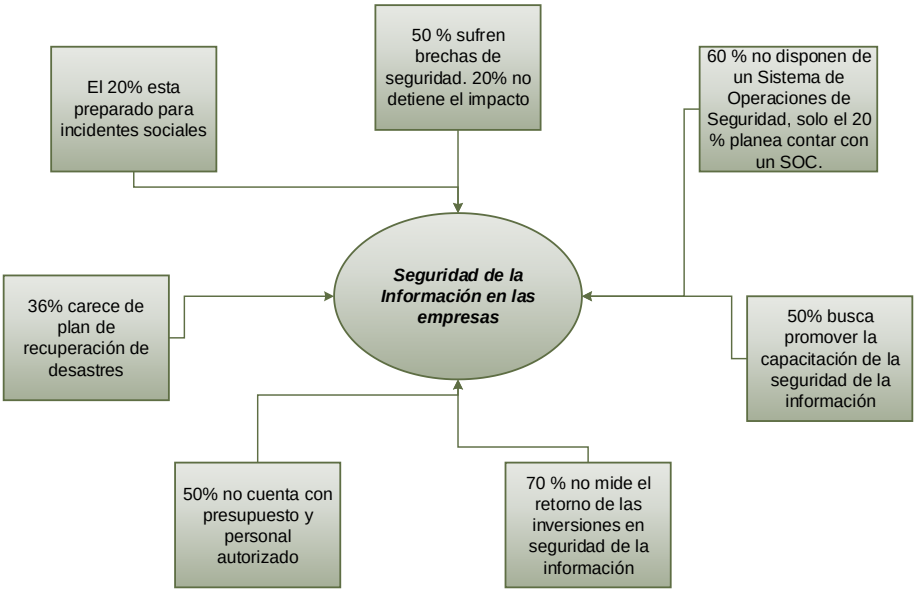

Figura 7. Seguridad de la Información en las empresas

Adaptada de Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018

Adicionalmente se cita un trabajo de investigación realizado por la empresa CEDIA el cual evaluó la gestión de seguridad de la información en 37 universidades (22 públicas y 15 privadas), resultado que se puede apreciar en la figura 8. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018)

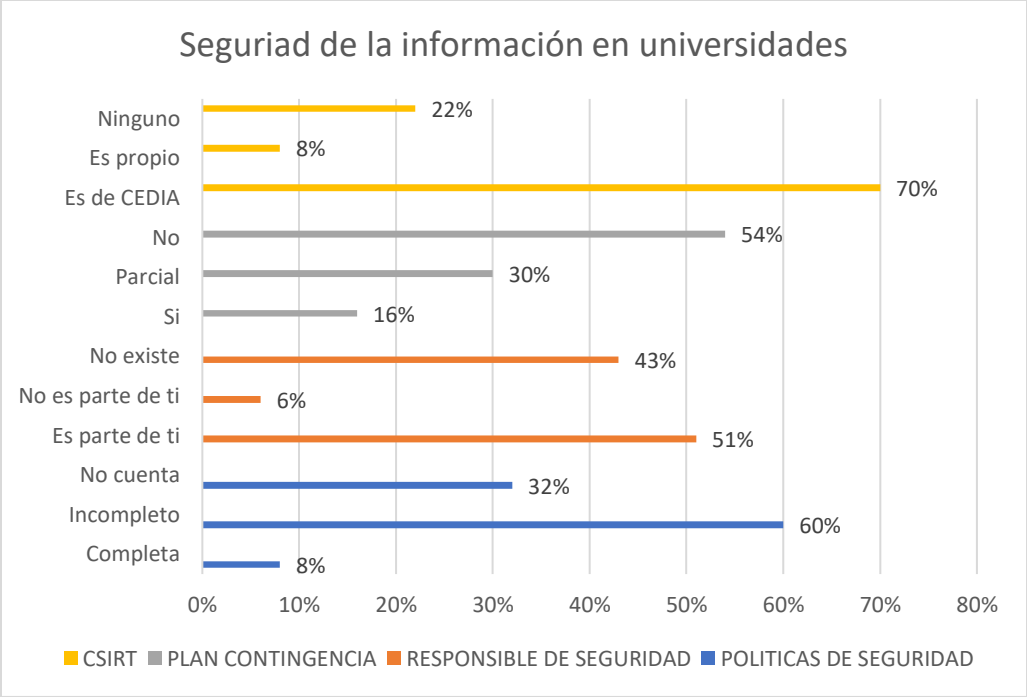

Figura 8. Seguridad de la Información en las universidades
Adaptada de Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018

Teniendo en cuenta los antecedentes planteados por el Ministerio de Telecomunicaciones y Sociedad de la Información tenemos claro que se debe realizar control sobre las TIC motivo por el cual se aplicaran normativas que permitan controlar las posibles amenazas que pueda enfrentar una organización.

3.1. Proceso de Gestión de Riesgos indicaciones principales

En el presente análisis realizaremos el análisis de gestión de riesgos utilizando el estándar INEN-ISO/IEC 27005:2012. Los objetivos principales de esta normativa son:

- Identificar los riesgos.
- Valorizar los riegos según su consecuencia y la probabilidad de ocurrencia.

- La comunicación y entendimiento de las consecuencias de los riesgos y de su probabilidad.
- Definir la como prioridad la gestión de riesgos.
- Establecer cuáles son las acciones empleadas para combatir los riesgos, por ejemplo, la prioridad para reducir la ocurrencia de estos
- Contar con la participación de todas las áreas involucradas al momento de tomar alguna decisión y también informar sobre posibles cambios en el modelo de tratamiento de riesgos.
- El monitoreo de riesgos tiene que ser eficiente y se tiene que realizar de forma periódica.
- Receptara información de forma constante para mejorar el enfoque de la gestión de riesgo.
- Capacitar a los directores y personal involucrado sobre cuáles son las medidas se deben tomar y como se mitigan los riesgos.

El presente proceso de gestión de riesgos se divide en: establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo. Este proceso se lo puede apreciar en el diagrama de flujo en la figura 9.

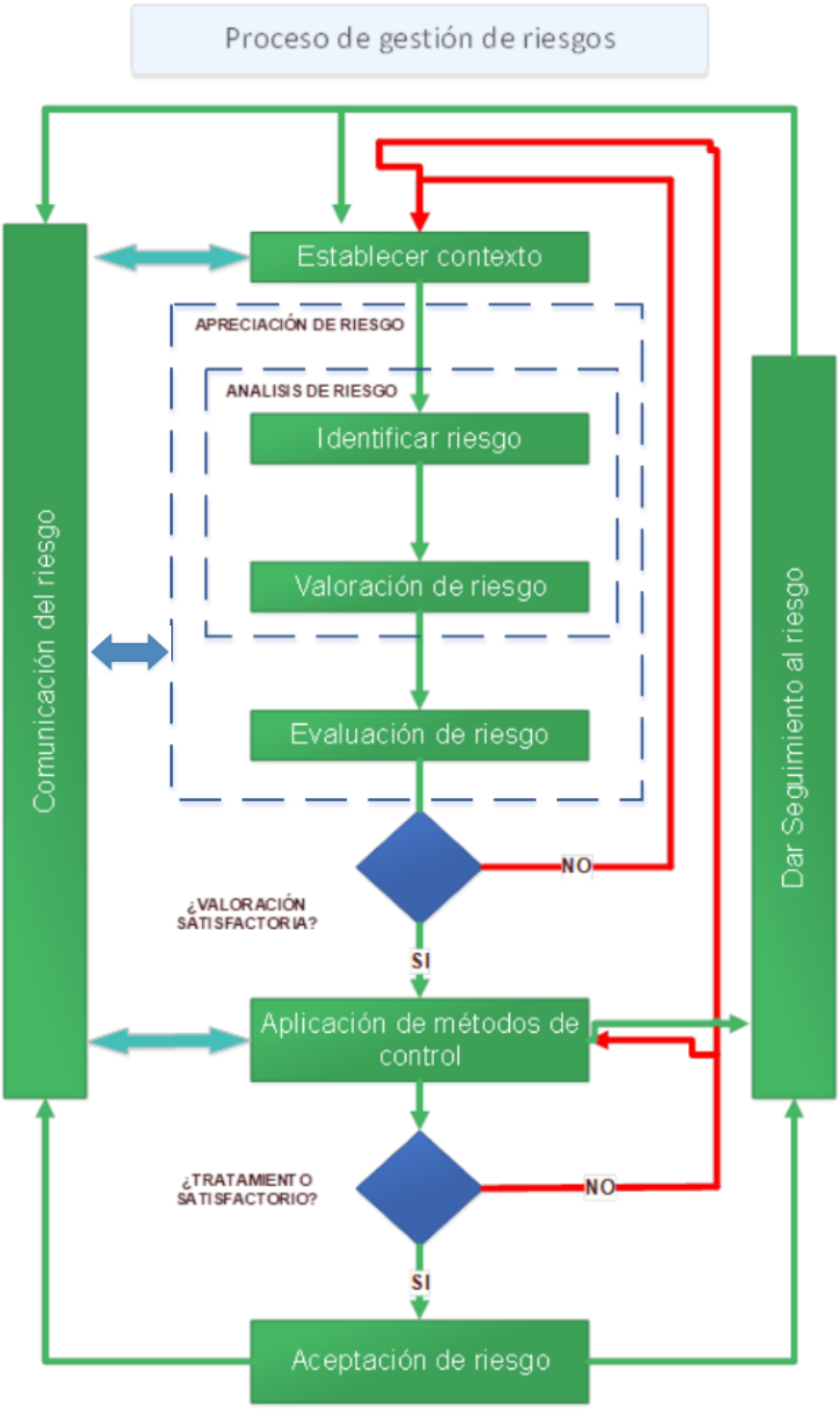

Figura 9. Proceso de gestión de riesgos

Adaptada de Instituto ecuatoriano de Normalización INEN, 2012

El funcionamiento del tratamiento del riesgo no siempre funciona de forma inmediata, lo que asegura su funcionamiento es la valoración correcta de cada riesgo. Para lograr esto se recomienda revisar el análisis del contexto de cada riesgo y de esta manera asegurar los correctos lineamientos que permitan tener un nivel residual de riesgo aceptable. Para que un nivel de riesgo residual sea aceptable tiene que ser aprobado por las autoridades de la entidad, debido a que puede ocurrir casos en que no se pueda mitigar en sus totalidades los posibles riesgos. La gestión de riesgos cuenta con 4 procesos fundamentales y cada uno de estos procesos tienen actividades como se puede apreciar en la tabla 2.

Tabla 2.

Procesos para el SGSI

Proceso de SGSI	**Proceso de gestión del riesgo de la seguridad de la información**
Planificar	Establecer el contexto, Valoración del riesgo, Planificación del tratamiento de riesgo, Aceptación del riesgo
Hacer	Implementación de plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continua del riesgo
Actuar	Mantener y mejorar el proceso de gestión del riesgo de la seguridad de la información

Adaptada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.2. Clasificación de activos

La presente sección tiene como objetivo detallar cuales son los conceptos, tipo de categorías y subcategorías de activos implementará en la metodología de gestión de riesgos.

3.2.1. Activos Primarios para actividades y procesos de negocios

Procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización, son procesos secretos o confidenciales y también son aquellos que nos necesarios para cumplir con requisitos legales.

3.2.2. Activos Primarios de Información

Información vital o estratégica para la ejecución de la misión del negocio, también puede ser de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo o implican un alto valor de adquisición

3.2.3. Activos de soporte

Son aquellos que tienen vulnerabilidades y que son explotables por amenazas cuya meta es deteriorar los activos primarios de procesos y de información. Su clasificación son las siguientes:

- Hardware
- Software
- Redes
- Personal
- Ubicación
- Estructura de la organización.

3.2.4. Categorías y subcategorías de activos

La clasificación de los activos organiza los bienes según su tipo, esto nos ayuda a establecer controles adecuados dependiendo su categoría y además permite optimiza las medidas de control, ya que cada control es diferente para cada categoría. Los tipos de categoría se pueden apreciar en la tabla 3. Con sus respectivas subcategorías.

Tabla 3.

Clasificación de categoría.

Categoría Activo	**Subcategoría Activo**
	Los procesos estratégicos, claves y de apoyo de la institución.

Primario Procesos Negocio	Las normas y reglamentos que son la razón de ser de la institución.
	Planes estratégicos y operativos de la institución y áreas específicas.
Primario Información	Los archivos generados por los servidores públicos, tanto de manera física como electrónica, razón de ser de la función que desempeñan en la institución.
	Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.
	De la operación de los aplicativos informáticos de los servicios informáticos: datos y metadatos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.
	Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad - relación, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba, etc.
	Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.
	De la imagen corporativa de la institución: manual corporativo (que incluye manual de marca y fuentes en formato electrónico de logos), archivos multimedia, tarjetas de presentación, volantes, banners, trípticos, etc.
Soporte Hardware	Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.

	Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.
	Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.
	Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plotter, máquina de fax, etc.
	Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.
	Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.
	Tableros: de transferencia (bypass) de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
	Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.
	Sistemas operativos.

Soporte Software	Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.
	Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, vídeo conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.
	Aplicativos informáticos del negocio.
Soporte Redes	Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.
	Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-ppoint, transceiver, equipo terminal de datos, etc.).
	Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.
	Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.
Soporte Personal	Persona a cargo de la toma de decisiones
	Persona que maneja información sensible o confidencial
	Usuarios externos
	Personal de operación/mantenimiento
	Desarrolladores
	Ambiente externo

Soporte Ubicación	Instalaciones
	Zona
	Servicios esenciales
	Servicios públicos
Soporte Estructura Organización	Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, etc.).
	Inventario referente a los sitios y edificaciones de la institución: planos arquitectónicos, estructurales, eléctricos, sanitarios, de datos, etc.
	Dirección física, dirección de correo electrónico, teléfonos y contactos de todo el personal de la institución.
	De los servicios esenciales: número de líneas telefónicas fijas y celulares, proveedor de servicios de Internet y transmisión de datos, proveedor del suministro de energía eléctrica, proveedor del suministro de agua potable, etc.

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.3. Análisis de valoración de Activos del Ministerio del Interior

3.3.1. Ponderación y definición de confidencialidad

Según la normativa ISO 27005:2012 la valoración de los activos según su confidencialidad se califica según la tabla 4, y su objetivo principal es medir que tan

importante es para la entidad garantizar que ese activo no sea disponible por ninguna persona que no esté autorizado.

Tabla 4.

Ponderación de confidencialidad

Ponderación	**Descripción**
Clasificada (5)	Activo de información confidencial, que está restringido por las leyes o regulado su acceso a funcionarios y servidores de alto nivel, cuyo uso indebido podría afectar la seguridad nacional.
Privada (4)	Activo de información, a la cual la ley tiene prohibido divulgar, ya que perjudica la seguridad institucional, o la intimidad personal, cuya revelación no autorizada pudiera perjudicar sus intereses o dificultar el cumplimiento de su misión
Restringida (3)	Activo de información con un nivel medio de confidencialidad, a la que por razones de interés público o institucional se ha restringido el acceso.
Uso Interno (2)	Activo de información con un nivel bajo de confidencialidad a la que pueden acceder los servidores de la institución; con limitado acceso a nivel externo

Público (1)	Activo de información a la que pueden acceder todas las personas a nivel interno y externo de la institución.

Adaptada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.3.2. Ponderación y definición de integridad

De igual manera nos basamos en la normativa ISO 27005:2012 la valoración de los activos según su integridad se calificará según la tabla 5, y su objetivo principal es garantizar que el activo siempre este bajo salvaguarda es decir debe estar integro y no debe tener ninguna modificación; la información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulación por terceros.

Tabla 5.

Ponderación de integridad

Ponderación	Definición
Muy Alto (5)	Datos inexactos, incompletos o modificados sin autorización, afectaría seriamente la seguridad nacional, generando altas pérdidas monetarias y/o crisis en la ciudadanía.
Alto (4)	Datos inexactos, incompletos o modificados sin autorización, afectaría seriamente las operaciones de la institución, generando altas pérdidas monetarias y/o de imagen institucional.

Medio (3)	Datos inexactos, incompletos o modificados sin autorización, no afectaría seriamente las operaciones de la institución y no dan lugar a altas pérdidas monetarias o de la imagen institucional; daría lugar a soluciones a corto plazo.
Bajo (2)	Datos inexactos, incompletos o modificados sin autorización, afecta muy poco la operación de la institución.
Muy Bajo (1)	Datos inexactos, incompletos o modificados sin autorización no afecta la operación de la institución.

Adaptada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.3.3. Ponderación y definición de Disponibilidad

Basándonos en la normativa ISO 27005:2012 la valoración de los activos según su integridad se calificará según la tabla 6, y busca definir la necesidad de que el activo este accesible para aquellos que estén autorizados en cualquier momento por ejemplo en los casos que se requiere que esté disponible las 24 horas del día.

Tabla 6.

Ponderación de disponibilidad

Ponderación	Descripción
Siempre (5)	La no disponibilidad de la información conlleva a un impacto negativo de índole legal o económica, retrasa sus funciones, o genera pérdidas de imagen severas a entes externos.
Casi Siempre (4)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen alta de la entidad.

Frecuentemente (3)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
Rara vez (2)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
Nunca (1)	La no disponibilidad de la información no afecta la operación normal de la entidad o entes externos, y no conlleva implicaciones legales, económicas o de pérdida de imagen.

Recuperada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.4. Categorización de los riesgos del Ministerio del interior

En la presente sección trataremos los diferentes criterios que se tomaran en cuenta para la categorización de los riesgos que presenta el Ministerio del Interior determinando categorías y subcategorías.

3.4.1. Clasificación según su amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. En la tabla 7 se puede apreciar la clasificación de las amenazas.

Tabla 7.

Clasificación amenazas

Tipo Amenaza	Amenazas
Daño físico	Fuego

	Daño por agua
	Contaminación
	Accidente importante
	Destrucción del equipo o los medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Pérdida de servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado
	Pérdida de suministro de energía
	Falla en el equipo de telecomunicaciones
	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometedoras
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
Fallas técnicas	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información

Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de los datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal
Piratería informática	Piratería
	Ingeniería social
	Intrusión, accesos forzados al sistema
	Acceso no autorizado al sistema
Criminal de la computación	Crimen por computador (por ejemplo, espionaje cibernético)
	Acto fraudulento (por ejemplo, repetición, personificación, interceptación)
	Soborno de la información
	Suplantación de identidad
	Intrusión en el sistema
Terrorismo	Bomba/terrorismo
	Guerra de la información (warfare)
	Ataques contra el sistema (por ejemplo, negación distribuida del servicio)
	Penetración en el sistema

	Manipulación del sistema
Espionaje industrial	Ventaja de defensa
	Ventaja Política
	Explotación económica
	Hurto de información
	Intrusión en la privacidad personal
	Ingeniería social
	Penetración en el sistema
	Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos	Asalto a un empleado
	Chantaje
	Observar información reservada
	Uso inadecuado del computador
	Fraude y hurto
	Soborno de información
	Ingreso de datos falsos o corruptos
	Interceptación
	Código malicioso (por ejemplo, virus, bomba lógica, troyano)
	Venta de información personal
	Errores en el sistema (bugs)
	Intrusión al sistema
	Sabotaje del sistema
	Acceso no autorizado al sistema

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.4.2. Clasificación según su Vulnerabilidad

Se define a la vulnerabilidad como la debilidad que presentan los activos y con facilidad las amenazas se pueden materializar. La clasificación según el área de seguridad a la que pertenece se puede apreciar en la tabla 8.

Tabla 8.

Clasificación Vulnerabilidad

Tipo (Área de seguridad)	**Vulnerabilidad**
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables.
	Punto único de falla
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad de la información
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos

	Ubicación en un área susceptible de inundación
	Red energética inestable
	Ausencia de protección física de la edificación, puertas y ventanas
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes
	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.
	Ausencia de procedimiento de control de cambios
	Ausencia de procedimiento formal para el control de la documentación del SGSI
	Ausencia de procedimiento formal para la supervisión del registro del SGSI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso del correo electrónico
	Ausencia de procedimientos para la introducción del software en los sistemas operativos
	Ausencia de registros en las bitácoras (logs) de administrador y operario.
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos

	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla
	Ausencia de autorización de los recursos de procesamiento de la información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad
	Ausencia de revisiones regulares por parte de la gerencia
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
	Ausencia de esquemas de reemplazo periódico.
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada

Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencia de pistas de auditoria
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlados de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Falla en la producción de informes de gestión

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.4.3. Análisis y Ponderación de Impacto de los riesgos

Se define como la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad, que provoca un cambio adverso en el nivel de los objeticos del

negocio. Por lo tanto, para evaluar el impacto de los posibles riesgos optamos por utilizar la ponderación indicada en la tabla 9.

Tabla 9.

Clasificación y ponderación de Impacto

Tipo Impacto	Impacto	Ponderación	Descripción
Legal	Muy alto	5	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad penal de los implicados.
	Alto	4	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad civil de los implicados.
	Medio	3	Se producen investigaciones administrativas de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad administrativa de los implicados.
	Bajo	2	Se producen investigaciones administrativas a nivel interno de la institución que pueden derivarse en sanciones administrativas graves para los implicados.
	Muy bajo	1	Se producen investigaciones administrativas a nivel interno de la institución que pueden derivarse en sanciones administrativas leves para los implicados.
Credibilidad o Imagen	Muy alto	5	Se afecta frente a los usuarios de la matriz y de las Unidades Desconcentradas de la institución.
	Alto	4	Se afecta frente a los usuarios de la matriz de la entidad.

	Medio	3	Se afecta frente a los usuarios de una o varias de las Unidades Desconcentradas de la institución.
	Bajo	2	Se afecta frente a funcionarios y contratistas de la entidad.
	Muy bajo	1	Se afecta frente al grupo de funcionarios de la entidad
Estratégico u Operativo	Muy alto	5	Se presentaría paro o no operación del proceso.
	Alto	4	Se presentarían intermitencias o dificultades en la operación del proceso
	Medio	3	Se tendrían que realizar ajustes en la interacción de procesos.
	Bajo	2	Se tendrían que realizar ajustes en los procedimientos del proceso.
	Muy bajo	1	Se tendrían que realizar ajustes a una actividad concreta del proceso.

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.4.4. Clasificación y Ponderación de probabilidad

Consiste en establecer la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. La clasificación de la probabilidad de ocurrencia de un riesgo y ponderación se pueden apreciar en la tabla 10.

Tabla 10.

Clasificación y ponderación de Probabilidad

Probabilidad	Ponderación	Descripción	Frecuencia (Referencial)
Muy alta	5	La materialización de la amenaza es inminente, no existen condiciones internas o externas que	Ocurre más de una vez al mes en un servicio

		impidan la materialización de esta.	
Alta	4	La materialización de la amenaza es alta, las condiciones internas o externas son insuficientes para impedir la materialización de esta.	Ocurre más de una vez al año en algún servicio
Media	3	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Ocurre menos de una vez al año en algún servicio
Baja	2	Existen condiciones que hacen poco probable la materialización de la amenaza en el largo plazo.	Ocurre más de una vez cada 5 años en algún servicio
Muy baja	1	Existen condiciones que hacen muy lejana la posibilidad de que la amenaza se materialice.	El evento ocurre rara vez en algún servicio

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

3.4.5. Mapa de riesgo inherente

Para realizar la evaluación de los riesgos, la normativa ISO 27005 propone la utilización del Mapa de riesgo (figura 10) inherente que es la suma de la probabilidad del riesgo (valor que van desde 0-4) y el impacto a la empresa (valor que van desde 0-4) dando como resultado que tipo de inherencia tiene el riesgo, valor que se pondera desde 0-8 y nos permite determinar qué tan importante o tolerables son los vulnerabilidades, según las políticas de aceptación del riesgo.

Es importante tener en cuenta que las medidas del riesgo se califican de la siguiente manera:

- Riesgo alto: 6-8
- Riesgo medio: 3-5
- Riesgo bajo: 0-2

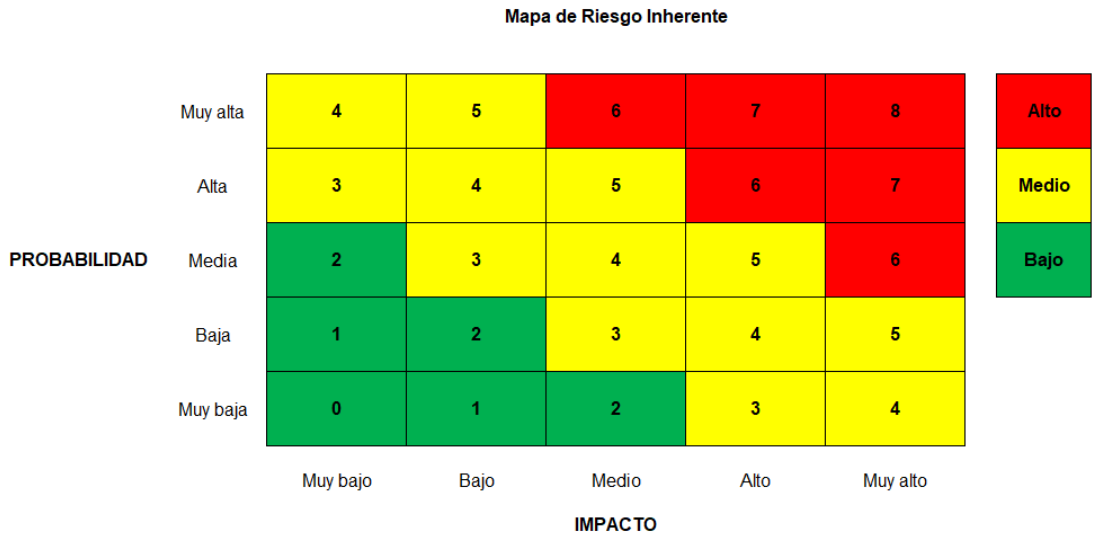

Figura 10. Mapa riesgo Inherente
Adaptada de Instituto ecuatoriano de Normalización INEN, 2012

4. Aplicación de metodología para la identificación de activos y riesgos del Ministerio del Interior.

Tomando en cuenta los criterios antes desarrollados se realizará la aplicación de la metodología planteada sobre los activos y riesgos del Ministerio del Interior.

4.1. Registro de activos

Parte de la gestión de riesgos es que la organización defina su el alcance y entorno, por lo que requiere se considere los aspectos de la organización como son los

objetivos y políticas, estructura y funciones, procesos de negocios, activos, expectativas y restricciones.

En esta sección nos dedicaremos en realizar el levantamiento de información sobre los activos del Ministerio del Interior, ya que los objetivos, estructura y funciones fueron definidos en el marco teórico como información institucional como parte informativa sobre el contexto de la organización.

La metodología establece el formato de presentación de la información el cual tiene que cumplir con los parámetros que se definen en el capítulo 3 de la definición de la metodología de análisis de riesgo.

4.1.1. Información general de activos

Para distribuir la información de forma ordena se aplicará un formato basado en los parámetros de evaluación de activos de la normativa ISO 27005:2012, el objetivo es desarrollar un levantamiento de información generalizado que permita comprender de que se trata cada activo a ver a que proceso institucional pertenece, el formato indicado se puede apreciar en la tabla 11. Para la Coordinación de tecnologías de la Información del Ministerio del interior contamos con dos macroprocesos generales y con los siguientes procesos los cuales son:

- Gestión de Administración de servicios y componentes de TI.
    - Gestión de servicios y componentes de TI.
    - Gestión de seguridad y evaluación Informática.
- Gestión de Diseño e Implementación de TI.
    - Gestión de desarrollo de TI.
    - Gestión de proyectos de TI.

Tabla 11.

Tabla de descripción de activos

No.	Macroproceso	Proceso	Activo		Descripción del Activo	Tipo de Activo	
			ID	Nombre		Categoría	Subcategoría
#	Proceso general al que pertenece el activo (establecido por la entidad)	Proceso o área específica a la que pertenece el activo (por la entidad)	Identificador del activo	Nombre del activo	Breve explicación de que representa el activo	Clase general al que pertenece el activo (por la normativa ISO 27005)	Clase específica a la que pertenece el activo (por la normativa ISO 27005)

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

4.1.2. Calificación según los criterios de seguridad

Basándonos en la normativa ISO 27005:2012 contamos con tres criterios fundamentales para calificar la importancia de los activos para la empresa. Los criterios se califican con una ponderación de 1 a 5 siendo 5 el más importante y 1 el menos importante.

Los criterios de cada ponderación se podrán apreciar en la tabla de calificación de activos, sin embargo, a partir de la sección 3.3.1. hasta la sección 3.3.3. contamos con la definición y la descripción más detallada de cada ponderación de cada criterio. En la tabla 12 podemos apreciar el formato que se utilizará para esta sección.

Tabla 12.

Tabla de tasación de criterios de seguridad

No	Activo	Criterios de Tasación de activos de la información						Importancia del Activo
	ID	Confidencialidad		Integridad		Disponibilidad		
#	#	Nivel de confidencialidad	Detalle del nivel de confidencialidad	Nivel de integridad	Detalle del nivel de integridad	Nivel de disposición	Detalle del nivel de disposición	Resultado de Importancia de activo

Tomada de (Instituto ecuatoriano de Normalización INEN, 2012)

4.2. Matriz de Activos tecnológicos del Ministerio del interior

En la siguiente matriz están enlistados los principales activos de la Coordinación General de las Tecnologías de Información del Ministerio del Interior, el objetivo de esta matriz es mostrar la importancia que tiene cada uno de ellos para la institución. Otro de los objetivos es tener un inventario real de que tipos de activos maneja la institución y sus características principales, esto ser virara como una forma ordenada de mostrar información.

La matriz de activos con sus características se muestra en la tabla 13.

Tabla 13.

Matriz de activos tecnológicos Ministerio del Interior

Matriz de Activos tecnológicos del Ministerio del interior							
No.	Macroproceso	Proceso	Activo		Descripción del Activo	Tipo de Activo	
			ID	Nombre		Categoría	Subcategoría
1	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-001	INTERNET - DATOS	Este servicio permitirá tener acceso a la red de datos institucional, acceso a los recursos y servicios informáticos basados en red y acceso a navegación de Internet.	Soporte Ubicación	Servicios esenciales
2	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-002	CORREO INSTITUCIONAL	Sistema de mensajería electrónico interno y externo	Soporte Software	Paquetes de software o software base de servicios
3	Gestión de Administración de Servicios y	Gestión de Seguridad y	DASC-003	FIREWALL	Sistema de seguridad perimetral para control de	Soporte Redes	Ruteador (router), cortafuego (firewall),

	Componentes TI	Evaluación Informática			ingresos y salidas de internet		controlador de red inalámbrica, etc.
4	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-004	ANTI-VIRUS	Sistema de protección de virus informáticos en la cual buscar y detectar para bloquearlos, desinfectar y prevenir una infección.	Soporte Software	Software de servicio, mantenimiento o administración.
5	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-005	HOSTING (servidores)	Este servicio permite que el usuario de la institución tenga acceso a la infraestructura de TI, alojen los aplicativos como sistemas informáticos, intranet e información en carpetas compartidas de las diferentes unidades administrativas de la institución.	Soporte Software	Paquetes de software o software base de servicios
6	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-006	CABLEADO ESTRUCTURADO	Este servicio permite instalar cableado estructurado de emergencia en red	Soporte Redes	Cables de comunicaciones

					de área local, readecuación de puntos, peinado de cables e instalación de equipos de comunicación		
7	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-007	EQUIPOS DE COMUNICACIÓN	Equipos de comunicaciones para la red interna (SW, AP, ETC)	Soporte Redes	Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-ppoint, transceiver, equipo terminal de datos, etc.).
8	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-008	DOMINIOS	Es cuando se habla de un dominio de Internet (también llamado “dominio virtual”) nos referimos al nombre que se le da a un sitio web para meterlo en el navegador y poder visitarlo.	Soporte Software	Paquetes de software o software base de servicios.

9	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-009	ANTI-SPAM	Es un sistema que sirve para prevenir el correo basura, tanto de entrada como de salida.	Soporte Software	Software de servicio, mantenimiento o administración.
10	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-010	UPS	Sistema de almacenamiento de energía	Soporte Hardware	Tableros: de transferencia (bypass) de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
11	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-011	VIDEO CONFERENCIA	Sistema de Comunicaciones virtuales internas y externas por video en tiempo real	Soporte Ubicación	Servicios esenciales
12	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-001	SISTEMA CONTROL DE OPERATIVOS - SITMINT	Registro de información de los establecimientos intervenidos en operativos realizados por las intendencias y comisarias, Registrar las	Primario Información	De la operación de los aplicativos informáticos de los servicios informáticos.

					solicitudes para la emisión de reportes telefónicos y Generación de permisos de funcionamiento de locales de expendio para comidas, bebidas y centros de diversión		
13	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-002	SISTEMA DE FACTURACIÓN	Facturación electrónica a todos los servicios que requieren la cancelación de rubros al estado por servicios que brinda el Ministerio del Interior	Soporte Software	Aplicativos informáticos del negocio.
14	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-003	SISTEMA E-LEARNING POLICIA NACIONAL	Sistema educativo de la Policía Nacional	Soporte Software	Aplicativos informáticos del negocio.
15	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-004	SISTEMA DE RECLUTAMIENTO EN LÍNEA	Selección de postulación a la Policía Nacional	Soporte Software	Aplicativos informáticos del negocio.

16	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-005	SISTEMA GESTOR DE CERTIFICADOS	Consulta y emisión de certificado de antecedentes penales, Consulta y emisión de certificado de no haber pertenecido a la institución policial, haber sido de baja, revista de comisario.	Soporte Software	Aplicativos informáticos del negocio.
17	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-006	SISTEMA SALDOS DE EMPRESAS SISALEM	Permite controlar las guías y los movimientos de las empresas que utilizan sustancias controladas	Soporte Software	Aplicativos informáticos del negocio.
18	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-007	SISTEMA ADMINISTRACI'ON DE SUSTANCIA CATALOGADAS SIAS	Permite registrara las incautaciones, depósito, destrucción y enajenación de sustancias catalogadas sujetas a fiscalización.	Soporte Software	Aplicativos informáticos del negocio.
19	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-008	SISTEMA SANCIONES ADMINISTRATIVAS	Llevar el control y seguimiento de las personas naturales y jurídicas que han incumplido la ley.	Soporte Software	Aplicativos informáticos del negocio.

20	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-009	SISTEMA XPERTUS	Permite el registro y control del inventario de los bienes, inmuebles, herramientas del MDI	Soporte Software	Aplicativos informáticos del negocio.
21	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-010	SISTEMA GLPI	Sistema de registro y atención a soporte técnico de la Coordinación General de Tecnología de la Información y Comunicaciones	Soporte Software	Aplicativos informáticos del negocio.
22	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-011	SISTEMA MIGRATORIO ECUATORIANO SIMIEC	Registro y control de entradas y salidas de ciudadanos ecuatorianos y extranjeros por las diferentes unidades de control migratorio, puertos, aeropuertos y puntos fronterizos.	Soporte Software	Aplicativos informáticos del negocio.
23	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-012	SISTEMA EMISION DE AUTORIZACIONES E INFORMES DE SEGURIDAD	Permite registrar y almacenar la información de forma centralizada del listado de inmuebles de las instituciones públicas, así como	Soporte Software	Aplicativos informáticos del negocio.

					también almacena los trámites por primera vez generados por cada institución pública.		
24	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-013	SISTEMA COMPAÑIAS DE SEGURIDAD PRIVADA SICOSEP	Permite recopilar la información de las compañías de seguridad privada (datos generales, guardias, armas, puestos de servicio) y la renovación de los permisos de operación de estas con los respectivos acuerdos	Soporte Software	Aplicativos informáticos del negocio.
25	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	GDTI-014	Sistemas GUBERNAMENTALES (QUIPUX, GPR, ESIGEF, eSbyE, Spryn)	Procesa información gubernamental como: Documentación, Proyectos, ingreso y egresos, bienes muebles y rol de pago)	Soporte Software	Aplicativos informáticos del negocio.

4.3. Matriz de Importancia de Activos tecnológicos del Ministerio del interior

La Coordinación General de las Tecnologías de Información del Ministerio del Interior cuenta con los activos mostrados en la sección 4.2., en esta parte mostraremos la importancia de cada uno según la normativa ISO 27005:2012. El resultado de esta matriz es la calificación de la importancia del activo, los resultados obtenidos se pueden apreciar en la tabla 14.

Tabla 14.

Matriz de importancia de activos tecnológicos Ministerio del Interior

Importancia de activos						
No.	Activo		Confidencialidad	Integridad	Disponibilidad	Importancia del Activo de Información
	ID	Nombre				
1	DASC-001	INTERNET - DATOS	Uso Interno (2)	Alto (4)	Casi Siempre (4)	MEDIA
2	DASC-002	CORREO INSTITUCIONAL	Uso Interno (2)	Alto (4)	Casi Siempre (4)	MEDIA
3	DASC-003	FIREWALL	Clasificada (5)	Alto (4)	Casi Siempre (4)	ALTA
4	DASC-004	ANTI-VIRUS	Clasificada (5)	Medio (3)	Casi Siempre (4)	ALTA
5	DASC-005	HOSTING (servidores)	Clasificada (5)	Muy Alto (5)	Casi Siempre (4)	ALTA
6	DASC-006	CABLEADO ESTRUCTURADO	Restringida (3)	Medio (3)	Rara vez (2)	MEDIA

7	DASC-007	EQUIPOS DE COMUNICACIÓN	Restringida (3)	Medio (3)	Frecuentemente (3)	MEDIA
8	DASC-008	DOMINIOS	Privada (4)	Alto (4)	Casi Siempre (4)	ALTA
9	DASC-009	ANTI-SPAM	Restringida (3)	Medio (3)	Frecuentemente (3)	MEDIA
10	DASC-010	UPS	Restringida (3)	Medio (3)	Frecuentemente (3)	MEDIA
11	DASC-011	VIDEO CONFERENCIA	Restringida (3)	Medio (3)	Frecuentemente (3)	MEDIA
12	GDTI-001	SISTEMA CONTROL DE OPERATIVOS - SITMINT	Privada (4)	Alto (4)	Siempre (5)	ALTA
13	GDTI-002	SISTEMA DE FACTURACIÓN	Privada (4)	Medio (3)	Frecuentemente (3)	MEDIA
14	GDTI-003	SISTEMA E-LEARNING POLICIA NACIONAL	Privada (4)	Alto (4)	Siempre (5)	ALTA
15	GDTI-004	SISTEMA DE RECLUTAMIENTO EN LÍNEA	Privada (4)	Alto (4)	Siempre (5)	ALTA

16	GDTI-005	SISTEMA GESTOR DE CERTIFICADOS	Clasificada (5)	Muy Alto (5)	Siempre (5)	ALTA
17	GDTI-006	SISTEMA SALDOS DE EMPRESAS SISALEM	Clasificada (5)	Muy Alto (5)	Siempre (5)	ALTA
18	GDTI-007	SISTEMA ADMINISTRACI'ON DE SUSTANCIA CATALOGADAS SIAS	Clasificada (5)	Muy Alto (5)	Siempre (5)	ALTA
19	GDTI-008	SISTEMA SANCIONES ADMINISTRATIVAS	Privada (4)	Muy Alto (5)	Siempre (5)	ALTA
20	GDTI-009	SISTEMA XPERTUS	Restringida (3)	Medio (3)	Casi Siempre (4)	MEDIA
21	GDTI-010	SISTEMA GLPI	Uso Interno (2)	Medio (3)	Casi Siempre (4)	MEDIA
22	GDTI-011	SISTEMA MIGRATORIO ECUATORIANO SIMIEC	Privada (4)	Muy Alto (5)	Siempre (5)	ALTA

23	GDTI-012	SISTEMA EMISION DE AUTORIZACIONES E INFORMES DE SEGURIDAD	Privada (4)	Muy Alto (5)	Siempre (5)	ALTA
24	GDTI-013	SISTEMA COMPAÑIAS DE SEGURIDAD PRIVADA SICOSEP	Restringida (3)	Medio (3)	Siempre (5)	ALTA
25	GDTI-014	Sistemas GUBERNAMENTALES (QUIPUX, GPR, ESIGEF, eSbyE, Spryn)	Privada (4)	Muy Alto (5)	Siempre (5)	ALTA

4.4. Registro de riesgos

Para el registro de riesgos utilizaremos los parámetros establecidos por la ISO 27005:2012, normativa que fue adoptada por la INEN (Instituto Nacional de Normalización), y establecida como la normativa que se debe acoplar toda institución dependiente del estado junto con los parámetros adicionales que propone el EGSI. Se realizará el registro únicamente de los activos que tienen importancia alta debido a que son prioridad para el Ministerio del interior y se deben prevenir posibles vulnerabilidades que afecten directamente a estos activos.

Adicionalmente se propone el proceso para tratamiento de riesgo mostrados en la figura 11, el cual describe el cuales son los pasos que tomar para solventar los riesgos, se recomienda tomar en cuenta el orden de los procesos para garantizar un control que tome en cuenta los parámetros necesarios y que sea efectivo en su aplicación.

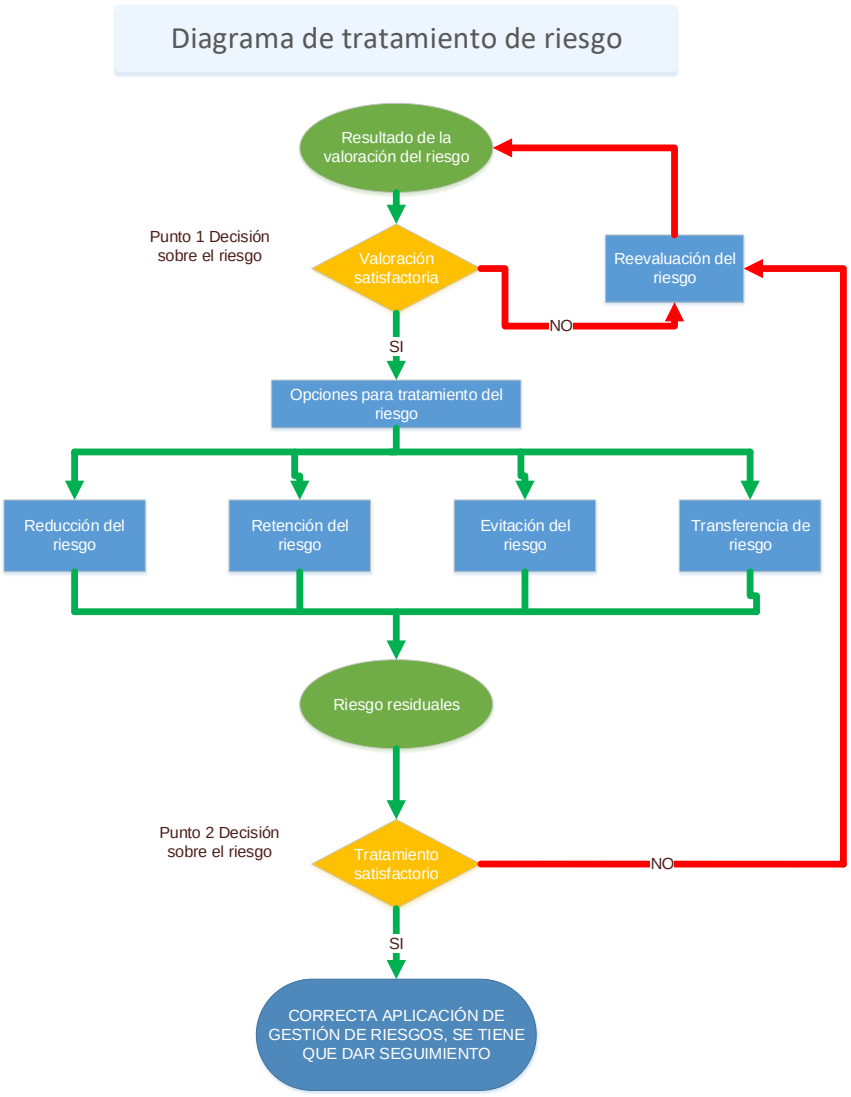

Figura 11. Actividad para tratamiento de riesgo

Tomada de Instituto ecuatoriano de Normalización INEN, 2012

Teniendo en cuenta todas las indicaciones sobre los registros de riesgos se desarrolló un formato que cumpla con todos los requerimientos antes planteados, a

continuación, se mostrará las partes que conforman este levantamiento de información.

4.4.1. Formato de matriz de vulnerabilidad y amenazas sobre los riesgos

Para esta sección contamos con la información sobre los tipos de vulnerabilidad y los tipos de amenaza que puede sufrir el activo, adicionalmente se proporciona una descripción breve de cada uno, en las secciones 3.4.1 y 3.4.2. contamos con la clasificación completa de todas las posibles amenazas y vulnerabilidades que son establecidas por la ISO 27005:2012. En la tabla 15 mostramos el formato de registro de riesgo.

Tabla 15.

Formato matriz de información de riesgos (vulnerabilidad y amenazas).

Información sobre riesgo								
ID de riesgo	Macroproceso	Proceso	Activos de Importancia Alta		Vulnerabilidad		Amenaza	
			ID	Nombre	Tipo	Descripción	Tipo	Descripción
Identificador de riesgo	Proceso general	Proceso o área específica	Identificador del activo	Denominación del activo	Clase de vulnerabilidad	Descripción de vulnerabilidad	Clase de amenaza	Descripción de amenaza

4.4.2. Matriz de riesgo Inherente

“El riesgo inherente se define como el riesgo existente ante la ausencia de alguna acción que la organización pueda aplicar para bajar tanto la probabilidad y el impacto del riesgo. Una vez que se define el riesgo inherente se tiene que definir métodos de control que permitan obtener un riesgo residual”. (Deloitte, 2019)

Se realizará la implementación de controles únicamente de los activos que tienen como riesgo inherente alto, debido a que son prioridad para el Ministerio del interior y se deben prevenir posibles vulnerabilidades que afecten directamente a estos activos.

Motivo por el cual contamos con el formato que muestra en la tabla 16, el cual tendrá como resultado el riesgo inherente por activo.

Tabla 16.
Formato matriz de riesgo Inherente.

Riesgo Inherente						
ID de riesgo	Probabilidad de que ocurra la amenaza		Impacto			Riesgo
	Nivel	Definición	Tipo	Nivel	Definición	
Identificador del riesgo	Nivel de amenaza	Descripción del nivel de amenaza	Categoría de impacto	Nivel de impacto	Descripción de impacto	Resultado de riesgo inherente

4.4.3. Riesgo residual

Se define como riesgo residual al riesgo que continua a presar de que aplicación métodos de controles, generalmente es menor al riesgo inherente, sin embargo, depende de la entidad si este riesgo residual es tolerable.

Por lo tanto, numéricamente se puede definir que le riesgo residual es el riesgo inherente menos le efectividad de los controles aplicados dejándonos una ponderación que definiera si los controles aplicados son efectivos o no. El tipo de formato que se utilizara para el riesgo residual se puede apreciar en la tabla 17.

Tabla 17.

Formato matriz de riesgo residual.

Riesgo Residual								
ID del riesgo	Controles Existentes	Responsable del Control	Frecuencia	Documentación del Control	Evaluación de la efectividad	Riesgo Residual	Tratamiento del riesgo	Requiere Plan de Mejoramiento
Identificador del activo	Describir controles existentes	Personal responsable	Regularidad que se realice un control	Nombre del documento de control	Que tan efectivo es el control	Resultado de riesgo residual	Que acción se va a tomar con el riesgo	Definir si requiere más controles

4.5. Mapa de vulnerabilidades y amenazas sobre los activos del Ministerio del interior

“Se recomienda contar con todos los activos enlistados y con importancia definida debido a que por disponibilidad de autoridades del Ministerio del interior solo se desarrollarán la gestión de riesgos a los activos que tengan importancia alta”. (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, 2018)

Es importante definir que la presencia de una vulnerabilidad no significa que se cause daños por sí mismo, para que ocurra alguna falencia en la seguridad de los activos se requiere que exista una amenaza que explote la vulnerabilidad. Tomar en cuenta que lista de servicios de desarrollo MDI están enlistados en la sección de activos, sin embargo, para no enlistar varias veces las mismas vulnerabilidades se abrevio a una sola lista. Adicionalmente en el caso de que una vulnerabilidad no cuente con una amenaza no se aplicara ningún control. A continuación, en la tabla 18 veremos los resultados los análisis de activos del Ministerio del interior y sus posibles vulnerabilidades.

Tabla 18.

Matriz de vulnerabilidades y amenazas sobre los activos del Ministerio del Interior

Información sobre riesgo									
No.	ID de riesgo	Macroproceso	Proceso	Activos de Importancia Alta		Vulnerabilidad		Amenaza	
				ID	Nombre	Tipo	Descripción	Tipo	Descripción
1	SGRI-001	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-003	FIREWALL	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallas técnicas	Incumplimiento en el mantenimiento del sistema de información
2	SGRI-002	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-003	FIREWALL	Red	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Fallas técnicas	Saturación del sistema de información
3	SGRI-003	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-003	FIREWALL	Red	Tráfico sensible sin protección	Espionaje industrial	Penetración en el sistema
4	SGRI-004	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-003	FIREWALL	Personal	Procedimientos inadecuados de contratación	Fallas técnicas	Mal funcionamiento del software

5	SGRI-005	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-003	FIREWALL	Lugar	Red energética inestable	Daño físico	Accidente importante
6	SGRI-006	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-004	ANTI-VIRUS	Red	Tráfico sensible sin protección	Criminal de la computación	Crimen por computador (por ejemplo, espionaje cibernético)
7	SGRI-007	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-004	ANTI-VIRUS	Personal	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Compromiso de las funciones	Error en el uso
8	SGRI-008	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-004	ANTI-VIRUS	Personal	Ausencia de mecanismos de monitoreo	Acciones no autorizadas	Uso no autorizado del equipo
9	SGRI-009	Gestión de Administración de Servicios y Componentes TI	Gestión de Seguridad y Evaluación Informática	DASC-004	ANTI-VIRUS	Personal	Procedimientos inadecuados de contratación	Fallas técnicas	Mal funcionamiento del software

10	SGRI - 010	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-005	HOSTING (servidores)	Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallas técnicas	Saturación del sistema de información
11	SGRI - 011	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-005	HOSTING (servidores)	Lugar	Red energética inestable	Daño físico	Accidente importante
12	SGRI - 012	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-005	HOSTING (servidores)	Organización	Ausencia de autorización de los recursos de procesamiento de la información	Fallas técnicas	Mal funcionamiento del software
13	SGRI - 013	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-008	DOMINIOS	Organización	Ausencia de planes de continuidad	Criminal de la computación	Acto fraudulento (por ejemplo, repetición, personificación, interceptación)
14	SGRI - 014	Gestión de Administración de Servicios y Componentes TI	Gestión de Servicios y Componentes de T.I.	DASC-008	DOMINIOS	Personal	Procedimientos inadecuados de contratación	Fallas técnicas	Mal funcionamiento del software

15	SGRI - 015	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	Lista de servicios de desarrollo MDI.	SISTEMAS DE INFORMACIÓN DE IMPORTANCIA ALTA EL MINISTERIO DEL INTERIOR	Red	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Fallas técnicas	Saturación del sistema de información
16	SGRI - 016	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	Lista de servicios de desarrollo MDI.	SISTEMAS DE INFORMACIÓN DE IMPORTANCIA ALTA EL MINISTERIO DEL INTERIOR	Red	Arquitectura insegura de la red	Piratería informática	Intrusión, accesos forzados al sistema
17	SGRI - 017	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	Lista de servicios de desarrollo MDI.	SISTEMAS DE INFORMACIÓN DE IMPORTANCIA ALTA EL MINISTERIO DEL INTERIOR	Organización	Ausencia de planes de continuidad	Fallas técnicas	Mal funcionamiento del software

18	SGRI - 018	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	Lista de servicios de desarrollo MDI.	SISTEMAS DE INFORMACIÓN DE IMPORTANCIA ALTA EL MINISTERIO DEL INTERIOR	Software	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Criminal de la computación	Acto fraudulento (por ejemplo, repetición, personificación, interceptación)
19	SGRI - 019	Gestión de diseño e Implementación de TI	Gestión de Desarrollo de TI	Lista de servicios de desarrollo MDI.	SISTEMAS DE INFORMACIÓN DE IMPORTANCIA ALTA EL MINISTERIO DEL INTERIOR	Software	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Fallas técnicas	Incumplimiento en el mantenimiento del sistema de información

Lista de servicios de desarrollo MDI	GDTI 012 - GDTI 014 - GDTI 015 - GDTI 016 - GDTI 017 - GDTI 018 - GDTI 019 - GDTI 022 - GDTI 023 - GDTI 024 - GDTI 25

4.6. Matriz de riesgo Inherente de los Riesgos del Ministerio del interior

Una vez establecido los identificadores de riesgos, se tiene que definir el nivel de probabilidad de ocurrencia de las amenazas determinadas en la sección 4.5. y también el impacto que tiene esta amenaza.

Parte del formato de la matriz es determinar con colores diferentes según el estado del riesgo inherente.

Para compres de mejor manera el nivel del riesgo residual contamos con la figura 12 que muestra la estructura que tiene la tabla 19.

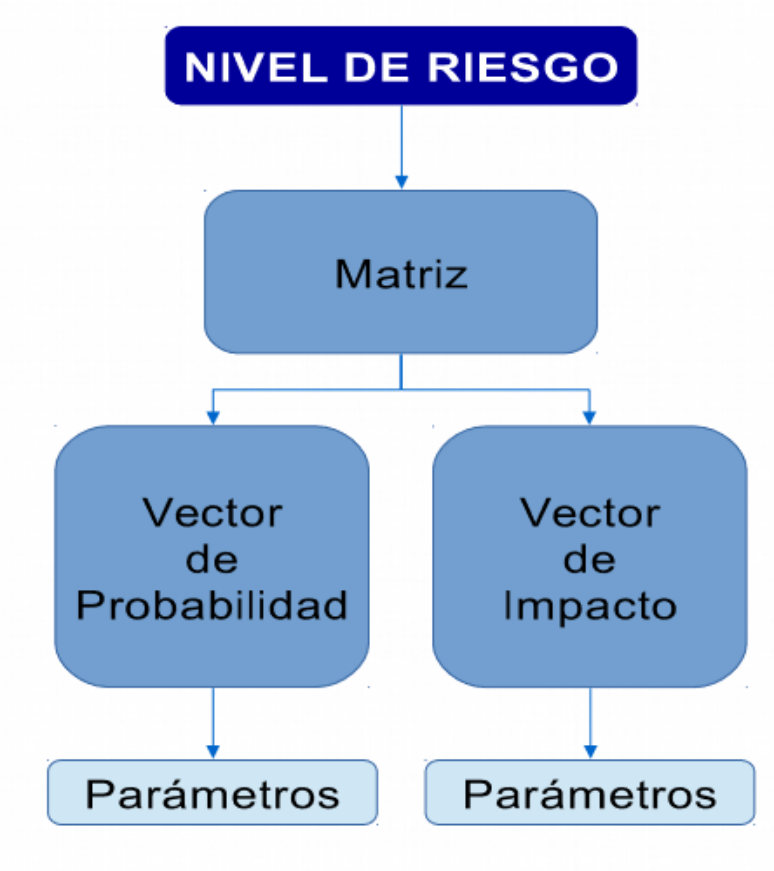

Figura 12. Estructura riesgo inherente
Tomada de Mora, 2016

Tabla 19.

Matriz de riesgo inherente sobre los riesgos del Ministerio del Interior

Riesgo Inherente							
No.	ID de riesgo	Probabilidad de que ocurra la amenaza		Impacto			Riesgo
		Nivel	Definición	Tipo	Nivel	Definición	
1	SGRI -001	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Alto	Se presentarían intermitencias o dificultades en la operación del proceso	MEDIO
2	SGRI -002	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Muy alto	Se presentaría paro o no operación del proceso.	ALTO
3	SGRI -003	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Legal	Alto	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad civil de los implicados.	MEDIO

4	SGRI -004	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Legal	Alto	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad civil de los implicados.	BAJO
5	SGRI -005	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO
6	SGRI -006	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO
7	SGRI -007	Alta	La materialización de la amenaza es alta, las condiciones internas o externas son insuficientes para impedir la materialización de esta.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO

8	SGRI-008	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO
9	SGRI-009	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Legal	Alto	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad civil de los implicados.	BAJO
10	SGRI-010	Alta	La materialización de la amenaza es alta, las condiciones internas o externas son insuficientes para impedir la materialización de esta.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO
11	SGRI-011	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO

12	SGRI -012	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Medio	Se tendrían que realizar ajustes en la interacción de procesos.	MEDIO
13	SGRI -013	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Alto	Se presentarían intermitencias o dificultades en la operación del proceso	MEDIO
14	SGRI -014	Baja	Existen condiciones que hacen poco probable la materialización de la amenaza en el largo plazo.	Estratégico u Operativo	Alto	Se presentarían intermitencias o dificultades en la operación del proceso	MEDIO
15	SGRI -015	Baja	Existen condiciones que hacen poco probable la materialización de la amenaza en el largo plazo.	Estratégico u Operativo	Alto	Se presentarían intermitencias o dificultades en la operación del proceso	MEDIO
16	SGRI -016	Baja	Existen condiciones que hacen poco probable la materialización de la amenaza en el largo plazo.	Estratégico u Operativo	Alto	Se presentarían intermitencias o dificultades en la operación del proceso	MEDIO

17	SGRI -017	Media	Existen condiciones que hacen poco probable la materialización de la amenaza en el corto plazo, pero no son suficientes para evitarlas en el largo plazo.	Estratégico u Operativo	Alto	Se presentarían intermitencias o dificultades en la operación del proceso	MEDIO
18	SGRI -018	Baja	Existen condiciones que hacen poco probable la materialización de la amenaza en el largo plazo.	Legal	Alto	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad civil de los implicados.	MEDIO
19	SGRI -019	Baja	Existen condiciones que hacen poco probable la materialización de la amenaza en el largo plazo.	Legal	Alto	Se producen investigaciones de entes externos a la institución que pueden derivarse en interrupción o afectación de ciertas actividades de la institución con responsabilidad civil de los implicados.	MEDIO

4.7. Matriz de riesgo residual del Ministerio del Interior

La presente matriz utiliza el identificador de riesgo definido en la sección 4.5. y a partir de este aplica los controles sobre las amenazas establecidas en la matriz de la sección 4.6. el resultado de la presente matriz es el riesgo residual el cual define si se necesita realizar un tratamiento extra sobre el riesgo, o los controles aplicados

son suficientes para solventar las posibles vulnerabilidades. Adicionalmente contamos con el resultado de tratamiento de riesgo que define cuatro posibilidades las cuales son:

- **Reducir riesgo:** es la opción más utilizada y consiste en aplicar controles de seguridad que permite mitigar el riesgo.
- **Transferir riesgo:** en el caso de que los controles de seguridad no puedan reducir el riesgo, se recomienda transferir la responsabilidad del solventar el riesgo a otra entidad o área de una organización, por ejemplo, contratar una aseguradora que garantice controlar los posibles riesgos.
- **Aceptar Riesgo:** en el caso de que las acciones necesarias para evitar el riesgo tienen un precio muy elevado, se debe considerar la posibilidad de tolerar este riesgo y convivir con el de formar regular, solo se recomienda minimizar su impacto.
- **Evitar Riesgo:** busca prevenir que ocurra el riesgo, es decir evitar las posibles acciones que se puedan desenvolver en una vulnerabilidad. (ISOTools, 2017)

El desarrollo de la matriz con el formato establecido en la sección 4.4.3. se puede apreciar a continuación en la tabla 19.

Es importante indicar que por medio de un acuerdo de confidencialidad no se puede revelar toda la información relacionada con la gestión de riesgo debido a que no es posible revelar datos que comprometa a la seguridad de la institución o de los funcionarios involucrados, ese es el motivo por el cual no se puede revelar los responsables de la gestión de riesgo, y los documentos de control.

Tabla 19.

Matriz de riesgo residual sobre los riesgos del Ministerio del Interior

Riesgo Residual									
No.	ID del riesgo	Controles Existentes	Responsable del Control	Frecuencia	Documentación del Control	Evaluación de la efectividad	Riesgo Residual	Tratamiento del riesgo	Requiere Plan de Mejoramiento
1	SGRI-001	Contratos de garantías del firewall	INFORMACION RESTRINGIDA	Permanente (Automático)	INFORMACION RESTRINGIDA	Se aplica y es efectivo	BAJO	Aceptar el riesgo	No
2	SGRI-002	Control de accesos a red y a los puertos de comunicaciones	INFORMACION RESTRINGIDA	Permanente (Automático)	INFORMACION RESTRINGIDA	Se aplica y es efectivo	BAJO	Reducir el riesgo	No
3	SGRI-003	Control de puertos, páginas, accesos a Internet en firewall	INFORMACION RESTRINGIDA	Permanente (Automático)	INFORMACION RESTRINGIDA	Se aplica y es efectivo	BAJO	Reducir el riesgo	No
4	SGRI-004	Gestionar Presupuesto	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	BAJO	Reducir el riesgo	No
5	SGRI-005	Gestionar Contratos de mantenimiento preventivo	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Transferir el riesgo	Si
6	SGRI-006	Controles de acceso al internet	INFORMACION RESTRINGIDA	Mensual	INFORMACION RESTRINGIDA	Se aplica y es efectivo	BAJO	Reducir el riesgo	No

7	SGRI -007	Emitir política de seguridad del antivirus y ejecutar	INFORMACION RESTRINGIDA	Mensual	INFORMACION RESTRINGIDA	Se aplica y es efectivo	BAJO	Reducir el riesgo	No
8	SGRI -008	Controlar que todos los equipos no tengan privilegios de administrador o estén atados a un dominio	INFORMACION RESTRINGIDA	Mensual	INFORMACION RESTRINGIDA	Se aplica y es efectivo	BAJO	Reducir el riesgo	No
9	SGRI -009	Gestionar Presupuesto	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	BAJO	Reducir el riesgo	No
10	SGRI -010	Gestionar contrato de mantenimiento Correctivo	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Transferir el riesgo	Si
11	SGRI -011	Gestionar Contratos de mantenimiento preventivo	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Transferir el riesgo	Si
12	SGRI -012	Gestionar proceso de renovación tecnológica que permita solventar la falta de procesamiento de los servidores	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Transferir el riesgo	Si
13	SGRI -013	Asignación de recursos en el Presupuesto para contratación	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No

14	SGRI -014	Gestionar a tiempo la renovación de licencia para no perder el domino y no estar propenso a robos de este.	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No
15	SGRI -015	Realizar monitoreo de servidores	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No
16	SGRI -016	Políticas de uso y de seguridad del internet	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No
17	SGRI -017	Gestionar Presupuesto	INFORMACION RESTRINGIDA	Anual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No
18	SGRI -018	Métodos de autentificación de usuarios, como controles biométricos al entrar al momento de configurar algún sistema.	INFORMACION RESTRINGIDA	Mensual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No
19	SGRI -019	Establecer controles de almacenamiento de información que garanticen el buen uso de los recursos de almacenamiento	INFORMACION RESTRINGIDA	Mensual	INFORMACION RESTRINGIDA	Se aplica, pero no efectivo	MEDIO	Reducir el riesgo	No

4.8. Análisis de resultados

En esta sección revisaremos los resultados obtenidos en el levantamiento de información en el estudio de gestión de riesgos informáticos del Ministerio del interior, se revisara los resultados del levantamiento de información sobre los activos informáticos, el resultado del riesgo de riesgo inherente en los activos de importancia alta, el riesgo residual de la aplicación de controles a las amenazas antes enumeradas, los resultados del tratamiento de riesgo y los procesos que requieren un tratamiento adicional para solventar el riesgo.

4.8.1. Resultado Importancia de activos

En el levantamiento de información sobre la importancia de los activos determinarnos los resultados obtenidos en la figura 13, los cuales demuestran que el Ministerio del interior cuenta con 15 activos con importancia alta y 10 con importancia alta.

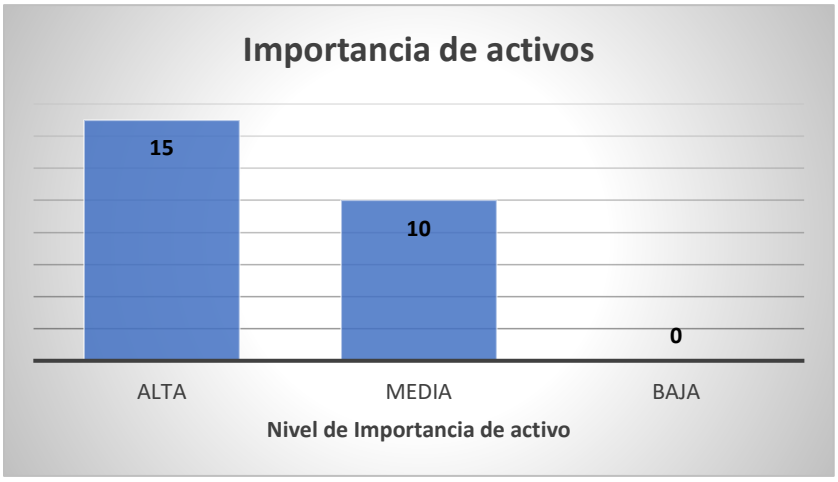

Figura 13. Resultado Importancia de activos

En la Coordinación General de las Tecnologías de Información del Ministerio del Interior se puede apreciar que todos los activos son de importancia media y alta

debido a que comprometen muchas áreas de trabajo y su disponibilidad es fundamental, en virtud del impacto que puede significar para la imagen que proyecta a entes externos o la ciudadanía, adicionalmente afecta directamente a las funciones principales de la entidad, esto es crucial en el caso de los sistemas migratorios o de los sistemas que controlan el uso de las sustancias controladas.

En el caso de los activos con importancia media la mayoría son relacionados con servicios internos que repercuten únicamente para las actividades internas, por lo que no afecta a la imagen de la entidad.

4.8.2. Resultado de Riesgo Inherente

El objetivo de esta sección es apreciar los resultados que se obtuvieron después de realizar el registro del impacto y de la probabilidad de ocurrencia sobre los activos, podemos notar en la figura 14 que casi en su totalidad los riesgos han bajado a nivel medio debido a que la probabilidad de ocurrencia es muy baja, esto provoca que el impacto se contrarreste y permita que el riesgo se reduzca y sea poco probable.

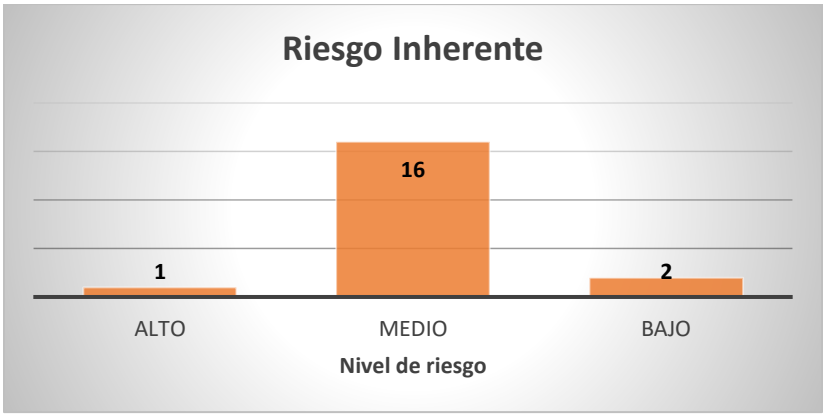

Figura 14. Resultado Riesgo Inherente

4.8.3. Resultado Riesgo Residual

La siguiente parte en el tratamiento de los riesgos contamos con la aplicación de métodos de control los cuales se contrarrestan con el nivel riesgo inherente para dar como resultado el un riesgo residual. La efectividad de los controles es medida según la experiencia a lo largo de los años en el área de Gestión de Seguridad y Evaluación informática del Ministerio del interior, los cuales son favorables en el control de posibles riesgos. En la figura 15 se pueden apreciar los resultados obtenidos.

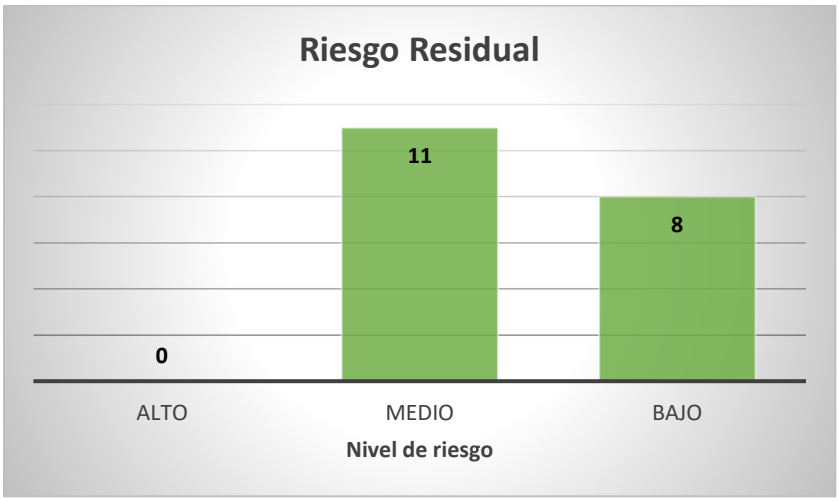

Figura 15. Resultado Riesgo residual

Se erradica en totalidad el riesgo residual de nivel alto ya que es fundamental que los controles sean efectivos, caso contrario se recomendaría seguir aplicando medidas para mitigar en su totalidad los posibles riesgos. Para el caso de riesgo residual medio queda en la entidad evaluar si este nivel de riesgo es aceptable o requiere aplicar más métodos de control permitan bajar el nivel de esta amenaza.

4.8.4. Resultado Tratamiento del Riesgo y sobre la necesidad de un plan de mejoras

Como se planteó en secciones anteriores contamos con cuatro opciones para tratar el riesgo residual, en la figura 16 contamos con una gráfica de forma de pastel que nos muestra el resultado del tratamiento de las amenazas.

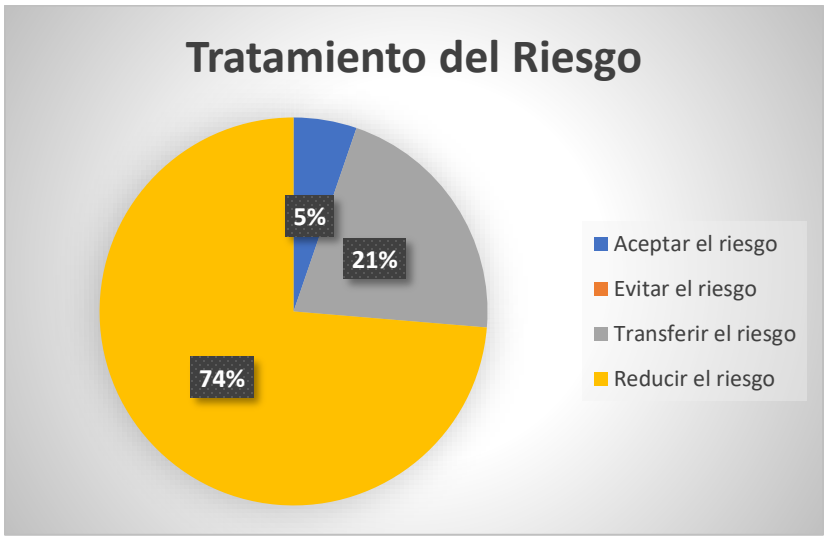

Figura 16. Tratamiento del riesgo métodos más utilizados

La gestión de riesgo busca implementar estrategias que permitan cuidar los activos de las empresas, tratando cualquier tipo de riesgo que los afecte, la reducción de riesgo alcanzo un 74%, un 21% en casos de transferencia de riesgo cuando el tratamiento de riesgo no es competencia de la Coordinación de Tecnologías de la Información y únicamente un 5% de aceptación de riesgo referente a posibles ataques por suplantación de identidad y se permita acceso a los sistemas, es un riesgo bajo y poco probable, pero de igual manera es importante tener en cuenta.

Por otro lado, es importante indicar que no se puede eliminar en totalidad el riesgo, debido a que por más mínimo que sea el riesgo sigue existiendo, una de las soluciones para eliminar el riesgo es evitar las actividades o procesos que sean

propensos a un riesgo, sin embargo, esto depende de los objetivos generales de la entidad si pueden permitirse o eliminar actividades y procesos que tengan riesgo.

En caso de que contemos con un riesgo que no sea aceptable para la entidad la solución es aplicar un plan de mejoramiento, en la figura 17 podemos apreciar que solo cuatro procesos requieren de un plan de mejoramiento.

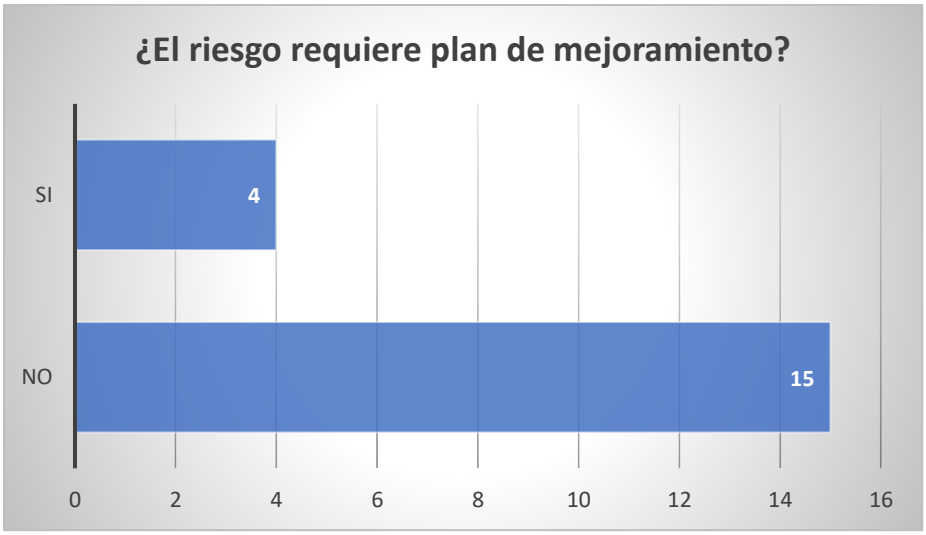

Figura 17. Consulta de procesos que requieren plan de mejoramiento

Los procesos que requieren mejoramiento son relacionados con la gestión administrativa para conseguir presupuesto, o agilidad en los trámites para realizar a tiempo los mantenimientos o en caso de las renovaciones de equipo adquirir los nuevos equipos a tiempo.

4.8.5. Importancia de la gestión de riesgo

Como muestra la figura 18 la gestión de riesgo cumple un papel muy importante en la gestión de tecnologías de la información, continuidad de negocio y la gestión de seguridad de la información, debido a que no siempre se pude controlar los todo lo que ocurre en torno a una organización por lo que es importante realizar un estudio que permita determinar vulnerabilidades o amenazas que puedan perjudicar a las entidades.

Figura 18. Importancia de la Gestión de riesgo
Tomada de Torres, 2016

El parámetro fundamental que se tiene que tener en cuenta al momento de realizar un estudio de gestión de riesgos es que el diagnostico que se obtuvo al realizar al análisis es válido para ese momento especifico en el tiempo. “La gestión de riesgos no es algo estático, esta se tiene que ir actualizando conforme avanzan los años, agregando nuevas amenazas, vulnerabilidades o activos que se puedan presentar en ese periodo de tiempo”. (Torres, 2016)

5. Conclusiones y Recomendaciones

5.1. Conclusiones

Una vez culminado el presente trabajo de investigación, se concluye que la gestión de los riesgos informáticos es un pilar que garantiza un desarrollo integral, confidencial y con tolerancia a fallos, de los procesos principales de las empresas, esto va de la mano con lo eficiente que sean las estrategias implementadas para mitigar los riesgos. De igual manera no hay que olvidar que una empresa que cuida su información da una excelente imagen las otras entidades, sin embargo, como se trata de una entidad pública, uno de sus propósitos es mostrar la mejor calidad de seguridad a todos los ecuatorianos.

Se analizó diferentes estándares relacionados con la seguridad de la información como fueron las normativas internacionales ISO 27000, ISO 31000 y MARGERIT, adicionalmente se examinó la normativa nacional del Esquema Gubernamental de Seguridad de la Información (EGSI) el cual está basado en la norma INEN-ISO/IEC 27005, de los cuales se desarrolló una metodología de gestión de riesgo que cumple con los requerimientos de la Secretaria Nacional de Gestión Pública.

Para el Ministerio del Interior es importante contar con un mapa de activos y de los riesgos que estos puedan presentar, ya que, les beneficiará con el respaldo de tener información que les permitirá desarrollarse sin problema y no tener sanciones administrativas por la falta de gestión en el área de la seguridad informática, debido a que es obligación para las entidades del estado contar con este tipo de estudios.

Debido a que las entidades públicas tienen ciertos parámetros que deben cumplir es complicado innovar en las técnicas de seguridad, en vista de que las entidades reguladores realizan las auditorias en base a las normativa para instituciones públicas, prácticamente exigen se realice los controles orientados únicamente a la

normativa nacional, complicando la aplicación de nuevas técnicas de control de riesgo, no obstante los controles de seguridad adicionales que se apliquen siempre son de mucha ayuda, aunque no es exigencia de los órganos reguladores.

Por otro lado los riesgos que atentan de forma directa a los servicios que brinda el Ministerio del interior son en su mayoría de carácter administrativo, este es el caso de los dispositivos de seguridad perimetral los cuales utilizan licencia para funcionar, sin embargo no siempre cuentan con el presupuesto asignado para la renovación de éstas licencias, dejando la seguridad perimetral en peligro, por otro lado esto también ocurre con la renovación de los dispositivos para brindar servicios por ejemplo, contar con más capacidad de almacenamiento para los diferentes programas informáticos que brinda el Ministerio del interior a la ciudadana ecuatoriana.

En el caso de los activos de tipo informático contamos con sistemas los cuales no están disponibles para el uso de cualquier ciudadano, si bien los servicios son para la ciudadanía solo personal autorizado puede acceder a esta información, como es el caso de los sistemas migratorios únicamente funcionarios del Ministerio del Interior pueden acceder a los sistemas, sin embargo la gestión de riesgos sobre este tipo de activos recalca a los controles de seguridad de red, ya que estos sistemas cuentan con enlaces dedicados exclusivamente para su uso exclusivo, por lo que se debe asegurar que la conexión entre los servidores y el sistema tengan un alto nivel de disponibilidad.

Los procesos de control ayudaron a mitigar casi en su totalidad el nivel de riesgo que cuentan los activos informáticos del Ministerio del Interior, esto se debe a que todos los activos de nivel alto deben ser tratados ya que se son prioridad para el funcionamiento correcto de la organización, también porque se trata de una entidad importante del estado que maneja información delicada.

La seguridad informática es un proceso que se renueva todo el tiempo, es decir el presente trabajo de levantamiento de información puede que no sea efectivo según los vayan pasando los años, es de su importancia que la lista de riesgos y activos se siga actualizando, ya que cada año hay nuevos tipos de vulnerabilidades y es responsabilidad de los encargados de la seguridad informática tratar estas vulnerabilidades.

5.2. Recomendaciones

A pesar de tener un sistema de seguridad eficiente, se recomienda que el Ministerio del Interior realice actualizaciones es sus sistemas de seguridad perimetral, ya que lleva varios años sin ser actualizado, por falta de presupuesto y con el limitante de las autoridades que exigen ejecuten servicios utilizando soluciones de software libre.

Otro de los aspectos delicados que necesita controlar esta organización son sistemas de monitoreo de red en tiempo real, que permitan garantizar la efectividad y la disponibilidad de los servicios que brindad, también esto permita mitigar riesgos de forma más rápida ya que permite encontrar problemas en la red institucional en tiempo real.

El divulgar la importancia de la gestión de riesgos a todos los usuarios pertenecientes a cualquier institución es el pilar fundamental que permitirá que a la organización crecimiento en el aspecto de seguridad, ya que todo funcionario comprenderá el impacto que puede significar un amenaza o vulnerabilidad que pueda afectar que la entidad cumpla sus objetivos principales.

Se sugiere utilizar los formatos y las indicaciones que encuentran en este guía para entidades públicas en general, ya que el presente trabajo de titulación está basado en las soluciones de gestión de riesgos de una entidad del estado ecuatoriano. Sin

embargo, esta déjala posibilidad a que se utilice el presente trabajo, para aumentar nuevas formas de análisis o adaptarla para que sea una solución universal y que no sea utilizada únicamente para entidades del Ecuador sino para cualquier entidad en el mundo.

REFERENCIAS

Barrientos, M. J. (2012). Capitulo 2 Amenazas y vulnerabilidades de la seguridad informática. Recuperado el 16 de mayo 2019 de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217/A5.pdf?sequence=5

Centro Criptológico Nacional. (2016). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Recuperado el 20 de mayo 2019 de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Deloitte. (2019). COSO - Evaluacion-Riesgos-COSO. Recuperado el 3 de mayo 2019 de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Evaluacion-Riesgos-COSO.pdf

Hidalgo, J. Y., Tupiza, D. L., & Sanchez, T. A. (2017). Políticas de Seguridad de una Red Multiservicios Corporativa, Utilizando Hacking Ético. Recuperado el 10 de mayo 2019 de http://www.laccei.org/LACCEI2016-SanJose/RefereedPapers/RP251.pdf

Instituto ecuatoriano de Normalizacion INEN. (2010). NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27002:2009. Quito: INEN.

ISO International Organization for Standardization. (2014). Sistema de Gestión de Seguridad de la Información (SGSI). Recuperado el 3 de junio 2019 de http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO International Organization for Standardization. (2019). ISO 31000:2018(es) Gestión de Riesgos. Recuperado el 5 de mayo 2019 de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISOTools. (2016). Iso 27001 Sistema Gestion Seguridad Informacio. Recuperado el 22 de abril 2019 de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISOTools. (2017). 4 opciones de mitigación en el tratamiento de riesgos según ISO 27001. Recuperado el 20 de abril 2019 de https://www.isotools.org/2017/08/20/4-opciones-mitigacion-tratamiento-riesgos-segun-iso-27001/

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2018). Gestion de Riesgos. Recuperado el 15 de mayo 2019 de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2018). PLAN DE LA SOCIEDAD DE LA INFORMACIÓNY DEL CONOCIMIENTO. Recuperado el 10 de junio 2019 de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/11/Plan-de-la-Sociedad-de-la-Informacion-PSIC-20181026.pdf

Ministerio del Interior. (2019). Valores / Misión / Visión. Recuperado el 11 de abril 2019 de https://www.ministeriointerior.gob.ec/valores-mision-vision/

Mora, L. H. (2016). Guia Practica - Armado una Precisa Matriz de Riesgo. Recuperado el 24 de abril 2019 de https://www.flexcompliance.com/repository/LUCIO_MORA_GUIA_PRACTICA_PARA_EL_ARMADO_DE_UNA_PRECISA_MATRIZ_DE_RIESGOS.pdf

Peñaherrera, C. C. (2016). EGSI. Recuperado el 15 de abril 2019 de https://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

Secretaría nacional de Gestión de la Política. (2017). EGSI. Recuperado el 10 de abril 2019 de https://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

Tarazona, C. (2007). Amenazas informáticas y seguridad de la información. Recuperado el 20 de junio 2019 de https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/

Torres, C. (2016). LA IMPORTANCIA DE REALIZAR UN ANÁLISIS DE RIESGO EN LAS EMPRESAS. Recuperado el 21 de junio 2019 de http://polux.unipiloto.edu.co:8080/00003266.pdf