UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"ELABORACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN PÚBLICA BASADO EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN"

Realizado por:

Ing. Marco Paúl Gallardo Ávila

Director del proyecto:

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN

DECLARATORIA

El presente trabajo de investigación titulado:

"ELABORACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN PÚBLICA BASADO EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN"

Realizado por:

MARCO PAÚL GALLARDO ÁVILA

Como requisito para la Obtención del Título de:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

Ha sido dirigido por el profesor

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

Quien considera que constituye un trabajo original de su autor

_____

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

DIRECTORA

LOS PROFESORES INFORMANTES

Los Profesores Informantes:

DIEGO FERNANDO RIOFRIO LUZCANDO

WALTER EDISON ESTRELLA MOGOLLON

Después de revisar el trabajo presentado,

lo han calificado como apto para su defensa oral ante

el tribunal examinador

_____	_____
Diego Fernando Riofrio Lascando	Walter Edison Estrella Mogollón

Quito, 14 de junio de 2018

DEDICATORIA

Este proyecto, así como todos los objetivos de mi vida, se los dedico mis padres, quienes con su fortaleza, comprensión y apoyo incondicional han sido el pilar de mi crecimiento personal. A mi amada esposa quien es la base fundamental de mi hogar al ser la participe de mis nuevos objetivos, a mis hermanas y a todas las personas que han estado a mi lado incondicionalmente.

AGRADECIMIENTOS

En este proyecto quiero agradecer a Dios por ser la luz que ilumina mi vida y llenarme de bendiciones.

A la Ing. Verónica Elizabeth Rodríguez Arboleda, MBA. directora de mi proyecto, quién con su experiencia, tiempo, conocimiento y apoyo supo encaminar el desarrollo de este, su predisposición y el ánimo transmitido que ha motivado la finalización exitosa del proyecto.

A mis padres, quienes serán siempre los grandes maestros que con sus luces han plasmado sus mejores valores en cada acto de mi vida.

RESUMEN

La Institución pública, al ser una institución pública ligada al Gobierno Central, debe cumplir los lineamientos establecidos por el Ministerio de Telecomunicaciones relacionados a la aplicación del Esquema Gubernamental de Seguridad de la Información (EGSI), que fue emitido mediante Acuerdo Ministerial 166 en el año 2013 y se basa en las mejores prácticas de la norma ISO/IEC 270001-2. La ejecución del EGSI será evaluada en julio de 2018.

En el presente estudio se plantea una Política de Seguridad de la Información para la misma, siguiendo las directrices del Esquema Gubernamental de Seguridad de la Información, lo que le permitirá garantizar la confidencialidad, disponibilidad e integridad de la información.

Para esto se identificó las aplicaciones críticas de la institución mediante las mejores prácticas de las normas ISO 27005, ISO 31000 y COBIT for Risk. Además, se analizó el riesgo para determinar su tratamiento y garantizar la continuidad del servicio que brinda esta Cartera de Estado, así también, se generó umbrales de aceptación del riesgo y estableció la base para la ponderación de sus activos en función de la criticidad y afectación que su inactividad pueda causar a la institución.

ABSTRACT

The public institution is managed by the Central Government. This institution must comply with the guidelines established by the Ministry of Telecommunications related to the application of the Esquema Gubernamental de Seguridad de la Informacion (EGSI), which was issued by Ministerial Agreement 166 in 2013. Additionally, this guideline is based on ISO / IEC 270001-2 best practices. The execution of the EGSI will be evaluated in July 2018.

This study proposes an Information Security Policy for that comply with the guidelines by EGSI. This policy would guarantee the confidentiality, availability and integrity of the information.

The critical applications of the institution were identified previously by applying ISO 27005, ISO 31000 and COBIT best practices for risk standards. The risk was analyzed to determine its appropriate treatment so that it guarantees the continuity of the service provided by this State Department. Likewise, risk acceptance thresholds were generated creating the basis to weigh its assets based on the criticality and impact that its inactivity may cause the institution.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

CAPÍTULO I
INTRODUCCIÓN

La Institución pública fue creada para el control de sustancias, o preparados que las contengan, vigilancia de sustancias que no constan en los anexos de la Ley y cobro de servicios relacionados a las actividades de producción, importación, exportación, comercialización, almacenamiento, distribución, transporte, prestación de servicios industriales no farmacéuticos, reciclaje, reutilización, análisis y uso de sustancias.

La institución pública cuenta con nueve sucursales denominadas "zonales" a nivel nacional, las cuales coordinan el manejo de sustancias, la descentralización de la institución permite tener una mejor intervención y aplicación de la Ley a nivel nacional. Para su ejecución la institución trabaja en conjunto con varias instituciones gubernamentales, entre otras.

1.1 El problema de la investigación

1.1.1 Planteamiento del problema

1.1.1.1 Diagnóstico

La Unidad de Gestión de TI está conformada por un equipo de nueve personas organizadas en tres campos de acción: infraestructura, desarrollo y soporte técnico, quienes deben garantizar la confidencialidad, integridad y disponibilidad de la información, estableciendo parámetros adecuados de seguridad. Con la finalidad de poder desarrollar la investigación se remitió un Oficio para contar con los accesos e información necesarios. (ANEXO A)

Según el levantamiento de información realizado en la unidad de Gestión de TI en el mes de noviembre de 2017 (ANEXO B) con la finalidad de diagnosticar la realidad institucional, verificar la existencia de políticas de seguridad y el cumplimiento del Esquema Gubernamental de Seguridad de la Información (EGSI), se identificó la

existencia de un proyecto fallido para la implementación de una política de seguridad de la información que pretendía cumplir con el Plan Nacional de Gobierno Electrónico 2014-2017 dispuesto por el ente regulador del Estado denominado Gobierno Electrónico bajo la autoridad competente del Ministerio de Telecomunicaciones.

Los sistemas desarrollados y aplicaciones utilizadas en la institución no cuentan con una política de seguridad, ni requerimientos básicos para su parametrización a nivel de seguridad informática y de la información.

Las reglas establecidas espontáneamente por la unidad de Tecnologías de la Información no fueron sujetas a revisión por el Oficial de Seguridad y tampoco socializadas y avaladas por la Máxima Autoridad, dejando a la institución inmersa en un proceso improvisado para asignar permisos, accesos y restricciones a la infraestructura, paquetes y sistemas informáticos, así como a la información de esta Cartera de Estado, siendo una gran debilidad para la unidad de Gestión de TI y la Coordinación a la que esta se debe.

Actualmente no se cuenta con una política de seguridad de la información adecuada que permita establecer los parámetros apropiados para salvaguardar la confidencialidad, disponibilidad e integridad de la infraestructura tecnológica, aplicaciones e información institucional.

1.1.1.2 Pronóstico

De acuerdo de los objetivos específicos de la institución pública y considerando que la Dirección de Gestión de TI no posee una política para salvaguardar la información, ni un control de la infraestructura de almacenamiento tanto en software como en hardware, se puede generar un desborde de la información, filtración de contenidos, falta de disponibilidad de los servicios de los cuales depende gran parte del transporte, importación, fabricación de sustancias, así como el aseguramiento de la información.

La falta de revisión de los sistemas y paquetes informáticos puede ocasionar la indisponibilidad de servicios de conectividad, datos y aplicaciones con varios países de la región, debido a que la institución es proveedora de aplicaciones para controlar el

transporte de narcóticos a otros países de la región, alojando sus bases de datos dentro del data center local.

La inadecuada administración y custodia de la información por parte de la Institución pública puede generar pérdidas económicas al Estado, parálisis en la producción y transporte de sustancias sujetas a control y descoordinación con los Ministerios y Secretarías con los que realizan un trabajo conjunto de los sistemas e infraestructura que reside dentro de la institución.

1.1.1.3 Control del Pronóstico

Para controlar lo pronosticado, se plantea en el presente estudio la elaboración de una política de Seguridad de la Información, la cual contempla controles para aseguramiento de la infraestructura a nivel hardware y software que almacenan las aplicaciones críticas de la Institución y permiten dar continuidad a los servicios que esta Cartera de Estado presta, evitando el desborde de la información, falta de disponibilidad de los servicios como transporte, importación, fabricación de sustancias por parte de las empresas.

Considerando que no existe una definición de criticidad de las aplicaciones y una medición de su riesgo de acuerdo a las prestaciones que estas brindan a nivel nacional e internacional, se pretende generar una matriz de identificación de criticidad de los activos, así como una matriz de riesgos para enfocar los controles en esos puntos estratégicos.

Con la finalidad de regular la inadecuada administración y custodia de la información de la Institución pública, se propone establecer los controles en función del Esquema Gubernamental de Seguridad de la Información, emitido por el Ministerio de Telecomunicaciones.

1.1.2 Formulación del problema

La Institución pública al ser una entidad de control utiliza sistemas propios y aplicaciones que permiten administrar sustancias y demás actividades de la institución, al no poseer una política de seguridad implementada existe un alto riesgo de pérdida o manipulación de la información, así como indisponibilidad de las aplicaciones lo cual conllevaría a pérdida de control de sustancias, retraso en las importaciones, entre otros.

1.1.3 Objetivo general

Elaborar una política de seguridad de la información para la Institución pública, basado en el Esquema Gubernamental de Seguridad de la Información que garantice la integridad, confidencialidad y disponibilidad en las aplicaciones tecnológicas institucionales.

1.1.4 Objetivos específicos

- Identificar los aplicativos críticos de la unidad de Gestión de TI mediante una metodología elaborada para el análisis de criticidad y riesgos que permita valorarlos conforme su nivel de funcionalidad dentro de la Institución pública.
- Proponer los hitos prioritarios del Esquema Gubernamental de Seguridad de la Información, de acuerdo con el análisis del nivel de criticidad de los aplicativos, para la elaboración de la política de seguridad de la información.
- Diseñar los procesos de la política de seguridad de la información de acuerdo al nivel de criticidad de los aplicativos institucionales e hitos del Esquema Gubernamental de Seguridad de la Información seleccionados, que permitan garantizar la confidencialidad, disponibilidad e integridad de la información de la Institución pública.

1.1.5 Justificación

Justificación Técnica.- La Institución pública al ser una entidad de control requiere que sus aplicaciones informáticas cumplan con los parámetros de seguridad de la información: confidencialidad, disponibilidad e integridad; una política de seguridad permitirá cumplir estos criterios y salvaguardar sus activos críticos, permitiendo la continuidad del negocio y previniendo el daño o ataque informático a sus aplicaciones principales y de esta manera cumplir con el Esquema Gubernamental de Seguridad de la Información.

Justificación Metodológica.- El presente estudio utiliza una metodología desarrollada por el autor basada en las normas de seguridad internacionales ISO 27001, ISO 27002, COBIT for risk y el EGSI, para validar dos aspectos fundamentales para la elaboración de la política de seguridad: la criticidad de los aplicativos y el análisis de

riesgos a los que están expuestos los aplicativos tecnológicos institucionales, manteniendo las mejores prácticas de las normas en mención y cumpliendo con lo establecido en el acuerdo ministerial 166 establecido por el Ministerio de Telecomunicaciones.

La información de la administración pública se divide en dos grandes grupos, la información que es de libre acceso y la información restringida o confidencial, el Esquema Gubernamental de Seguridad de la Información fue emitido en septiembre del 2013, se publicó mediante Registro Oficial No. 88 con el Acuerdo Ministerial No. 166, y dispone que todas las instituciones públicas deben utilizar las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 enfocada en la Gestión de Seguridad de la Información. La SNAP (Secretaría Nacional de la Administración Pública, 2013). Este acuerdo obliga a diseñar e implementar el EGSI de acuerdo con los siguientes hitos:

- Creación de un Comité de Seguridad de la Información, liderado por el Oficial de Seguridad de la Información.
- Implementación de controles prioritarios
- Implementación del EGSI, en función de los hitos correspondientes a cada institución conforme su competencia.

El Esquema Gubernamental de Seguridad de la Información – EGSI, es una resolución del Gobierno para implementar controles de seguridad en todas las entidades públicas que dependen de la función ejecutiva, es decir, indica cuales son los controles básicos que se deberían tener dentro de una organización (Secretaría Nacional de la Administración Pública, 2013).

El EGSI cubre los controles de seguridad definidos en el estándar ISO/IEC 27002. El esquema ha sido enmarcado para cumplir con hitos obligatorios en su primera fase y con hitos optativos en la segunda fase. Este proceso fue definido por el Gobierno con la finalidad de identificar nivel de madurez de seguridad que tienen las instituciones públicas en el manejo de la información.

Entre los beneficios de este sistema, se destaca el hecho de que permite, por un lado, “determinar o diagnosticar cual es la información más importante que existe dentro de

una institución, y, por otro lado, ver como dicha información puede ser protegida, para evitar de esta manera el robo de datos a través de ataques informáticos.” (Sistemas de Gestión de Seguridad de la Información SGSI, 2016).

Bajo este antecedente se justifica la implementación de una política institucional de seguridad de la información orientada a salvaguardar la información almacenada en los servidores de aplicaciones, debido a que el Esquema Gubernamental de seguridad de la Información cumple con la norma internacional ISO/IEC 27001 e ISO/IEC 27002, en función de las directrices emitidas por el Gobierno Central.

1.2 Marco Teórico

1.2.1 Institución pública

“La Institución pública en el ámbito de su competencia y de acuerdo con la Ley se enfoca en diversos campos de intervención: Salud, educación, laboral, comunitario, familiar, cultural, recreativo, deportivo, comunicación, información y desarrollo alternativo preventivo; donde ejecuta la coordinación, articulación, gestión, evaluación y seguimiento de la aplicación de esta Ley.

La Institución pública dentro el estatuto orgánico institucional está conformado por subsecretarías, coordinaciones y direcciones conforme a sus puntos estratégicos de acción, la unidad de Gestión de TI pertenece a la Coordinación de Gestión de Planificación y Gestión Estratégica.

De acuerdo al Plan Estratégico Institucional de la Institución pública y conforme a sus lineamientos definidos en la creación de políticas de control y fiscalización, se ha tomado del documento (Institución Pública, 2016, pp. 5, 6) la información que se detalla continuación:

Misión

> “Regular, coordinar, articular, facilitar y controlar la implementación de procesos intersectoriales de salud con un enfoque centrado en los sujetos y su buen vivir. (Institución Pública, 2016, pp. 5, 6)

Visión

La intervención integral y articulada del Estado, sobre el fenómeno socio económico de la salud, para fortalecer el bienestar de los ciudadanos”. (Institución Pública, 2016, pp. 5, 6)

Objetivo general

Incrementar la prevención del fenómeno socioeconómico de la salud y la regulación, control y administración de sustancias en el ámbito nacional.

Objetivos específicos

- Incrementar la generación de conocimiento y evidencia científica para el direccionamiento de la política pública sobre salud.
- Incrementar los mecanismos de prevención integral del uso y consumo de alcohol y otras sustancias.
- Incrementar la eficiencia y eficacia en la regulación, control y administración de sustancias.
- Incrementar la eficiencia institucional de la institución pública.
- Incrementar el desarrollo del talento humano de la institución pública.
- Incrementar el uso eficiente del presupuesto de la institución pública. (p. 5)

Esquema Gubernamental De Seguridad De La Información - EGSI.

“La Secretaria Nacional de la Administración Púbica creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, la misma que desarrollo para las instituciones de la Administración Pública un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información y su proceso de mejora continua, llamado Esquema Gubernamental de Seguridad de la Información - EGSI; la cual enfatiza ciertas directrices y no reemplaza a la norma INEN ISO/IEC 27002 para la Gestión de la Seguridad de la Información.

Mediante Acuerdo Ministerial N° 166 el 25 de septiembre de 2013 entra en vigencia el EGSI, en la cual se indica: Que, es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades

de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva. (Alvarado, 2015)

Figura 1. Los 11 puntos de contenido del EGSI.

Fuente: (Secretaría Nacional de la Administración Pública, 2013)

El Esquema Gubernamental de Seguridad de la Información, contiene 11 puntos que Wilmer Acosta (2016) los resume en:

1) **Política de Seguridad de la Información,** donde consta: el documento de la política de seguridad de la Información y revisión de la política.
2) **Organización de la Seguridad de la Información,** donde la máxima autoridad de la institución se compromete a hacer el seguimiento, disponer de capacitaciones y conformar el Comité de Gestión de la Seguridad de la Información (CGSI) y sus integrantes, la coordinación de la gestión de la seguridad, autorizaciones para nuevos servicios, acuerdos de confidencialidad, cuando y cuales autoridades se deben contactar según el incidente, revisiones independientes de la seguridad de la información, identificación de riesgos externos, y seguridades con ciudadanos, clientes o terceros.

3) **Gestión de los Activos:** Donde se debe realizar el inventario de activos primarios, hardware, software, redes y de la estructura organizaciones; definiendo reglamentos para el uso del correo electrónico, acceso y uso del internet y de los sistemas de videoconferencia
4) **Seguridad de los Recursos Humanos:** contempla la funciones y responsabilidades, selección, términos y condiciones laborables, responsabilidad de la directiva a cargo del funcionario, educación, formación y sensibilización en seguridad de la información, proceso disciplinario, responsabilidades de terminación de contrato, devolución de activos y retiro de los privilegios de acceso
5) **Seguridad Física y del Entorno:** en donde se debe detallar el perímetro de seguridad física, controles de acceso físico, seguridad de oficinas, protección contra amenazas externas, trabajos en áreas seguras, áreas de descargo y despacho, ubicación y protección de los equipos, servicio de suministro, seguridad del cableado, Mantenimiento de los equipos, seguridad de los equipos y seguridad en la reutilización de los equipos, retiro de activos de propiedades.
6) **Gestión de Comunicaciones y Operaciones,** contempla la documentación de los procedimientos de operación, gestión del cambio, distribución de funciones, separación de las instancias de desarrollo, pruebas, capacitación y producción, presentación del servicio, monitoreo y revisión de los servicios por terceros, gestión de los cambios en los servicios ofrecidos por terceros, gestión de la capacidad, aceptación del sistema, controles contra código malicioso, controles contra código móviles, respaldo de la información, controles de las redes, seguridad de los servicios de la red, gestión de los medios removibles.
7) **Control de Acceso:** donde exista políticas de control de acceso, registro de usuarios, gestión de privilegios, revisión de los derechos de acceso de los usuarios, uso de contraseñas, equipo de usuario desatendido, política de puesto de trabajo despejado y pantalla limpia, sistema de gestión de contraseñas, control de conexión a las redes, trabajo remoto.
8) **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información:** contempla el análisis y especificaciones de los requerimientos de seguridad, validación de datos de entrada y de salida, protección de los datos de prueba del sistema, procedimiento

de control de cambios, restricción del cambio de paquetes de software, fuga de información y controles de las vulnerabilidades técnicas.

9) **Gestión de los Incidentes de la Seguridad de la Información:** generando reportes sobre los eventos de seguridad de la información, las debilidades en la seguridad; además de responsabilidades y procedimientos, recolección de evidencias.
10) **Gestión de la Continuidad del Negocio:** Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio, continuidad del negocio y evaluación de riesgo, desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información, estructura para la planificación de la continuidad del negocio, pruebas, mantenimientos y revisión de os planes de continuidad del negocio.
11) **Cumplimiento:** Se debe identificar la legislación aplicable, conocer los derechos de propiedad intelectual, protección de registro en cada entidad, prevención del uso inadecuado de servicios de procesamiento de información, reglamentación de controles criptográficos, verificación del cumplimiento técnico, protección de las herramientas de auditoría de los sistemas de información.

Norma ISO/IEC 27001:2013

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

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido

implementada en esa organización en cumplimiento con la norma ISO 27001 (Advisera Expert Solutions Ltd, 2018).

Figura 2. ISO 27001 - 27002

Fuente: (Seguridad Informática, 2008)

El Estándar Internacional ISO/IEC 27001, según el portal GES Consultor (2016) indica que:

> La Seguridad de la Información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad al máximo nivel, en los entornos globalizados actuales, donde las transacciones de negocio y servicio (Administraciones Públicas) llevan en su praxis el sufijo 'electrónico', esta prioridad se maximiza ante las especiales características del medio en que se desarrollan y sus riesgos asociados.
>
> La norma ISO/IEC 27001 especifica… los siguientes requisitos:
>
> - Definición del alcance del SGSI
> - Definición de una Política de Seguridad
> - Definición de una metodología y criterios para el Análisis y Gestión del Riesgo
> - Identificación de riesgos
> - Evaluación de los posibles tratamientos del riesgo
> - Elaboración de un Declaración de Aplicabilidad de controles y requisitos

- Desarrollo de un Plan de Tratamiento de Riesgos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información
- Gestión de recursos y operaciones
- Gestión de incidencias
- Elaboración de procedimientos y documentación asociada.

Norma ISO 27002

Al referirse sobre la ISO 27002, “esta norma es muy relevante dentro del sector ya que, toma como base todos los riesgos a los que se enfrenta la organización en su día a día, tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de la organización.” (Sistemas de Gestión de Seguridad de la Información SGSI, 2016)

Según (ISO Tools Excellence, 2016) La norma ISO 27002 se encuentra estructurada en 14 capítulos que describen las áreas que se deben considerar para garantizar la seguridad de la información de las que se dispone. El documento recomienda un total de 114 controles, si bien no hace falta cumplirlos todos, sí que hay que tenerlos en cuenta y considerar su posible aplicación, además del grado de esta, como se resume en los siguientes puntos:

1. Políticas de Seguridad de la Información

Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

2. Organización de la Seguridad de la Información

Los controles indicados en este capítulo buscan estructurar un marco de seguridad eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles.

Debemos tener presente que cada vez es mayor el peso que está ocupando el teletrabajo dentro de las empresas, y por ello, se deben tener en cuenta todas sus características especiales para que ningún momento la seguridad de la información de la que se dispone se vea afectada.

3. Seguridad relativa a los recursos humanos

Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

4. Gestión de activos

Se centra en la atención en la **información como activo** y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la **seguridad y en la alteración no deseada**.

5. Control de acceso

Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo, no todas las **personas de una organización** necesitan acceder para realizar su actividad diarias a todos los datos, sino que tendremos roles que **necesitan un mayor acceso** y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, **gestión de los privilegios de acceso**, etc. siendo algunos de los controles que se incluyen en este apartado.

6. Criptografía

En el caso de que estemos **tratando la información sensible o crítica** puede ser interesante utilizar diferentes técnicas criptográficas para **proteger y garantizar** su autenticidad, confidencialidad e integridad.

7. Seguridad física y del entorno

A nivel de Seguridad de la información (lógica y física), se contempla la seguridad física como un punto a considerar dentro de las amenazas y riesgos que se pueden presentar.

La seguridad física es el primer filtro de acceso a la información en toda institución pública, para lo cual se consideran varios factores como guardianía, sistema contra incendios, video vigilancia, control de accesos con tarjetas u otro dispositivo de autenticación y demás seguridades que se puedan tomar para que la información no se pierda o sea vulnerada.

8. Seguridad de las operaciones

Tiene un marcado componente técnico entrado en todos los **aspectos disponibles como la protección** del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

9. Seguridad de las comunicaciones

El intercambio de información y datos en distintas escalas **se llevan a cabo mediante diferentes medios**, estos pueden ser físicos o digitales, a través de redes sociales, correo electrónico, herramientas de gestión documental o dispositivos magnéticos por lo cual se garantizar la seguridad y protección de forma adecuada de estos medios de transmisión de estos datos.

10. Adquisiciones, desarrollo y mantenimiento de los sistemas de información

La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, no que es general, **abarca toda la organización** y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del sistema de gestión.

11. Relación de proveedores

Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben **establecer medidas de seguridad** pudiendo ser muy recomendable e incluso necesario en determinados casos.

12. Gestión de incidentes de seguridad de la información

No podemos hablar de **controles de seguridad** sin mencionar un elemento clave, los incidentes en seguridad. Y es que, estar preparados para cuando estos incidentes ocurran, dando **una respuesta rápida y eficiente** siendo la calve para prevenirlos en el futuro.

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio

No sabemos lo que necesitábamos un dato hasta que lo hemos perdido. Sufrir una pérdida de **información relevante y no poder recuperarla** de laguna forma puede poner en peligro la continuidad de negocio de la organización.

14. Cumplimiento

No podemos hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que **se encuentre relacionadas con este campo** y con las que conviven en las organizaciones. Debemos tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben **garantizar que se cumple** y que están actualizados con los últimos cambios siendo esencial para no llevarnos sorpresas desagradables.

Norma ISO 31000:2011 GESTIÓN DEL RIESGO

La Gestión del Riesgo se hace necesaria para controlar y manejar las amenazas que se presentan a nivel organizacional y tecnológico, con los recursos disponibles, a fin de que no se materialicen estos riesgos y afecten los productos y/o servicios que ofrece la empresa.

Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis, luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios del riesgo. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando con el fin de garantizar que no se requiere tratamiento adicional del riesgo. Esta norma describe este proceso sistemático y lógico en detalle.

Aunque todas las organizaciones gestionan el riesgo en algún grado, esta norma establece un número de principios que es necesario satisfacer para hacer que la gestión del riesgo sea eficaz. Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos. (Icontec, 2011)

COBIT 5 For Risk

ISACA (ISACA, 2017) COBIT 5 For Risk sustituye al anterior marco de referencia Riesgos de TI e incluye una guía sobre cómo COBIT 5 es compatible con el gobierno y la gestión de riesgos, y cómo establecer y mantener una función de riesgos eficaz y eficiente, basada en los siete facilitadores de COBIT:

- Principios, políticas y marcos de referencia.
- Procesos.
- Estructuras organizacionales.
- Cultura, ética y conducta.
- Información.
- Servicios, infraestructuras y aplicaciones.
- Gente, habilidades y competencias

Dos perspectivas sobre cómo usar COBIT 5 en un contexto de riesgo:

1. Perspectiva de la función de riesgo: describe lo que se necesita en una empresa para crear y mantener una gestión eficiente y eficaz de las actividades de gestión y gobernanza del riesgo.
2. Perspectiva de la gestión de riesgos: describe cómo los habilitadores de COBIT 5 pueden ayudar a identificar, analizar, responder e informar el riesgo sobre el proceso central de gestión de riesgos.

1.2.2 Estado del arte

Análisis del riesgo y el sistema de gestión de seguridad de la información

Según Gild (2014), en su documento "el enfoque ISO 27001:2005" hace referencia a la implementación de una norma basada en seguridad de la información, misma que necesita determinar los requerimientos básicos y trabajo en conjunto con las autoridades y técnicos relacionados a la seguridad de la información. El propósito fundamental es el de asegurar la información mediante confidencialidad, integridad y disponibilidad en función del análisis realizado por el equipo de trabajo, para establecerlo como guía base en la implementación de los controles que se ajustan a las necesidades del negocio. En tal virtud, apalanca la elaboración de una política y fundamenta el desarrollo del presente estudio involucrando a las autoridades, personal técnico y demás funcionarios para cumplir con el objetivo propuesto.

Según Mesquida, Esperança y Cabestrero (2010), "las normas ISO 27001, plantean una visión de la situación actual de varios estándares y debido a su demanda en función de la seguridad de la información, convergen en un sistema de gestión integrado, mismo que optimiza y cumple con los requisitos específicos de gestión de servicios de TI y de seguridad de la información". De esta manera, se alinea la aplicación del Esquema Gubernamental de Seguridad de la Información que abarca las mejores prácticas de la norma ISO 27001 e ISO 27002, así como el alineamiento para blindar en primera instancia los aplicativos denominados como críticos.

En el documento Fundamentos de ISO 27001 y su aplicación en las empresas según Ladino, Villas y López (2011), describen los fundamentos de la norma y su aplicación en organizaciones, mostrando un caso práctico de implementación en una

organización con el objetivo de obtener una certificación y perfeccionar aspectos de seguridad de la empresa dando como resultado un adecuado resguardo de la información, funcionalidad, seguridad y continuidad al negocio considerada como una buena práctica de TI y optimizando los recursos económicos de la empresa. Al ser una entidad estatal la Institución pública requiere asegurar la continuidad del servicio y a su vez garantizar que la información de carácter confidencial sea cubierta adecuadamente conforme a la implementación de controles apropiados para sus necesidades.

En función del artículo “Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios” de Ramírez y Ortiz (2011) menciona “ El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico. En función de lo antes mencionado es indispensable que la institución pública identifique sus activos críticos que puedan ser susceptibles a los riesgos tecnológicos actuales y enfoque acciones pertinentes para mitigar o aceptar los mismos.

1.2.3 Adopción de una perspectiva teórica

Dado el análisis de la teoría y de los artículos mencionados, se realiza la política de seguridad de la información para asegurar la confidencialidad, disponibilidad e integridad de la información, permitiendo mantener un adecuado control y seguimiento de sus aplicaciones, en función de las buenas prácticas de aseguramiento de TI.

Se establece una secuencia de acciones a seguir para cumplir con los parámetros especificados en el EGSI, mismos que son acogidos de norma ISO, de esta manera se busca cumplir con las buenas prácticas de uso y manipulación de la información que son parte de los requerimientos que una institución del estado requiere para su certificación y aprobación de políticas de la autoridad competente, siendo el Ministerio de Telecomunicaciones la autoridad competente.

En la norma ISO 27001, según GES Consultor (2016) se establecen ciertos pasos que debe cumplir una política para poder ser implementada, estos pasos son:

- **Adaptabilidad,** las políticas deben orientarse exclusivamente a las necesidades de la institución pública.
- **Definición de los objetivos,** determina las formas de aprobación y revisión.
- **Compromiso,** las autoridades son responsables de respaldar la implementación y el uso de la política.
- **Comunicación,** definir las formas de comunicación entre los interesados.
- **Revisión,** las políticas deben ser revisadas de forma periódica para mantener actualizadas conforme a las necesidades de la institución pública.

De acuerdo a estos antecedentes se define la perspectiva teórica con la adopción del Esquema Gubernamental de Seguridad de la Información, mismo que tiene como referencia la norma ISO 27001 e ISO 27002, con la finalidad de establecer una política que asegure la información de la Institución pública.

1.2.4 Marco Conceptual

- **EGSI:** "… está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional, establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. (Alvarado, 2015)
- **INEN ISO/IEC 27002**: "La Norma ISO/IEC 27002 establece las directrices y principios generales para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización. Es un catálogo de buenas prácticas, obtenido a partir de la experiencia y colaboración de numerosos participantes, los cuales han alcanzado un consenso acerca de los objetivos comúnmente aceptados para la gestión de la seguridad de la información" (Servicio Ecuatoriano de Normalización, 2015)

- **Políticas de Seguridad de la Información:** “importancia que ocupa la disposición de una **adecuada política de seguridad**, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.” (Sistemas de Gestión de Seguridad de la Información SGSI, 2016)
- **El SGSI (Sistema de Gestión de Seguridad de la Información)** “es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías”. (Portal ISO 27000, 2013)
- **Información**: “Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.” (Alvarado, 2015)

CAPÍTULO II
ANÁLISIS Y DISEÑO

2.1 Análisis

2.1.1 Situación Actual

La Institución pública desde su inicio, ha experimentado varios cambios de su infraestructura tecnológica, considerando servidores de archivos y aplicaciones.

En su esquema tecnológico ha evolucionado de forma deficiente, la arquitectura que tiene actualmente ha sido una adecuación de diferentes tecnologías que se han adaptado entre ellas, pero de forma básica, sin poder utilizar y optimizar los recursos en su máximo potencial.

Al tener una data center híbrido, constituido de varias soluciones tecnológicas, la Institución pública optó por realizar el desarrollo de sus aplicaciones localmente, siendo estas alojadas en los diferentes servidores y bases de datos que existen, adaptando sus aplicaciones de core del negocio a la infraestructura técnica provista.

2.1.2 Esquema Actual de Infraestructura Tecnológica

La institución pública en su afán de mantener su parque tecnológico parcialmente actualizado adaptó el data center de la Procuraduría General del Estado, con sus equipos e infraestructura anterior, considerando la posibilidad de que las tecnologías establecidas puedan trabajar en conjunto para solventar las necesidades institucionales.

Con la finalidad de cumplir con la normativa básica del Esquema Gubernamental de Seguridad de la Información y conforme al crecimiento de su infraestructura y solicitud de nuevos requerimientos se acoplaron diferentes racks de comunicaciones para distribuir los servidores conforme a los servicios y aplicaciones que posee la institución.

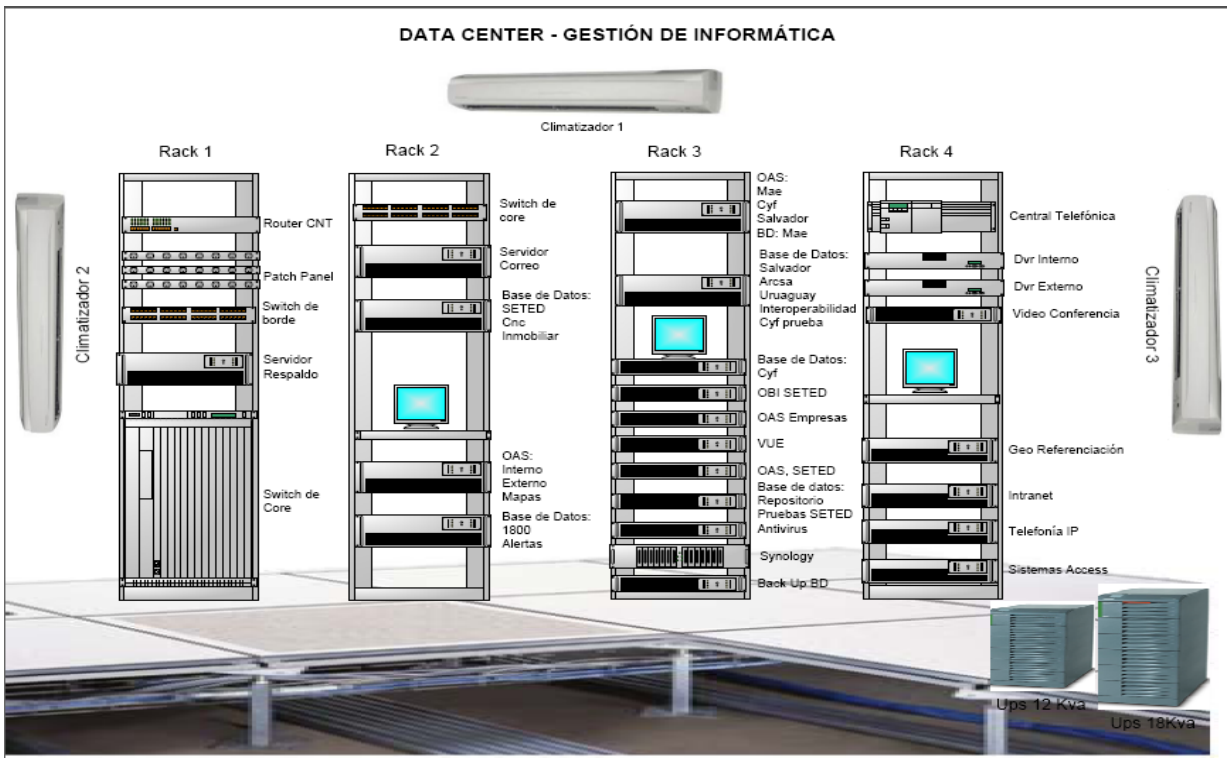


Figura 3. Data Center – Gestión de informática

Fuente: (Institución Pública, 2018)

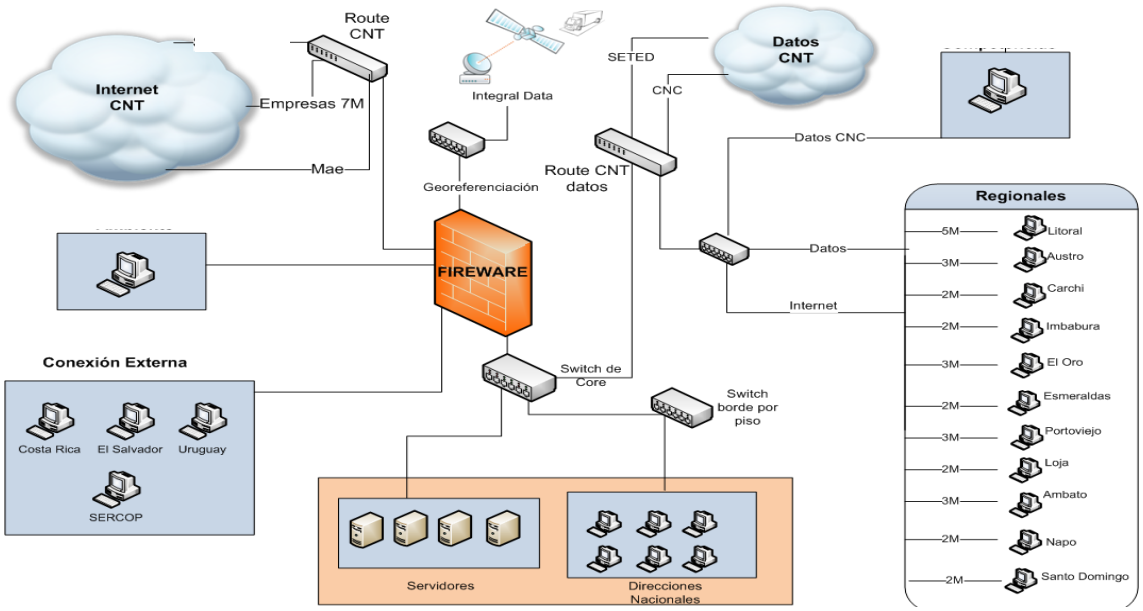


Figura 4. Diagrama de Red

Fuente: (Institución Pública, 2018)

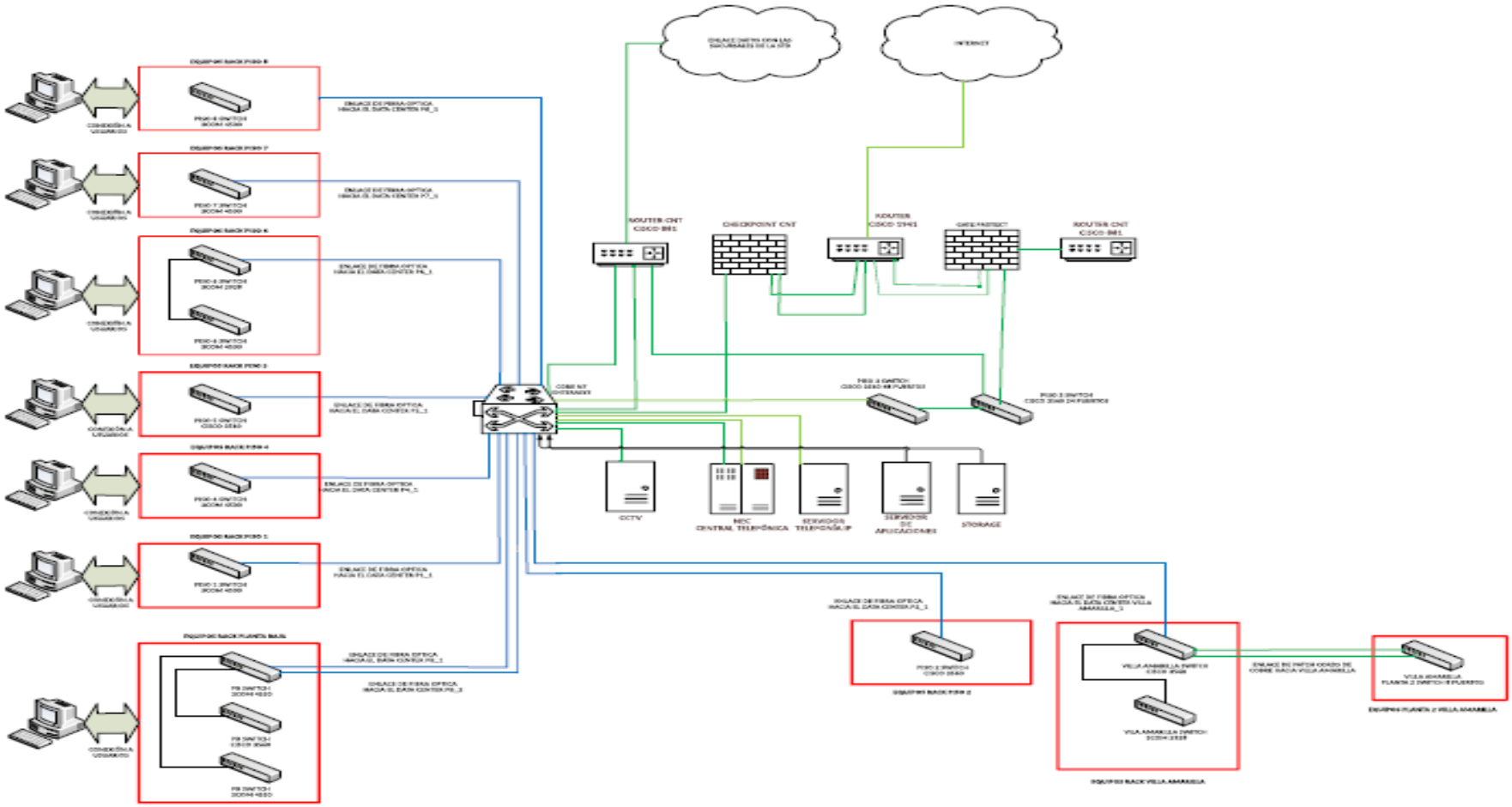


Figura 5. Esquema de Red la Institución Pública

Fuente: (Institución Pública, 2017)

2.1.3 Identificación de Aplicativos desarrollados para análisis de criticidad

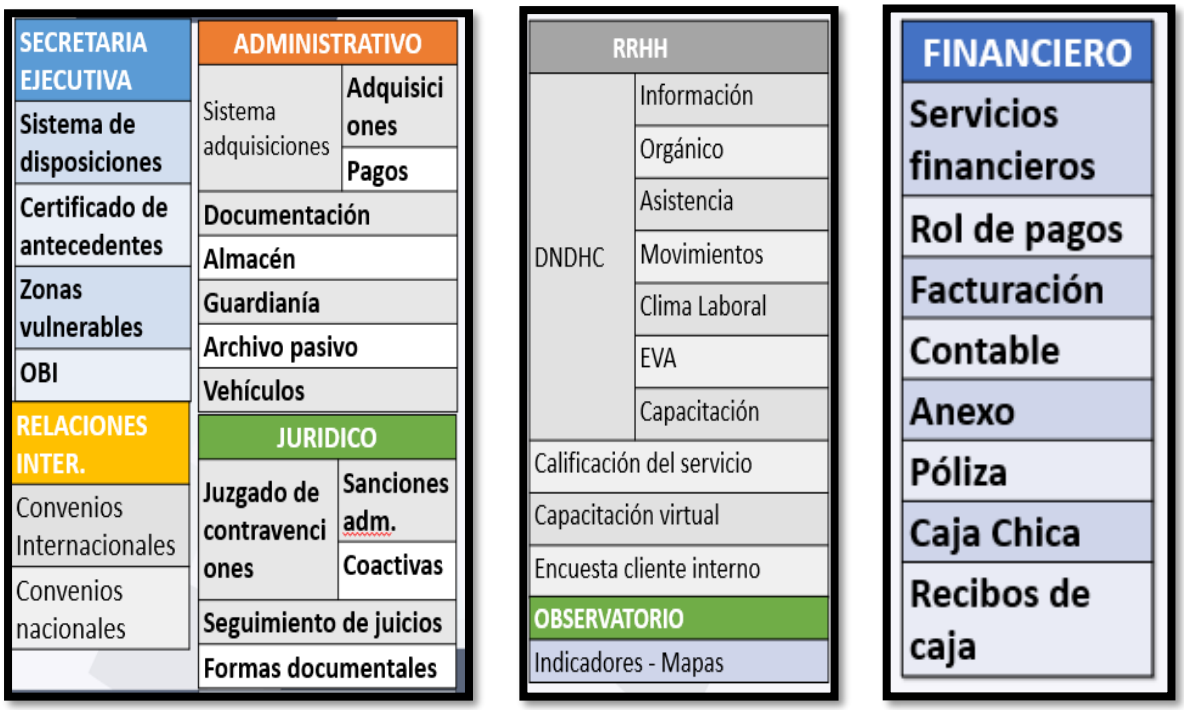


Figura 6. Análisis de criticidad

Fuente: (Institución Pública, 2018)

		BIENES		RRHH	DISPOSICIONES	PLANIFICACION		INTER-OPERATIBILIDAD	INFRA-ESTRUTURA
NACIONALES	INMOBILAR	x							x
	ARCSA		x						x
	MAE		x						x
	PROCURADURIA			x	x				
	CNC					x			x
	POLICIA						x		
	ADUANA						x	x	
	SERCOP							x	

Figura 7. Servicios de la Institución Pública hacia externos

Fuente: (Institución Pública, 2018)

2.2 Esquema Gubernamental de Seguridad de La Información

El Esquema Gubernamental de Seguridad de la Información (Anexo E) fue emitido como acuerdo Ministerial 166 por la Secretaría Nacional de la Administración Pública y publicado en el Registro Oficial de 25 de septiembre de 2013.

En función del análisis funcional del EGSI se puede definir que está compuesto por la Norma ISO 27000 incorporando dentro de sus planes de acción:

2.2.1 Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI está compuesto por varias normas, las cuales promueven la implementación y operación de un SGSI. De acuerdo con la "Guía de iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001" del Colegio Oficial de ingenieros de Telecomunicaciones (Colegio Oficial de Ingenieros de Telecomunicaciones, 2009) "La familia de normas SGSI incluye bajo el título general de: Tecnologías de la información. Técnicas de seguridad las siguientes normas internacionales (listadas en orden numérico):

- **ISO/IEC 27000**, Sistemas de Gestión de Seguridad de la Información. Descripción general y vocabulario.
- **ISO/IEC 27001**, Sistemas de Gestión de Seguridad de la Información. Requisitos.
- **ISO/IEC 27002**, Código de práctica para los controles de seguridad de la información.
- **ISO/IEC 27003**, Guía para la implementación de los Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27005**, Gestión de riesgos de seguridad de la información."

2.2.2 Normativa Legal

Todas las atribuciones y responsabilidades conferidas al "Comité de Seguridad de la Información - CSI" en el Esquema Gubernamental de Seguridad de la Información - EGSI, emitido a través del Acuerdo Ministerial No. 166, serán asumidas por la Unidad de Gestión Estratégica o quien haga sus veces en cada entidad de la Administración Pública Central, Institucional y que depende de la Función Ejecutiva; o por la unidad encargada de la Gestión de Riesgos Institucionales o Seguridad de la Información, cuando

se cuente con aquella dependencia en la estructura orgánica institucional. (Registro Oficial 776, 2016)

2.2.3 Estructura del EGSI

El EGSI fue diseñado para adaptar las mejores prácticas de las normas internacionales fundamentalmente de la Norma ISO/IEC27001/2, para asegurar la seguridad de la información de las instituciones públicas, a diferencia de la norma ISO/IEC 27002, que adapta la seguridad de la información para las empresas.

Diferencia entre EGSI e ISO 27002

Tabla 1. EGSI vs ISO 27002

EGSI		ISO 27002	
TIPO	TOTAL	TIPO	TOTAL
DOMINIO	11	DOMINIO	14
HITO	133	OBJETIVO DE CONTROL	35
CONTROLES * Prioritarios	113	CONTROLES	114
CONTROLES	707		

Fuente: (SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información, 2017)

Información de la ISO 270002

Formato estructura del EGSI

El Esquema Gubernamental de Seguridad de la Información, al tener como base los controles establecidos por la Norma ISO 27001-27002 consta de tres partes: dominio, hito y control.

Los controles pueden ser de dos tipos: normales y prioritarios, siendo estos últimos identificados por un (*).

DOMINIO	**2. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION**
HITO	2.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información
CONTROL	a) Realizar el seguimiento de la puesta en marcha de las normas de este documento (*).

Figura 8. Estructura de dominios del EGSI

Fuente: (Secretaría Nacional de la Administración Pública, 2013)

2.2.4 Marco de referencia para el Gobierno y la gestión del riesgo.

ISO 31000

Es importante que los Dueños de Proceso comprendan el valor de los activos tecnológicos contenidos dentro de los procesos que lideran, y que dispongan de un marco para la evaluación e implementación de los planes de respuestas; para ello se define la metodología de gestión del riesgo tecnológico, siguiendo el proceso indicado en la Figura 8 basada en la guía metodológica de ISO 31000.

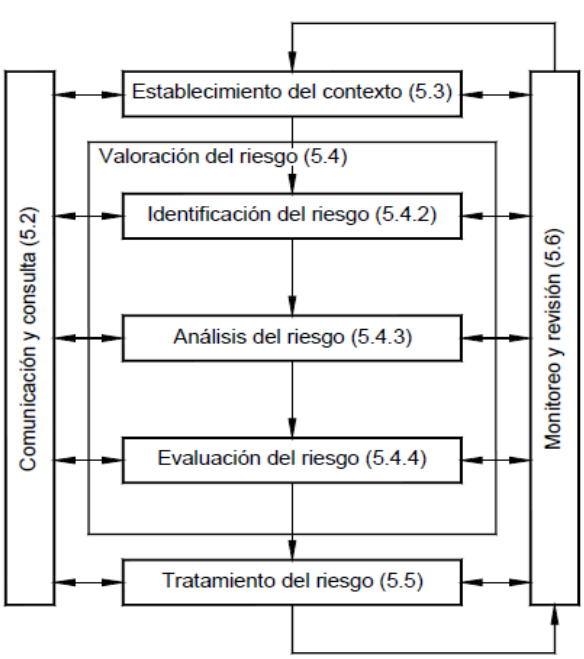


Figura 9. Proceso de gestión de riesgos tecnológicos

Fuente: (Icontec, 2011)

De acuerdo con la metodología establecida y las normas base se establece una guía para identificar, analizar y dar respuesta al riesgo, a través de la aplicación de los procesos principales de gestión de riesgos en COBIT 5 y mediante el uso de escenarios de riesgos.

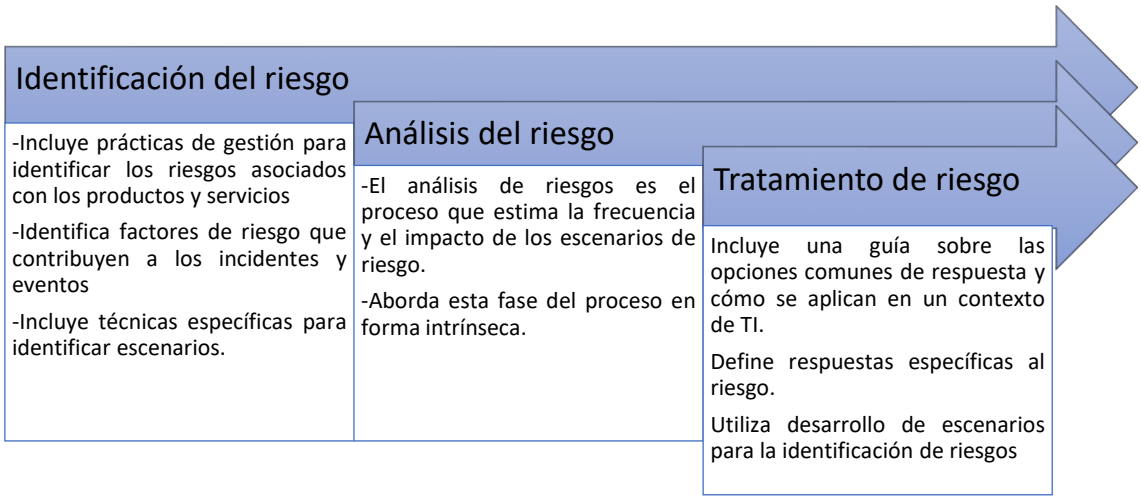


Figura 10. Cobit 5

Fuente: (ISACA, 2017)

- **Riesgo en la habilitación de valor/beneficio de TI**:

  Asociado con las oportunidades perdidas de utilización de la tecnología con el fin de mejorar la eficiencia o efectividad de los procesos de negocio.

- **Riesgo en la entrega de programas y proyectos de TI**:

  Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas, generalmente bajo la forma de programas y proyectos que forman parte de portafolios de inversión.

- **Riesgo en la entrega de operaciones y servicios de TI**:

  Asociado con todos los aspectos del negocio como el desempeño normal de sistemas y servicios de TI, los que pueden destruir o reducir el valor para la institución.

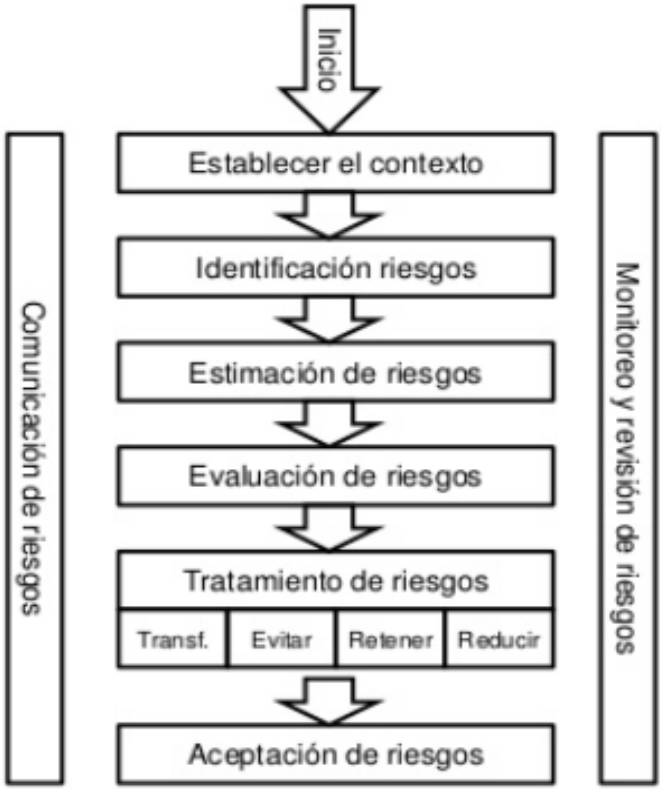


Figura 11. ISO 27005: 2011 - Gestión del riesgo de seguridad de la información

Fuente: (Ramírez, 2011)

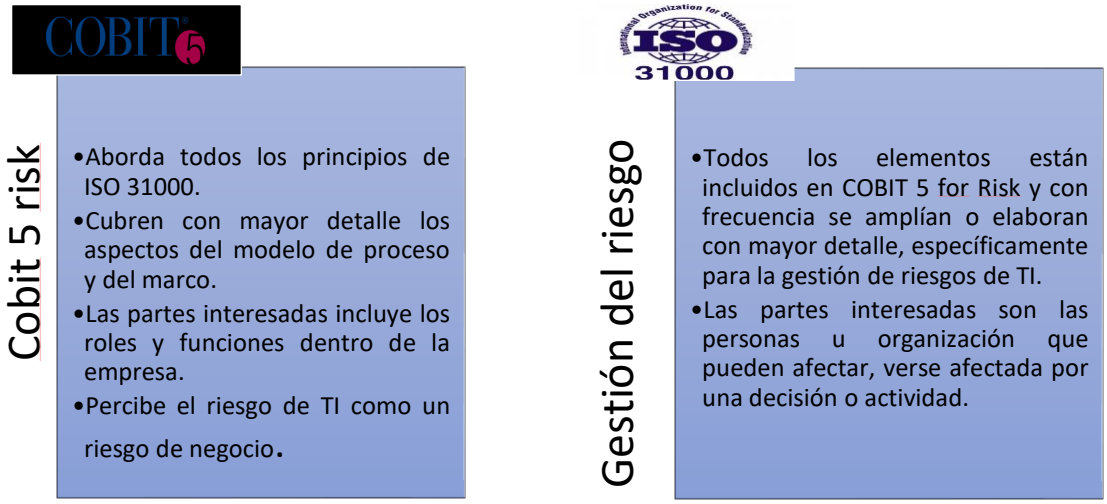


Figura 12. Comparativa Cobit 5 – ISO 31000

Fuente: Autor de la Investigación

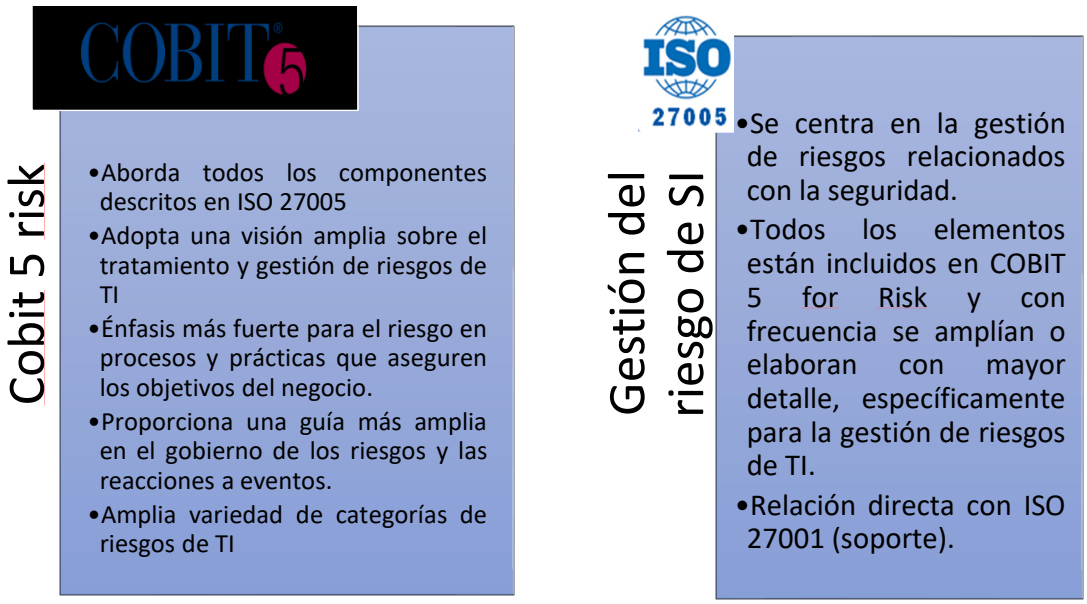


Figura 13. Comparativa Cobit 5 – ISO 27005

Fuente: Autor de la Investigación

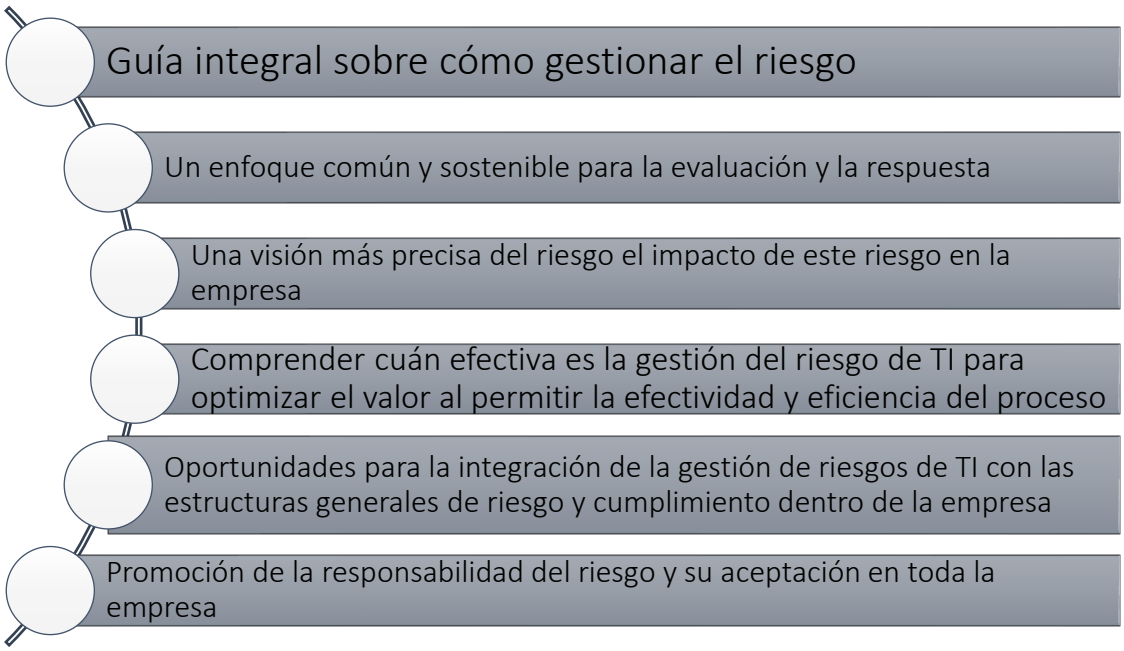


Figura 14. Beneficios de Cobit 5 Risk

Fuente: (ISACA, 2017)

Factores de riesgo

Un factor de riesgo se determina como una condición que puede influenciar en frecuencia e impacto y finalmente, el impacto de los eventos y escenarios de TI en la institución.

Los factores de riesgos también pueden ser interpretados como causas del escenario que se está materializando debido a vulnerabilidades o debilidades, considerando las discriminaciones del caso al ser una institución pública. Estos factores incluyen:

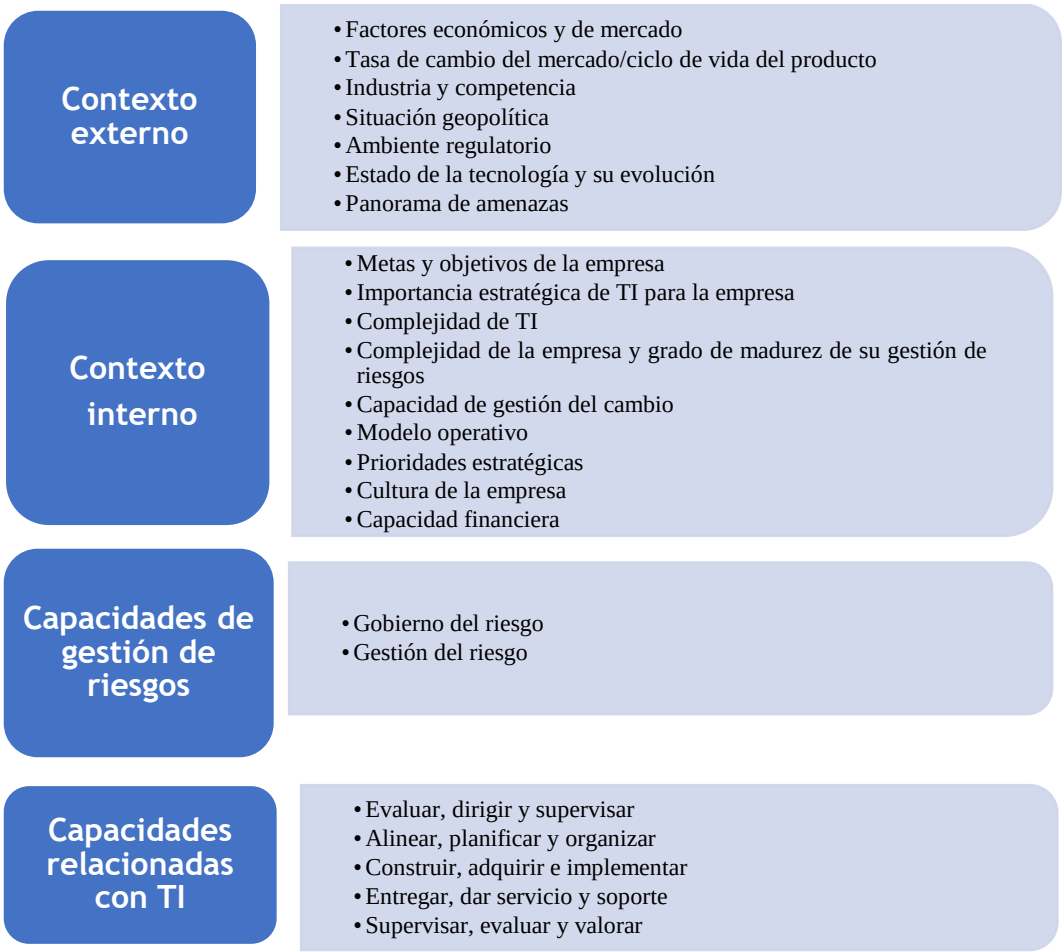


Figura 15. Factores de riesgo

Fuente: Cobit 5 for risk

Identificación del riesgo

La identificación del riesgo es la primera actividad del ciclo de gestión de riesgos y su objetivo es conocer el nivel de exposición de los activos tecnológicos críticos, o el nivel de incertidumbre para el cumplimiento de los objetivos estratégicos de la Institución pública.

De acuerdo a los factores descritos en la Figura 14. Factores de Riesgo, los administradores identifican para los activos tecnológicos los siguientes aspectos:

- Grupo de activos a gestionarle riesgos.
- Partes interesadas afectadas con la materialización del riesgo.
- Dueño del riesgo.
- **Tipo de riesgo:** dentro de estos existen tres tipos de riesgo:

  Riesgo en la habilitación de valor/beneficio de TI: Asociado con las oportunidades perdidas de utilización de la tecnología con el fin de mejorar la eficiencia o efectividad de los procesos de negocio.

  Riesgo en la entrega de programas y proyectos de TI: Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas, generalmente bajo la forma de programas y proyectos que forman parte de portafolios de inversión.

  Riesgo en la entrega de operaciones y servicios de TI: Asociado con todos los aspectos del negocio como el desempeño normal de sistemas y servicios de TI, los que pueden destruir o reducir el valor para la empresa.

Escenarios de riesgo

Un escenario de riesgo es la descripción de un posible evento que si ocurre tendrá un impacto incierto en la institución.

En los escenarios se definen los siguientes elementos de información que son clave para identificar, analizar y responder al riesgo:

- **Actor:** lo que genera la amenaza que aprovecha una vulnerabilidad. Los actores pueden ser internos o externos y pueden ser humanos o no humanos:

- **Tipo de amenaza:** pueden ser: daño físico, naturaleza, pérdida de los servicios esenciales, perturbación debida a la radiación, compromiso de la información, fallas técnicas, maliciosa, compromiso de las fuentes, requerimiento externo y accidental.
- **Amenaza:** es la causa potencial de la materialización de un riesgo.
- **Vulnerabilidad:** debilidad de los activos (aplicaciones), que pueden ser explotados por una o más amenazas.

Análisis de riesgos

Se realiza el análisis de acuerdo con la información obtenida en la etapa de identificación del riesgo. Los aspectos analizados; son frecuencia de ocurrencia e impacto ocasionado en la organización en caso de materializarse.

Análisis por frecuencia

Es la posibilidad de ocurrencia del riesgo durante un cierto período de tiempo o probabilidad de ocurrencia considerando los factores de riesgo, aunque éste no se haya materializado.

2.2.5 FMECA

Según Sistemas de Gestión de Seguridad de la Información SGSI (2016) se trata de un análisis de modos y efectos de falla que incluye evaluación de criticidad y análisis de causa raíz del modo de falla. Esta técnica se ha estado posicionando en la industria por estar basada en riesgo y por buscar eliminar la causa de falla, ambos requisitos de una gestión moderna de activos bajo ISO 55000 o PAS 55.

El FMECA hace un análisis que cumple los requisitos de un FMEA (Análisis de Modo y Efectos de Falla), pero además identifica la causa raíz del modo de falla, su criticidad (riesgo) y una tarea para reducir o eliminar el riesgo, todo bajo un ambiente de priorización basada en riesgo.

2.2.6 Ciclo de Deming - Metodología PHVA

Las siglas del **ciclo o fórmula PHVA** (ISO TOOLS, 2015) forman un acrónimo compuesto por las iniciales de las palabras **P**lanificar, **H**acer **V**erificar y **A**ctuar. Cada uno de estos 4 conceptos corresponde a una fase o etapa del ciclo:

- **Planificar**: En la etapa de planificación se **establecen objetivos** y se **identifican los procesos** necesarios para lograr unos determinados resultados de acuerdo con las políticas de la organización. En esta etapa se determinan también los **parámetros de medición** que se van a utilizar para controlar y seguir el proceso.
- **Hacer**: Consiste en la **implementación de los cambios o acciones necesarias** para lograr las mejoras planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente posibles errores en la ejecución, normalmente se desarrolla un **plan piloto** a modo de prueba o testeo.
- **Verificar**: Una vez se ha puesto en marcha el plan de mejoras, se establece un **periodo de prueba para medir y valorar la efectividad de los cambios**. Se trata de una fase de regulación y ajuste.
- **Actuar**: Realizadas las mediciones, en el caso de que los resultados no se ajusten a las expectativas y objetivos predefinidos, se realizan las **correcciones y modificaciones necesarias**. Por otro lado, se toman las decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos.

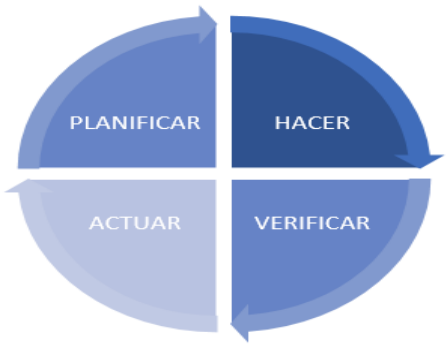


Figura 16. El ciclo PHVA
Fuente: (ISO Tools, 2015)

2.3 Definición de la metodología para determinar activos (aplicaciones críticas) para aplicación de Política de Seguridad:

Basada en el Método FMECA - Análisis de Criticidad, Efectos, y Modos de Falla (Failure Mode, Effects and Criticality Analysis).

5	M (5)	M (10)	A (15)	A (20)	A (25)
4	M (4)	M (8)	A (12)	A (16)	A (20)
3	B (3)	M (6)	M (9)	A (12)	A (15)
2	B (2)	B (4)	M (6)	A (8)	A (10)
1	B (1)	B (2)	M (3)	A (4)	A (5)
Frecuencia / **Consecuencia**	1	2	3	4	5

Criticidad del Activo = Frecuencia * Consecuencia

Frecuencia = Frecuencia de Falla

Consecuencia = Ponderación de aspectos relacionados con el impacto que genera el activo en caso de presentar fallas

Aspectos Para Evaluar

Tabla 2. Frecuencia de falla

1. Frecuencia de Falla	Corresponde a la cantidad de veces que falla algún componente del activo o el activo completo desde el ámbito funcional o de seguridad de la información	
	No más de 1 por mes	1
	Entre 1 y 4 por mes	2
	Entre 4 y 8 por mes	3
	Entre 8 y 12 por mes	4
	Más de 12 por mes	5

Fuente: Autor de la Investigación

Tabla 3. Consecuencia (Ponderación)

No.	Aspectos a Evaluar	Ponderación
1	Impacto al negocio	0,3
2	Nivel de afectación a clientes	0,3
3	Impacto operativo al activo	0,15
4	Costo de reparación del activo	0,15
5	Tiempo promedio de reparación del activo	0,1
TOTAL		1

Fuente: Autor de la Investigación

Tabla 4. Consecuencia (Calificación Final)

Ponderación de Aspectos Evaluados	Consecuencia (Calificación Final)
1 – 1,4	1
1,5 – 2,4	2
2,5 – 3,4	3
3,5 – 4,4	4
4,5 - 5	5

Fuente: Autor de la Investigación

Consecuencias

Tabla 5. Impacto al negocio

1. Impacto al Negocio	Pérdidas generadas a la línea de negocio por fallas del activo. Lucro cesante y multas por incumplimientos legales, regulatorios o contractuales	
No hay afectación al negocio y no hay riesgo de multa		1
Hay afectación parcial al negocio y un riesgo mínimo de multa		3
Hay afectación considerable al negocio y riesgo inminente de multa		5

Fuente: Autor de la Investigación

Tabla 6. Niveles de afectación a clientes

2. Nivel de Afectación a clientes	La afectación repercute en hacia los clientes
La(s) falla(s) no afectan al cliente	1
La(s) falla(s) afectan parcialmente a los clientes	3
La(s) falla(s) afectan totalmente las actividades que realizan los clientes	5

Fuente: Autor de la Investigación

Tabla 7. Impacto operativo al negocio

3. Impacto Operativo al Activo	Afectación del activo y la continuidad del negocio
La(s) falla(s) no afectan la operación del activo	1
La(s) falla(s) afectan parcialmente la operación del activo; algunas de sus funcionalidades siguen operando con normalidad	3
La(s) falla(s) afectan totalmente la operación del activo dejándolo fuera de servicio	5

Fuente: Autor de la Investigación

Tabla 8. Tiempo promedio para reparar

4. Costo de reparación	Costo promedio de reparación del activo cuando presenta fallas, teniendo en cuenta los materiales necesarios y las horas hombre requeridas para la reparación
No requiere de personal externo para la reparación	1
Requiere de personal externo para la reparación sin cambios de hardware	3
Requiere de personal externo e inminente cambio de hardware	5

Fuente: Autor de la Investigación

Tabla 9. Tiempo promedio para reparar

5. Tiempo promedio para reparar	Tiempo estimado que se demora la reparación del activo, cuando este presenta fallas. Es importante tener en cuenta el tiempo que toma la detección de la falla, el tiempo que se demoran en llegar los repuestos (en caso de ser necesario) y el tiempo de reparación del activo	
	Menos de 2 horas	1
	Entre 2 y 4 horas	2
	Entre 4 y 6 horas	3
	Entre 6 y 12 horas	4
	Más de 12 horas	5

Fuente: Autor de la Investigación

Establecida la definición para la identificación de los activos críticos de la Institución pública, se procede a diagramar en función de los parámetros establecidos y aprobados en reuniones de trabajo Anexo B (Acta de reunión), la metodología identificará y determinará los activos críticos, definidos para la implementación inicial de la política establecida en función de los parámetros del EGSI.

Para la aplicación de la metodología es pertinente el uso de la siguiente fórmula:

=Nivel de afectación a clientes * 0,3 + Impacto al negocio * 0,3 + Impacto operativo al activo * 0,15 + Costo de reparación del activo * 0,15 + Tiempo promedio de reparación del activo * 0,1

Frecuencia * Consecuencia = Criticidad del activo

El presente diagrama es una representación e identificación base, mismo que se detalle en el Anexo C (Matriz de activos críticos)

Tabla 10. Matriz de calor de ponderación para criticidad de aplicaciones

No.	Aplicación	Dispositivo/Software	Marca/Fabricante	Frecuencia	Nivel de Afectación a Clientes	Impacto al negocio	Impacto operativo al activo	Costo de reparación del activo	Tiempo promedio de reparación del activo	Criticidad del Activo	Consecuencia	Criticidad del Activo	Confidencialidad	Integridad	Disponibilidad
CONTROL Y FISCALIZACION															
1	SISACYF	Calificación y renovaciones	GRANJA DE SERVIDORES HP (G5,	2	5	5	5	3	3	4,5	5	Alta	x	x	x
2		Ampliaciones e inclusiones		3	5	5	3	3	3	4,2	4	Alta	x	x	x
3		Compras ocasionales		1	1	1	1	1	2	1,1	1	Baja	x		x
4		Perfilador de riesgos		1	1	1	3	3	4	1,9	2	Baja	x		x
5		Importaciones y exportaciones		3	3	3	3	1	2	2,6	3	Media	x		x

2.4 Definición de Activos Críticos

De acuerdo con la matriz establecida para la definición de activos críticos y conforme a la necesidad de la de resguardar los activos con nivel de criticidad alto, se establece la siguiente ponderación, considerando el caso de estudio y un diseño de la política de seguridad enfocado a los activos críticos.

De los 72 activos definidos dentro de la Institución pública se establece según la matriz 20 activos denominados como críticos.

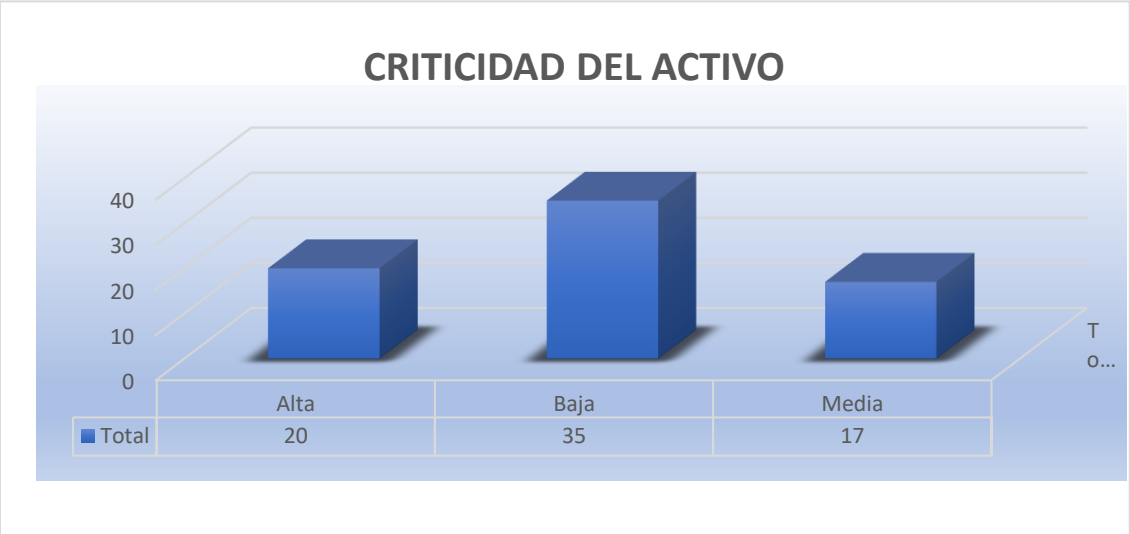


Figura 17. Criticidad del activo

Fuente: Autor de la Investigación

2.5 Definición de la Metodología para la Gestión de Riesgos

2.5.1 Lineamientos

Los dueños de proceso con el acompañamiento del Gestor de Riesgos Tecnológicos y/o quien haga sus veces, son los encargados de tratar los riesgos identificados para los activos tecnológicos, dentro de su área de responsabilidad.

Conforme a las recomendaciones del autor de este documento, la Institución pública, estableció que su metodología de gestión de riesgos tecnológicos se base en los siguientes marcos: COBIT 5 for Risk, ISO 31000 e ISO 27005.

La Institución pública ha definido como “Moderado” su Nivel de Riesgo Aceptable - NRA, el cual corresponde al nivel de riesgo con el que, en conocimiento de las

autoridades, el responsable de tecnología ha decidido convivir, por lo tanto, se establecerán planes de respuesta para los riesgos identificados en los niveles Alto y Extremo.

2.5.2 Roles y responsabilidades

2.5.2.1 Coordinación General de Planificación Estratégica

Asignar obligaciones y responsabilidades para la gestión de riesgos tecnológicos en los niveles respectivos dentro de la organización.

Garantizar la asignación de recursos necesarios para la gestión de riesgos tecnológicos.

Garantizar que el marco de referencia para gestionar el riesgo tecnológico es adecuado a la institución.

Gestionar la implementación de políticas, normas y procedimientos necesarios para la implementación de los planes de tratamiento de activos críticos.

Establecer mecanismos de control apropiados que permitan medir el nivel ejecución de los planes de tratamiento de riesgos tecnológicos.

2.5.2.2 Responsable de Tecnologías de la Información

Liderar la gestión de riesgos tecnológicos.

Comunicar los beneficios de la gestión de riesgos tecnológicos a los interesados.

Apoyar la ejecución del proceso de para una adecuada gestión de riesgos tecnológicos, es decir; identificación, análisis, evaluación y tratamiento.

Apoyar la implementación y evaluación del tratamiento a los riesgos tecnológicos identificados.

2.5.2.3 Administradores de activos tecnológicos (Dueño del Riesgo Tecnológico)

En conjunto con el gestor de riesgos, participar en el proceso de gestión, es decir, identificación, análisis, evaluación y tratamiento del riesgo.

Registrar el proceso de gestión y tratamiento de riesgos tecnológicos en los formatos definidos para ello.

Trabajar de manera integrada en la gestión de riesgos tecnológicos con el grupo o áreas asignadas. Realizar la implementación y evaluación de los planes de tratamiento de los riesgos tecnológicos identificados. Garantizar que los controles implementados sean eficaces y eficientes tanto en el diseño como en la operación.

2.5.2.4 Oficial de Seguridad de la Información

Verificar, evaluar, investigar y supervisar la respuesta a incidentes y las violaciones de políticas, normas y directrices relacionadas con los planes de tratamiento de riesgos tecnológicos.

2.5.3 Metodología de gestión de riesgos tecnológicos

Considerando la frecuencia, la medición del riesgo en este proyecto se lo realizará en función de las siguientes especificaciones:

Tabla 11. Análisis por frecuencia

FRECUENCIA DEL RIESGO		
Improbable	1	No se ha presentado en los últimos 3 años.
Irregular	2	Al menos una vez en los últimos 3 años.
Posible	3	Al menos una vez en los últimos 2 años.
Probable	4	Al menos una vez en el último año.
Muy probable	5	Más de una vez al año.

Fuente: Autor de la Investigación

2.5.3.1 Análisis por impacto

De acuerdo al análisis por impacto se determina las consecuencias que pueden ocasionar a la institución la materialización del riesgo.

Considerando los criterios establecidos y el impacto, se determina que la medición del se define a partir de las siguientes especificaciones:

2.5.3.1.1 Impacto económico al negocio

Determina el nivel de afectación a los procesos de la cadena de valor de aseguramiento de ingresos incluidos en los servicios que la institución pública presta a las empresas ecuatorianas en función de permisos y transporte.

Tabla 12. Impacto económico

Detalle	Nivel
Existe afectación a uno o dos procesos de la cadena de valor de aseguramiento de ingresos.	1
Existe afectación a tres o cuatro procesos de la cadena de valor de aseguramiento de ingresos.	3
Existe afectación a cinco o más procesos de la cadena de valor de aseguramiento de ingresos.	5

Fuente: Autor de la Investigación

2.5.3.1.2 Impacto operativo al negocio

Determina el nivel de afectación de la operación en la institución.

Tabla 13. Impacto operativo

Detalle	Nivel
Afecta menos del 5% de la operación	1
Afecta hasta el 15% de la operación	3
Afecta más del 15% de la operación	5

Fuente: Autor de la Investigación

2.5.3.1.3 Impacto regulatorio o legal

Determina las consecuencias regulatorias o legales, según la necesidad de continuidad del negocio que representa la institución pública de acuerdo con el ámbito administrativo, ejecución del presupuesto y normatividad legal vigente.

Tabla 14. Impacto regulatorio

Detalle	Nivel
El impacto no genera riesgo de multa o demandas.	1
El impacto genera un riesgo mínimo de multa o demandas.	3
El impacto genera un riesgo inminente de multa o demandas.	5

Fuente: Autor de la Investigación

2.5.3.1.4 Impacto de imagen y reputación

Determina la pérdida de la imagen o reputación en el medio público e instituciones adscritas.

Tabla 15. Impacto imagen y reputación

Detalle	Nivel
El impacto que ocasiona la materialización del riesgo en los Clientes Internos	1
El impacto que ocasiona la materialización del riesgo en los Clientes Externos	2
El impacto que ocasiona la materialización del riesgo en los Clientes Gubernamentales	3

Fuente: Autor de la Investigación

2.5.3.1.5 Impacto en la seguridad de la información

Determina el impacto en los principios base de seguridad de la información las cuales son confidencialidad, integridad y disponibilidad de la información procesada los activos críticos tecnológicos.

Tabla 16. Impacto en la seguridad de la información

Detalle	Nivel
El impacto genera afectación en uno de los principios de seguridad de la información.	1
El impacto genera afectación en dos de los principios de seguridad de la información.	2
El impacto genera afectación en los tres principios de seguridad de la información,	3

Fuente: Autor de la Investigación

Cada tipo de impacto analizado aporta un peso para la siguiente ponderación:

Tabla 17. Ponderación de los impactos

No.	Aspectos evaluados	Ponderación
1	Impacto económico al negocio	25%
2	Impacto operativo al negocio	15%
3	Impacto regulatorio o legal	25%
4	Imagen y Reputación	20%
5	Seguridad de la información	15%
TOTAL		**100%**

Fuente: Autor de la Investigación

La ponderación final genera cinco (5) tipos de impactos, mostrados en la siguiente tabla:

Tabla 18. Impacto final

Ponderación de aspectos evaluados	Impacto (Calificación Final)	Descripción
0 – 1	1	Insignificante
1,1 – 2,1	2	Menor
2,2 – 3,2	3	Moderado
3,3 – 3,4	4	Mayor
3,5 – 5	5	Catastrófico

Fuente: Autor de la Investigación

2.5.4 Evaluación del riesgo

Según la Guía de Administración del Riesgo (2015) Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la organización; de esta forma es posible distinguir entre los riesgos aceptables y no inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para evaluar el riesgo se considera la siguiente operación:

Valor del riesgo = Calificación Impacto * Calificación frecuencia

En la Tabla 19. Mapa de calor del riesgo, se muestra la calificación dada para la frecuencia y la para el impacto, es decir, la evaluación del riesgo. Para esto se construye una matriz donde se evalúan estas variables, tal como se muestra a continuación.

Tabla 19. Mapa de calor del riesgo

MAPA DE CALOR DEL RIESGO						
FRECUENCIA	**5 Muy probable**	Alto (5)	Alto (10)	Extremo (15)	Extremo (20)	Extremo (25)
	4 Probable	Moderado (4)	Alto (8)	Alto (12)	Extremo (16)	Extremo (20)
	3 Posible	Baja (3)	Moderado (6)	Alto (9)	Extremo (12)	Extremo (15)
	2 Irregular	Baja (2)	Baja (4)	Moderado (6)	Alto (8)	Extremo (10)
	1 Improbable	Baja (1)	Baja (2)	Moderado (3)	Alto (4)	Alto (5)
IMPACTO		**1 Insignificante**	**2 Menor**	**3 Moderado**	**4 Mayor**	**5 Catastrófico**

La salida de este proceso será una lista de riesgos priorizados acorde con los criterios de valoración.

2.5.5 Efectividad de los controles existentes

Por cada riesgo inherente identificado, se deben relacionar los controles existentes. Así mismo, se determinan las cualidades y características de cada control que tienen la posibilidad de disminuir el nivel de riesgo, desplazarlas a una zona de riesgo menor a la inherente y determinar si definitivamente es aceptable o no.

Lo anterior significa que, dependiendo de la efectividad de los controles asociados (o ya existentes) a cada riesgo, se obtiene un nuevo valor de la frecuencia e impacto al identificar el riesgo residual y determinar el tipo de tratamiento a los riesgos.

La valoración de la efectividad de los controles se determinará por medio de los siguientes parámetros:

Tabla 20. Evaluación del control existente

PARÁMETRO	DESCRIPCIÓN	CRITERIOS	PESO
Naturaleza del control	Determina el nivel de automatización del control	Manual	0,15
		Mixto	0,2
		Automático	0,3
¿El control se encuentra documentado?	Establece si existe evidencia documentada a través de una política, procedimiento, instructivo o guía.	Si	0,3
		No	0
Periodicidad de ejecución	Periodo de tiempo en que se realiza o se ejecuta el control	Diario	0,25
		Semanal	0,2
		Mensual	0,15
		Anual	0,1
		Según ocurrencia	0,05
Responsable	Determina si la responsabilidad de ejecución del control se encuentra definida	Si	0,15
		No	0

Fuente: Autor de la Investigación

Tabla 21. Criterios de efectividad del control existente

CRITERIOS	DEFINICIÓN	NIVEL DE EFECTIVIDAD
Muy Efectivo	Se cuenta con controles eficientes y que garantizan la gestión del riesgo.	>= 0,76
Efectivo	Los controles existentes brindan un nivel de seguridad razonable para la gestión del riesgo.	<0,75 y 0,51
Poco Efectivo	Los controles existentes evidencian un bajo nivel de madurez para la gestión del riesgo.	<0,50

Fuente: Autor de la Investigación

Lo anterior significa que, dependiendo de la efectividad de los controles asociados (o ya existentes) a la gestión de cada riesgo, se obtiene un nuevo valor de la frecuencia e

impacto que ayudan en la determinación del riesgo residual y el tratamiento que se le dará a cada uno de los riesgos.

2.5.6 Tratamiento de riesgos

Los criterios definidos por Institución pública para el adecuado tratamiento de los riesgos tecnológicos son:

- **Evitar el riesgo:** Significa dejar de hacer las actividades o salir de las condiciones que permiten que el riesgo se presente. Evitar el riesgo sólo aplica cuando ninguna otra respuesta al riesgo es adecuada.

Este es el caso cuando:

  - No existe otra respuesta efectiva en costo que pueda ser exitosa para disminuir la frecuencia o el impacto debajo de los umbrales definidos para la tolerancia al riesgo.
  - El riesgo no puede ser compartido o transferido.
  - El nivel de exposición ha sido considerado inaceptable por la Máxima Autoridad.

- **Reducir/Mitigar el riesgo:** significa tomar acciones de mitigación para reducir la frecuencia y/o el impacto de un riesgo.
- **Asumir/Aceptar un riesgo:** aceptar significa que se reconoce la exposición a la pérdida, pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada, en caso de que ocurra. Esto es diferente a no estar consciente de un riesgo; aceptar un riesgo supone que se conoce el riesgo y que las autoridades han tomado una decisión informada para aceptarlo como tal.
- **Compartir/Transferir el riesgo:** Compartir significa reducir la frecuencia o el impacto del riesgo transfiriendo o compartiendo una porción del riesgo. Las técnicas comunes incluyen la contratación de seguros y la externalización.

2.5.7 Plan de tratamiento de riesgo

La Institución pública, establece un plan de tratamiento de los riesgos para los niveles alto y extremo. Dicho plan requiere una definición clara de las actividades a desarrollar

y en cada una se debe contar con el registro de los siguientes ítems, que se llevarán acorde al siguiente formato:

Plan de tratamiento

Tabla 22. Tratamiento de riesgos

Nivel de riesgo	Tratamiento a dar
Bajo	Asumir
Moderado	Asumir
Alto	Reducir – Evitar - Compartir
Extremo	Reducir – Evitar - Compartir

Fuente: Autor de la Investigación

- **Responsable:** es el administrador del activo tecnológico que ejecutará el control descrito en el plazo asignado.
- **Referencia de control:** proporciona una referencia al responsable para la implementación del control establecido, por ejemplo, guías de buenas prácticas, normas ISO, entre otros.
- **Tiempo de ejecución:** establece el inicio y finalización de la implementación del control.

2.5.8 Monitoreo y seguimiento

La Institución pública, realiza el monitoreo y seguimiento a las medidas o controles planteados.

Se debe considerar los siguientes aspectos:

- Modificaciones a los valores de criticidad de los activos tecnológicos.
- Nuevas causantes de riesgos (amenazas y vulnerabilidades).
- Incidentes de seguridad informática y seguridad de la información.
- Cambios en los factores de riesgo.

Así mismo, se ha determinado la realización de la valoración de los riesgos al menos una vez al año y considerando los siguiente:

- La institución.

- Infraestructura Tecnológica.
- Procesos de negocio.

El oficial de seguridad de la información está a cargo del monitoreo y seguimiento del tratamiento del riesgo.

Las actividades definidas para la realización del monitoreo y seguimiento son:

- Auditorías internas y externas de TI.
- Análisis de vulnerabilidades técnicas y Ethical Hacking.
- Seguimiento al cumplimiento de los planes de tratamiento del riesgo.
- Revisión periódica de los controles implementados.

Los controles implementados, con el fin de mitigar el valor del riesgo calculado, deben ser medible a través de su eficacia. La aplicación de un control no necesariamente implica la reducción total del valor de riesgo obtenido, sino la reducción a los niveles de riesgo aceptables establecidos por la Institución pública.

La funcionalidad de los controles debe ser constantemente evaluada; en caso de no obtener los resultados esperados se les deben aplicar las mejoras a través de una nueva aplicación de la metodología PHVA.

2.5.9 Comunicación del riesgo

Es importante un intercambio bidireccional de información y opiniones sobre el riesgo, pues esto promueve una mayor comprensión y determinación de acciones apropiadas para la gestión de estos. Esta comunicación sucede en varias instancias:

- Al realizar el proceso de gestión de riesgos tecnológicos por parte del gestor de riesgos y los administradores de los activos tecnológicos.
- Al materializarse un riesgo de nivel alto o extremo se realiza una reunión con la Alta Dirección, y las demás partes involucradas.
- Anualmente en reunión de revisión por la Alta Dirección.
- En sesiones de capacitación a las partes involucradas.

2.5.10 Definición de Controles Prioritarios para el Desarrollo de Política

Considerando que el marco referencial para este caso de estudio es el Acuerdo Ministerial No.166, el cual detalla el Esquema Gubernamental de Seguridad de la Información, se definen los controles mínimos prioritarios para desarrollar una Política de Seguridad que proteja los activos críticos institucionales.

2.5.11 Identificación de hitos y controles para aplicación de Política de Seguridad:

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
1.	**1. POLITICA DE SEGURIDAD DE LA INFORMACION**	1.1	***1.1. Documento de la Política de la Seguridad de la Información***	1.1.a)	a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (*)(1).
1.				1.1.b)	b) Se difundirá la siguiente política de seguridad de la información como referencia (*): "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". ***(1) (*) En todo este documento esta marca significa que se trata de un control/directriz prioritario*** Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.
2.	**2. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION**	2.1	***2.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información***	2.1.a)	a) Realizar el seguimiento de la puesta en marcha de las normas de este documento (*).
2.				2.1.b)	b) Disponer la difusión, capacitación y sensibilización del contenido de este documento (*).

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
2.		2.2	***2.2. Coordinación de la Gestión de la Seguridad de la Información***	2.2.a)	a) La coordinación estará a cargo del Comité de Gestión de Seguridad de la Información el cual tendrá las siguientes funciones: - Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del CSI. El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará a la máxima autoridad de la institución (*). - Designar formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el director o responsable del área de Tecnologías de la Información de la Institución (*).
2.		2.5.	***2.5. Acuerdos sobre Confidencialidad (*)***	2.5.a)	a) Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI.
2.				2.5.b)	b) Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción.
2.				2.5.c)	c) Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos.
2.				2.5.d)	d) Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción.
2.				2.5.e)	e) Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas, proveedores, pasantes, entre otros) que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de información.
3.	**3. GESTION DE LOS ACTIVOS**	3.1.	***Inventariar los activos de soporte de Hardware (*):***	3.1.j)	j) Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.
3.				3.1.k)	k) Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.
3.				3.1.l)	l) Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.
3.				3.1.m)	m) Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plóter, máquina de fax, etc.
3.				3.1.n)	n) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
					flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.
3.				3.1.o)	o) 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.
3.				3.1.p)	p) Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.
3.				3.1.q)	q) Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.
3.			***3.1. Inventario de activos Inventariar los activos de soporte de Software (*):***	3.1.r)	r) Sistemas operativos.
3.				3.1.s)	s) 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.
3.				3.1.t)	t) 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.
3.				3.1.u)	u) Aplicativos informáticos del negocio.
3.			***3.1. Inventario de activos Inventariar los activos de soporte de redes (*):***	3.1.v)	v) 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.
3.				3.1.w)	w) Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-ppoint, transceiver, equipo terminal de datos, etc.).
3.				3.1.x)	x) Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.
3.				3.1.y)	y) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.
3.		3.3.	***3.3. Uso aceptable de los activos***	3.3.d)	d) Reglamentar el uso de correo electrónico institucional (*):
					- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
					- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
					- Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de las institución.
					- Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
					- La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
					- Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios.
					- Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
					- Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
					- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
					- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.
					- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.
3.				3.3.e)	e) Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios (*):
					- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.
					- Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución.
					- Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
					- El Oficial de Seguridad de la Información debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas.
					- Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.
					- El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.
					- La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.
					- Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.
					- Se prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.
3.		3.4.	***3.4. Directrices de clasificación de la información***	3.4.a)	a) Clasificar la información como pública o confidencial. (*)
4.	**4. SEGURIDAD DE LOS RECURSOS HUMANOS**	4.1.	***4.1. Funciones y responsabilidades***	4.1.a)	a) Verificar a los candidatos, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida (*).
4.				4.1.b)	b) Entregar formalmente a los funcionarios sus funciones y responsabilidades (*).
4.		4.4.	***4.4. Responsabilidades de la dirección a cargo del funcionario***	4.4.a)	a) Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles (*).

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
5.	**5. SEGURIDAD FISICA Y DEL ENTORNO**	5.1.	***5.1. Perímetro de la seguridad física***	5.1.b)	b) Definir una área de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio (*).
5.		5.2.	***5.2. Controles de acceso físico***	5.2.a)	a) Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida (*).
5.				5.2.c)	c) Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas (*).
5.		5.3.	***5.3. Seguridad de oficinas, recintos e instalacio***	5.3.b)	b) Proteger las instalaciones claves de tal manera que se evite el acceso al público (*).
5.				5.3.d)	d) Ubicar las impresoras, copiadoras, etc., en un área protegida(*).
5.		5.4.	***5.4. Protección contra amenazas externas y ambientale***	5.4.d)	d) Realizar mantenimientos de las instalaciones eléctricas y UPS.(*)
5.				5.4.e)	e) Realizar mantenimientos en los sistemas de climatización y ductos de ventilación (*).
5.		5.7.	***5.7. Ubicación y protección de los equipos***	5.7.c)	c) Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información (*).
6.	**6. GESTION DE COMUNICACIONES Y OPERACIONES**	6.1	***6.1. Documentación de los procedimientos de Operación***	6.1.e)	e) Documentar los contactos de soporte, necesarios en caso de incidentes (*).
6.		6.6.	***6.6. Monitoreo y revisión de los servicios, por terceros.***	6.6.b)	b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos (*).
6.				6.6.c)	c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos (*).
6.				6.6.d)	d) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado (*).
6.		6.8.	***6.8. Gestión de la capacidad***	6.8.a)	a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos (*).

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
6.		6.10.	***6.10. Controles contra código malicioso.***	6.10.a)	a) Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado. (*).
6.				6.10.c)	c) Instalar y actualizar periódicamente software de antivirus y contra código malicioso (*).
6.				6.10.d)	d) Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles (*).
6.		6.12.	***6.12. Respaldo de la información.***	6.12.a)	a) Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información (*).
6.				6.12.b)	b) Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención (*).
6.				6.12.c)	c) Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución (*).
6.		6.14.	***6.14. Seguridad de los servicios de la red.***	6.14.a)	a) Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red (*).
6.				6.14.b)	b) Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc. (*)
6.		6.26.	***6.26. Registros de auditorías.***	6.26.h)	h) Registrar los accesos y tipos de acceso (*).
6.				6.26.i)	i) Registrar las direcciones y protocolos de red (*).
6.				6.26.j)	j) Definir alarmas originadas por el sistema de control de acceso(*).
6.				6.26.k)	k) Activación y desactivación de los sistemas de protección como detección de intrusos (IDS) (*).
6.		6.27.	***6.27. Monitoreo de uso del sistema.***	6.27.a)	a) Registrar los accesos autorizados, incluyendo(*):
					- Identificación del ID de usuario; - Fecha y hora de eventos clave; - Tipos de evento; - Archivos a los que se han tenido acceso; - Programas y utilitarios utilizados;
6.				6.27.c)	c) Monitorear intentos de acceso no autorizados, como (*):
					- Acciones de usuario fallidas o rechazadas; - Violación de la política de acceso y notificaciones de firewalls y gateways; - Alertas de los sistemas de detección de intrusos;
6.				6.27.d)	d) Revisar alertas o fallas del sistema, como (*):
					- Alertas y/o mensajes de consola; - Excepciones de registro del sistema; - Alarmas de gestión de red; - Alarmas del sistema de control de acceso;
6.		6.29.	***6.29. Registros del administrador y del***	6.29.a)	a) Incluir al registro, la hora en la que ocurrió el evento (*).
6.				6.29.b)	b) Incluir al registro, información sobre el evento (*).

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
6.				6.29.c)	c) Incluir al registro, la cuenta de administrador y operador que estuvo involucrado (*).
6.				6.29.d)	d) Añadir al registro, los procesos que estuvieron implicados (*).
6.		6.30.	***6.30. Registro de fallas***	6.30.a)	a) Revisar los registros de fallas o errores del sistema (*).
6.				6.30.b)	b) Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles (*).
6.				6.30.c)	c) Asegurar que el registro de fallas esté habilitado (*).
7.	**7. CONTROL DE ACCESO**	7.4.	***7.4. Gestión de contraseñas para usuarios***	7.4.a)	a) Establecer un proceso formal para la asignación y cambio de contraseñas (*).
7.		7.6.	***7.6. Uso de contraseñas***	7.6.a)	a) Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados (*).
7.				7.6.b)	b) Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta (*).
7.				7.6.c)	c) Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables; por ejemplo: admin, administrador, administrador, user, usuario, entre otros (*).
7.				7.6.d)	d) Controlar el cambio periódico de contraseñas de los usuarios (*).
7.				7.6.e)	e) Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información (*).
7.		7.10.	***7.10. Autenticación de usuarios para conexiones externas***	7.10.a)	a) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR) (*).
7.		7.11.	***7.11. Identificación de los equipos en las redes***	7.11.a)	a) Identificar y documentar los equipos que se encuentran en las redes (*).

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
7.		7.12.	***7.12. Protección de los puertos de configuración y diagnóstico remoto***	7.12.b)	b) Los puertos, servicios (ej., fftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados (*).
7.		7.13.	***7.13. Separación en las redes***	7.13.a)	a) Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución (*).
7.		7.15.	***7.15. Control del enrutamiento en la red***	7.15.a)	a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución (*). Las puertas de enlace de la seguridad fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red. Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (LCA), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos de usuarios con salida libre y sin control, en base a las políticas de la institución.
7.		7.16.	***7.16. Procedimiento de registro de inicio seguro***	7.16.a)	a) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada (*).
7.				7.16.b)	b) Llevar un registro de definición para el uso de privilegios especiales del sistema (*).
7.				7.16.c)	c) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema (*).
7.				7.16.d)	d) Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios (*).
7.				7.16.e)	e) Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución (*).
7.				7.16.f)	f) Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente (*).
7.				7.16.i)	i) Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos (*).
7.				7.16.j)	j) Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica (*).
7.		7.17.	***7.17. Identificación y autenticación de***	7.17.a)	a) Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
					responsables de administraciones críticas de la institución (*).
7.				7.17.b)	b) Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado (*).
7.				7.17.d)	d) Evitar el uso de usuarios genéricos (*).
7.				7.17.e)	e) Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación (*).
7.		7.18.	***7.18. Sistema de gestión de contraseñas***	7.18.a)	a) Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible (*).
7.				7.18.b)	b) Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad (*).
7.				7.18.c)	c) Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión (*).
7.		7.25.	***7.25. Computación y comunicaciones móviles***	7.25.a)	a) Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo. (*)
7.		7.26.	***7.26. Trabajo remoto***	7.26.d)	d) No se permite el uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución (*).
7.				7.26.f)	f) Deberá considerarse la protección de antivirus y reglas del Firewall (*).
8.	**8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION**	8.1.	***8.1. Análisis y especificaciones de los requerimientos de seguridad***	8.1.a)	a) Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc. (*).
8.				8.1.b)	b) Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad. (*).
9.	**9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓ**	9.1.	***9.1. Reporte sobre los eventos de seguridad de la información***	9.1.a)	a) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información (*).

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)					
No.	**DOMINIO (D)**	**No.**	**HITO (H)**	**No.**	**CONTROL (C)**
9.				9.1.c)	c) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden (*):
					- Identificar el incidente
					- Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
					- Notificar al Oficial de Seguridad de la Información de la institución.
					- Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
					- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
					- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
					- Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado.
					- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
					- Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
					- Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

Figura 18. Esquema Gubernamental de Seguridad de la Información

Fuente: (Secretaría Nacional de la Administración Pública, 2013)

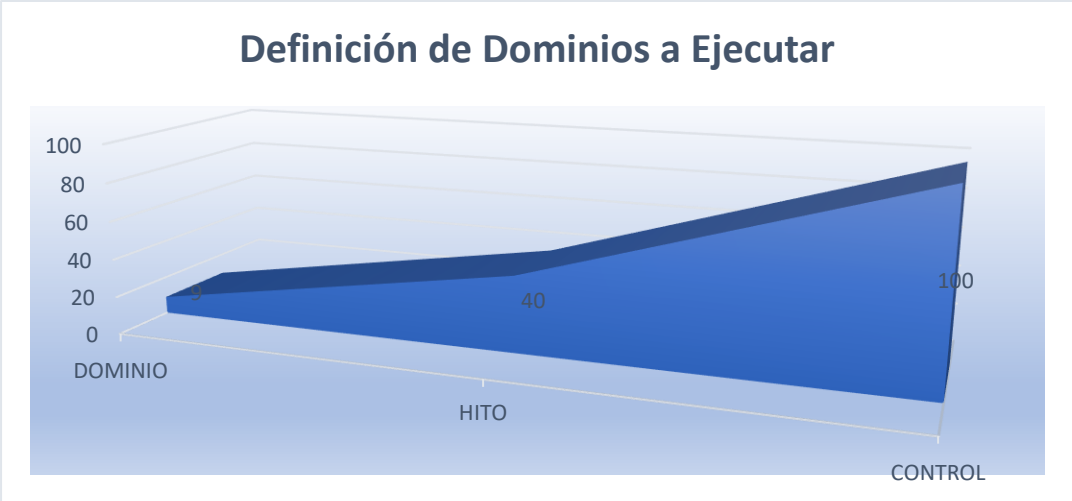
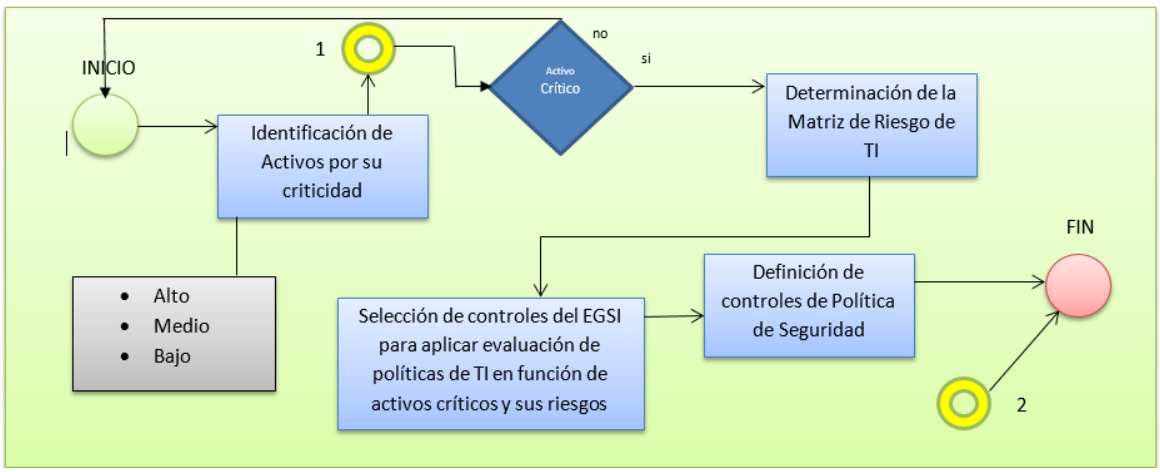


Figura 19. Definición de dominios a ejecutar

Fuente: Autor de la Investigación

2.6 Definición de proceso

Para llevar a cabo el adecuado diseño y elaboración de políticas de seguridad en base a la metodología planteada y bajo los lineamientos del Esquema Gubernamental de Seguridad de la información, es importante definir el proceso que se debe aplicar para su ejecución.



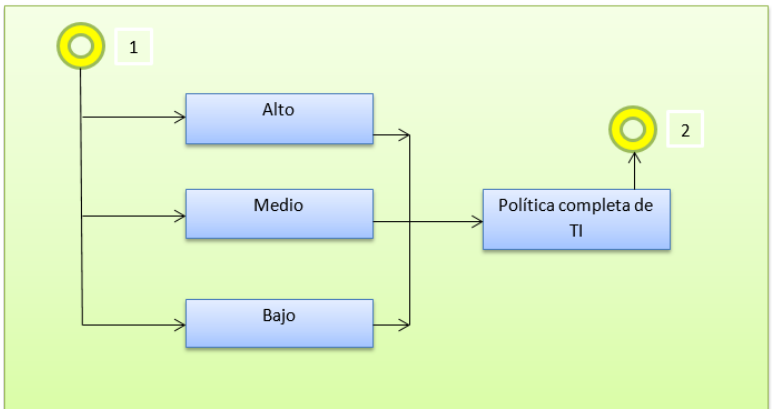


Figura 20. Proceso Política completa de TI

Fuente: Autor de la Investigación

CAPÍTULO III

POLÍTICA

3.1 Validación del análisis para el desarrollo de la política de Seguridad de la Información

De acuerdo al análisis realizado en el capítulo anterior, se considera que una política de seguridad de la información es de vital importancia para la Institución pública siempre y cuando la misma pueda ser aplicada.

La metodología establecida para la generación de la política abarca dos parámetros fundamentales que generalmente son criticidad de activos y gestión de riesgos, los cuales son inobservados por las instituciones públicas y actualmente dedican sus labores a cumplir con los hitos establecidos por el Esquema Gubernamental de Seguridad de la Información EGSI en papel, siendo este el habilitante para ponderar en el ranking del Ministerio de Telecomunicaciones, mientras se procede con la auditoría de la ejecución del cumplimiento de las mismas.

Los controles establecidos permiten salvaguardar la información institucional, considerando que en su mayoría se trabaja con información confidencial, La institución pública al ser una institución transversal, es decir, que trabaja conjuntamente con diferentes instituciones públicas para controlar, registrar, permitir, eliminar y transportar sustancias.

Las identificaciones de los activos críticos permiten establecer las políticas apropiadas para salvaguardar los intereses institucionales y generar un control efectivo para permitir la continuidad de los servicios que presta esta Cartera de Estado.

3.2 Política de Seguridad de la Información

Introducción de aplicación de política de seguridad de la información

3.2.1 Objetivo

Establecer los lineamientos orientados a garantizar y preservar la información organizacional en base a los principios de seguridad de la información:

confidencialidad, integridad y disponibilidad, conforme a los requerimientos de la institución, leyes, normativas y/o regulaciones aplicables.

3.2.2 Alcance

El presente documento y las políticas definidas en él estudio, aplican para todo el ámbito de la Institución pública, su cumplimiento es mandatorio para todos los servidores y terceras partes debidamente autorizadas (auditores, consultores, proveedores, entre otros) que utilicen los activos de información de la institución para el desarrollo de sus actividades o funciones.

3.2.3 Definiciones

a. **Sistema de Gestión de Seguridad de la Información**. Parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información. (ISO27000, 2007)

b. **Política.** Es la definición de principios básicos que la institución está **obligada a cumplir, de acuerdo con las directrices establecidas por la** Máxima Autoridad y considerar una serie de reglas y directrices sobre comportamiento que se espera de sus servidores.

c. **Principios básicos de seguridad.** Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

d. **Confidencialidad.** Es la garantía de que sólo el personal autorizado accede a la información preestablecida.

e. **Integridad.** Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

f. **Disponibilidad.** Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades.

g. **Cumplimiento.** Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones

controladas están sujetos.

h. **Responsable de la información**. Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

i. **Sistema de información.** Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

j. **Gestión de incidentes.** Acciones para atender las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

k. **Gestión de riesgos.** Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

l. **Incidente de seguridad.** Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de la información.

m. **Administración de la continuidad. -** Es un proceso permanente que garantiza la continuidad de las operaciones del negocio a través de la efectividad del mantenimiento del plan de continuidad. (Congreso Nacional de Innovación y Servicios Públicos, 2018)

3.2.4 Responsabilidades

a. Área Responsable y con autoridad para implementar, actualizar y vigilar el cumplimiento de estas políticas: Coordinación de Planificación Estratégica

b. Área responsable de normalización de este documento: Tecnologías de la Información y Comunicación

c. Áreas responsables de conocer y aplicar estas políticas: Todas las áreas de la Institución pública

3.2.5 Referencias

a. Esquema Gubernamental de Seguridad de la Información (EGSI) (Secretaría Nacional de la Administración Pública, 2013)

b. ISO/IEC 27001:2013. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (GES Consultor, 2016)

c. ISO/IEC 27002:2013. Código de Practica para Controles de Seguridad de la Información. (Iso27000.es, 2012)

3.2.6 Principios generales de la seguridad de la información

La Institución pública concede un interés prioritario a la protección de la información considerando su carácter estratégico y como medio para asegurar la continuidad del negocio, sustentado en un conjunto de principios que establecen el marco de los diferentes desarrollos normativos, esquematizando:

a. La seguridad como un proceso integral.

b. Gestión de seguridad basada en análisis de riesgos.

c. Mitigación, reacción y plan de recuperación.

d. Sistemas de defensa.

e. Evaluación periódica.

f. La seguridad como parte de Gobierno de TI.

3.2.7 Objetivos de la seguridad de la información

Los objetivos de la seguridad de la información se encuentran orientados a contribuir, mitigar y controlar los riesgos de la institución, para lo cual la Institución pública definirá una serie de objetivos consistentes, considerando que deberán ser medibles de acuerdo con las métricas definidas por la institución y adicionalmente, deberán ser revisados anualmente con el fin de velar por su alineación con la estrategia de la institución.

3.2.8 Enunciado de la política de seguridad de la información

La Institución pública se compromete a velar por el fiel cumplimiento de la legislación y reglamentación de protección de datos y seguridad de la información, aplicable a todos sus procesos de negocio, salvaguardando la confidencialidad, integridad y disponibilidad de la información, apalancado en una cultura de seguridad y la implementación de estándares que promueven la eficacia de los procesos, mejora continua y madurez del sistema de gestión.

3.3 Política general de seguridad de la información

[EGSI Hito 1.1 Controles: a, b]

Para la Institución pública la administración de la Seguridad de la Información es un proceso global, transversal y que genera valor, basado en lineamientos adecuados a las necesidades de la institución y a los requerimientos regulatorios de acuerdo a su ámbito de competencia.

En la Institución pública la información se considera como un activo fundamental para el cumplimiento de sus actividades institucionales y servicios, en tal virtud existe el compromiso de protección a sus activos más significativos como parte de una estrategia enfocada a la continuidad del negocio, administración de los riesgos y promover una cultura de seguridad.

De acuerdo con las necesidades actuales institucionales, la institución pública implementa un Sistema de Gestión de Seguridad de la Información, herramienta definida para identificar, mitigar y minimizar los riesgos donde se expone la información, dicho sistema apoya a la disminución de costos operativos, concienciando en una cultura de seguridad para velar el cumplimiento de los requerimientos y normativa legal vigente.

El Sistema de Gestión de Seguridad de la Información está basado en la versión más reciente del Esquema Gubernamental de Seguridad de la Información - EGSI /

Acuerdo Ministerial 166 y su operación es competencia de los funcionarios públicos, personas externas, proveedores y todos aquellos que manipulen o accedan a los códigos y aplicativos fuentes, repositorios, recursos de procesamiento y cualquier otro activo de información de la institución, por lo cual se debe adoptar las directrices establecidas en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y disponibilidad de los activos de información.

La Política General de Seguridad de la Información de la Institución pública será soportada por normas, directrices y procedimientos específicos, mediante estándares que garantizan la ejecución del control interno y su efectividad conforme los objetivos y actividades de la institución.

Nota: *Con la aplicación de la política de seguridad de la información se establece una directriz base para controlar los activos de la institución.*

3.3.1 Compromiso de la dirección

[EGSI Hito 2.1 Controles: a, b]

La Máxima Autoridad de la Institución pública promueve la Política de Seguridad de la Información reafirmando su compromiso mediante:

a. El cumplimiento de la normatividad vigente y requisitos aplicables a seguridad de la información.
b. Concienciación para una cultura de seguridad.
c. Destinar los recursos necesarios para la implementación de la política de seguridad.
d. La mejora continua para la ejecución del Esquema Gubernamental de Seguridad de la Información aplicando mejores prácticas para proteger la confidencialidad, integridad y disponibilidad de la información.

Nota: *Se compromete a las autoridades para que avalen la implementación de la política de seguridad de la información.*

3.3.2 Políticas específicas de seguridad de la información

3.3.2.1 Organización de la seguridad de la información

3.3.2.2 Estructura organizacional de seguridad de la información

[EGSI Hito 2.2 Controles: a]

La Institución pública determinará de acuerdo al Esquema Gubernamental de Seguridad de la Información, en el cual se definen roles y responsabilidades que involucren actividades de administración, operación y gestión de la seguridad de la información.

La coordinación la presidirá el Comité de Gestión de Seguridad de la Información con las siguientes funciones:

- Designar formalmente un Oficial de Seguridad de la Información quien coordinará el Comité de Gestión de Seguridad de la Información, es importante considerar que el Oficial de Seguridad no debe pertenecer a la unidad de Tecnologías de la Información, pero deberá tener un conocimiento apropiado para poder manejar cualquier incidente y reportará a la máxima autoridad de la institución.
- Designar formalmente al Responsable de Seguridad del área de Tecnologías de la Información.

Nota: *Se formaliza las designaciones a los responsables de hacer cumplir la política de seguridad.*

3.3.2.3 Uso de dispositivos móviles

[EGSI Hito 3.1 Controles: j]
[EGSI Hito 3.3 Controles: e]

La Institución pública establecerá las condiciones para el manejo de dispositivos

móviles tales como: smartphones, tabletas, laptops, etc., así como dispositivos móviles personales que hagan uso de los servicios de la institución; de igual manera validará que los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la institución.

> ***Nota:*** *Control del equipamiento externo que se conecta a la red interna institucional para mitigar amenazas en los activos críticos institucionales.*

3.3.2.4 Uso de conexiones remotas

[EGSI Hito 7.10 Controles: a]

[EGSI Hito 7.11 Controles: a]

[EGSI Hito 7.26 Controles: d, f]

El área de Tecnologías de la Información definirá los requisitos para el establecimiento de conexiones remotas a la infraestructura tecnológica de la institución pública; de igual manera proveerá herramientas y controles adecuados para que las conexiones estén aseguradas.

> ***Nota:*** *El aseguramiento, control y administración de las aplicaciones se lo establece a través de conexiones seguras mediante uso de VPN.*

3.3.2.5 Seguridad del personal

Vinculación de funcionarios

[EGSI Hito 4.1 Controles: a, b]

La Institución pública identifica la importancia del personal para cumplir con los objetivos establecidos de la institución, referente a contar con un personal capacitado y calificado, de esta manera se garantizará que los nuevos funcionarios no se encuentren impedidos de su derecho al trabajo por los organismos de control.

Al ingreso del nuevo personal a la institución, la Dirección de Talento Humano deberá participar la política de seguridad de la información establecida en este

documento, para conocimiento y aplicación de la misma.

Permanencia y creación de condiciones laborales

[EGSI Hito 4.4 Controles: a]

La Institución pública con la finalidad de proteger la información, aplicaciones y recursos de procesamiento, promoverá al personal que se encuentre debidamente capacitado y concienciado en seguridad de la información para el uso adecuado de los activos de información y ejecutará el respectivo proceso disciplinario por su incumplimiento a las políticas de seguridad de la información de la institución.

Los funcionarios de la institución pública no deben divulgar información confidencial en lugares públicos, conversaciones u otras situaciones que atenten con la seguridad y el buen nombre de la institución de acuerdo al acuerdo de confidencialidad establecido en el ANEXO F.

Desvinculación, licencias, vacaciones o cambio administrativos de los funcionarios

La Institución pública garantizará que sus funcionarios sean desvinculados o reasignados por cambios administrativos para la ejecución de nuevas labores bajo los lineamientos del área de Talento Humano, jefe inmediato de manera controlada y segura.

> ***Nota:*** *La difusión de la política de seguridad permitirá prevenir que el personal de la institución atente contra la confidencialidad, disponibilidad e integridad de la información institucional.*

3.3.2.6 Gestión de activos de información

Responsabilidad por los activos

[EGSI Hito 3.1 Controles: j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y]

La Institución pública al ser propietaria de la información física, información generada, procesada, almacenada y transmitida mediante su plataforma tecnológica,

establecerá responsables de las áreas sobre todos los activos de información, garantizando el cumplimiento de la seguridad de la información.

Todo dispositivo como: estaciones de trabajo, portátiles, impresoras, aplicaciones y demás sistemas de procesamiento de datos; así como archivo físico e información de propiedad de la institución, son activos institucionales que se proporcionan a los funcionarios y terceras personas debidamente autorizadas, para cumplir con los propósitos de la institución.

Los documentos que sean considerados confidenciales o de información sensible de la institución pública y los activos donde esta información se almacena y procesa deben ser asignados a un custodio, debidamente inventariados y clasificados, en función de los requerimientos y criterio sobre el manejo de información emitido por autoridad competente a través de la Coordinación Estratégica de Planificación y su delegado para el cumplimiento del EGSI. Los custodios de los activos de información deberán realizar el levantamiento y actualización del inventario periódicamente.

Clasificación y manejo de la información

[EGSI Hito 3.4 Controles: a]
[EGSI Hito 6.12 Controles: a]

La Institución pública establecerá los niveles de clasificación de la información institucional, de acuerdo con su sensibilidad y definirá lineamientos para clasificar la información, con la finalidad de que los custodios de esta cataloguen y determinen los controles adecuados para su aseguramiento.

Toda la información de la institución pública debe ser identificada, clasificada y documentada de acuerdo con los lineamientos de clasificación de la información establecidos por la máxima autoridad a través del área de Seguridad Informática para el cumplimiento de los lineamientos del EGSI.

Una vez identificada y clasificada la información, la institución garantizará los recursos necesarios para la ejecución y aplicación de controles necesarios con la

finalidad de garantizar la confidencialidad, integridad y disponibilidad de la misma, de esta manera motivar el uso adecuado por parte de los funcionarios de la institución y terceras personas que se encuentren debidamente autorizados para la ejecución de sus actividades.

> ***Nota:*** *La identificación de la y clasificación de la información física o digital que se encuentra en la institución pública es fundamental para definir la criticidad de los activos y aplicaciones que la manejan.*

Uso de periféricos y medios de almacenamiento

[EGSI Hito 2.3 Controles: c]

Para la utilización de periféricos y medios de almacenamiento en los recursos tecnológicos de la institución pública establecerán los respectivos controles por el área de Tecnologías de la Información, tomando en cuenta las actividades realizadas por los funcionarios y su necesidad de uso.

> ***Nota:*** *El aseguramiento de acceso a los periféricos mitiga la fuga de información, así como, la instalación de software malicioso que atente contra la funcionalidad o disponibilidad de la misma en los equipos y aplicaciones institucionales.*

Uso y acceso a internet

[EGSI Hito 3.3 Controles: e]

Asignación del Servicio

1. El acceso a internet será provisto a los/as servidores/as de la Institución pública como una herramienta de apoyo al cumplimiento de sus tareas y actividades laborales; por lo tanto, los privilegios de uso de Internet estarán limitados acorde a la naturaleza de las tareas y actividades a desarrollarse.

2. El uso de navegadores, interfaces o aplicaciones que permitan acceso a Internet,

será definido por la Unidad de Tecnologías de Información y Comunicación. Los computadores de usuario final serán configurados dentro de los perfiles a los servidores/as, luego de su respectiva legalización por parte del área de bienes quien está a cargo de estos equipos.

3. Únicamente se habilitarán a través de la red de datos e internet de la Institución pública los servicios de navegación, en equipos móviles institucionales e invitados con sus debidas restricciones para el correcto funcionamiento de la LAN Institucional.

Categorías del Servicio

El acceso a internet será aprobado y suministrado conforme los permisos y categorías de navegación especificadas por las normas, estándares, procedimientos y políticas establecidas por la Unidad de Tecnologías de Información y Comunicación dentro de la cuales se consideran los siguientes permisos y categorías:

Categoría 1: Estándar

En esta categoría está definida para los usuarios con permisos de navegación general, aplicando el uso del internet para las actividades de búsqueda y navegación que realicen los funcionarios relacionadas con los siguientes temas:

- Herramientas de comunicación entre funcionarios o terceros, que estén asociados a procesos institucionales.
- Revisión en sitios web asociados al cumplimiento de los objetivos institucionales.

(Entidades financieras, instituciones gubernamentales, sitios de educación en general, la descarga de archivos con extensiones de documentación en general (pdf, xls, etc.) y demás sitios que no representen riesgos para la Institución pública.

Categoría 2: Comunicación

Aquellos que, por actividades específicamente asociadas a la institución, el usuario requiera la habilitación a páginas restringidas en la categoría uno, excluyendo páginas de pornografía, música online, etc.

Categoría 3: Autoridades.

Este perfil aplicará de manera exclusiva al Nivel Jerárquico Superior de la institución, la cual mantendrá un acceso preferencial a Redes Sociales, Streaming y demás este nivel incluye las siguientes autoridades:

- Máxima Autoridad
- Miembros
- Coordinadores/as
- Directores/as de Áreas

Servicios a Usuarios Externos

La Unidad de Tecnologías de Información y Comunicación asignará claves temporales de acceso y navegación para estos usuarios, de acuerdo con las normas, procedimientos y políticas vigentes.

Se otorgará temporalmente permisos de navegación en computadoras de escritorio o portátiles que no pertenezcan a los activos tecnológicos la Institución pública, a personas que no sean funcionarios de la institución y que permanecerán temporalmente en la institución, de esta manera poder garantizar su participación en talleres, capacitaciones, eventos y demás actividades relacionadas con los requerimientos de la .

La solicitud para el acceso de internet a terceros deberá realizarla la autoridad responsable del requerimiento, a través de la Mesa de Ayuda con al menos 1 hora de anticipación, a fin de planificar las actividades necesarias y configuración de los servicios tecnológicos solicitados.

Los funcionarios de la Institución pública que interactúen con usuarios finales externos y requieran el acceso a recursos institucionales, serán los responsables de que los accesos se utilicen para la actividad y exclusivamente durante el tiempo autorizado.

Prohibiciones

El acceso a páginas relacionadas con el contenido de adultos, webproxys, hacking, riesgos de seguridad informática o cualquier otra determinada contra la ética, moral, políticas o leyes vigentes.

El acceso y el uso de servicios web 2.0, redes sociales, mensajería instantánea y similar, que tengan como objetivo intercambiar información o para fines diferentes a las actividades de la Institución pública.

La información generada dentro y fuera de la institución no podrá ser intercambiada sin la autorización de la autoridad competente, de sus clientes o de sus funcionarios, con terceros por este medio.

La descarga o uso de videojuegos, música, películas, protectores de pantalla, software no autorizado, información, archivos ejecutables, herramientas, aplicaciones y productos que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica.

La descarga o uso de información audiovisual ajena a las actividades de la Institución pública, que afecten la disponibilidad del servicio.

La navegación a través de la red de datos de equipos móviles particulares.

> ***Nota:*** *El control de acceso a internet evita el ingreso a páginas que puedan contener algún tipo de amenaza informática que pueda comprometer los equipos y por ende la red local, asegurando las aplicaciones críticas.*

3.3.2.7 Control de acceso

Acceso a redes y recursos de red

[EGSI Hito 7.15 Controles: a]

[EGSI Hito 7.16 Controles: f, i, j]

El área responsable de administrar la plataforma tecnológica, las redes de datos y demás recursos de red institucionales deben asegurar que sean debidamente protegidas contra accesos no autorizados a través de controles de acceso lógico.

Administración de acceso de usuarios

[EGSI Hito 7.4 Controles: a]

[EGSI Hito 7.16 Controles: a]

[EGSI Hito 7.17 Controles: d]

La Institución pública por medio de la Coordinación Estratégica de Planificación y el área de Tecnologías de la Información, determinará privilegios para el acceso lógico de los usuarios o grupo de usuarios a las redes de datos, aplicaciones y sistemas de información de la institución.

Asegurará que los funcionarios y terceros tengan acceso exclusivamente a la información necesaria para el desarrollo de sus actividades y esté debidamente regulado por normas y procedimientos establecidos para tal fin.

Responsabilidades de acceso de los usuarios

[EGSI Hito 7.17 Controles: a, b]

[EGSI Hito 7.18 Controles: a, b, c]

Los usuarios de la plataforma tecnológica de la institución pública velarán por el uso adecuado y responsable de los mismos, salvaguardando la seguridad de la información a la cual tienen acceso.

Uso de altos privilegios y utilitarios de administración

[EGSI Hito 7.16 Controles: b, c]

Las Áreas responsables de administrar la plataforma tecnológica, velarán porque los recursos de las aplicaciones y plataforma tecnológica incluyendo los servicios de red de la Institución pública se operen y administren en condiciones controladas y de seguridad informática y de la información, permitiendo un análisis posterior a la actividad de los usuarios con perfiles de administración.

CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

[EGSI Hito 7.6 Controles: a, b, c, d, e]
[EGSI Hito 7.16 Controles: d, e]

La unidad de Tecnologías de la Información como propietaria de los sistemas de información y aplicaciones que contribuyan con la ejecución de procesos, velarán por la adecuada asignación de privilegios para acceder a sus sistemas o aplicativos de manera controlada.

El área responsable de administrar la plataforma tecnológica, sistemas de información y aplicativos, asegurará que estos activos sean debidamente protegidos y eviten accesos no autorizados mediante sistemas de acceso lógico.

Se garantizará que los desarrolladores internos y externos, apliquen las buenas prácticas de desarrollo en las aplicaciones generadas para controlar los accesos y evitar vulnerabilidades en el caso de accesos no autorizados a los sistemas administrados.

> ***Nota:*** *La definición de perfiles para el acceso a redes y aplicaciones controlará la administración y manipulación de los activos críticos, evitando así la ejecución de comandos que puedan comprometer el código fuente o la información alojada dentro de las aplicaciones.*

3.3.2.8 Criptografía

Controles criptográficos

[EGSI Hito 6.14 Controles: a]

[EGSI Hito 7.17 Controles: e]

La Institución pública asegurará que la información será cifrada de acuerdo con lo definido en los lineamientos establecidos para el manejo de activos de información.

> ***Nota:*** *El uso de criptografía asegura la confidencialidad e integridad de la información a pesar de que haya sido vulnerada para que no pueda ser usada por terceros.*

3.3.2.9 Seguridad física y medioambiental

Áreas seguras

La Institución pública establecerá mecanismos de seguridad física y control de accesos que aseguren sus instalaciones en todas sus dependencias y controlará cualquier amenaza física interna o externa, así como las condiciones ambientales de sus oficinas.

Las áreas designadas para el procesamiento o almacenamiento de información, equipos informáticos y redes de comunicaciones que soporten sistemas de información y comunicación serán consideradas como áreas restringidas.

Seguridad para los equipos

[EGSI Hito 5.3 Controles: d]
[EGSI Hito 5.4 Controles: d]
[EGSI Hito 7.25 Controles: a]

La Institución pública para mitigar la pérdida, robo o cualquier peligro de los recursos tecnológicos de la institución ubicados al interior o exterior de sus instalaciones, facilitará los recursos apropiados para mitigar los riesgos sobre el parque informático a través de la Unidad de Tecnologías de la Información.

3.3.2.10 Seguridad en las operaciones

Asignación de responsabilidades operativas

[EGSI Hito 6.6 Controles: c]

[EGSI Hito 6.8 Controles: a]

La Unidad de Tecnologías de la Información de la Institución pública, determinará actividades específicas a sus funcionarios, los cuales serán los encargados de la operación y administración de los recursos tecnológicos, documentando los procesos operativos que se utilicen para ejecutar sus actividades. Evaluará continuamente los controles implantados a los procesos relacionados sobre a los recursos tecnológicos para salvaguardar los parámetros relacionados a la seguridad de la información administrada.

La Unidad de Tecnologías de la Información de la institución, contemplará los requerimientos tecnológicos necesarios para garantizar la capacidad de procesamiento requerida de los aplicativos y sistemas tecnológicos, planificando el aprovisionamiento adecuado para la plataforma tecnológica a mediano y largo plazo, dentro de los parámetros de la obsolescencia tecnológica.

> ***Nota:*** *Se brindará todo el contingente tecnológico necesario para mantener la disponibilidad de la información a nivel de procesamiento y almacenamiento.*

Protección frente a software malicioso

[EGSI Hito 6.10 Controles: a, c, d]

[EGSI Hito 7.26 Controles: f]

La Institución pública asignará los recursos necesarios para la implementación de herramientas de protección de la información y recursos tecnológicos donde se la procesa y almacena, aplicando controles adecuados para evitar la vulneración de los activos tecnológicos, divulgación, alteración o daño permanente ocasionado por el contagio de software malicioso, así también concienciará en aspectos relacionados a

la seguridad de la información a los funcionarios y terceros frente a los ataques de software malicioso.

> ***Nota:*** *El uso de herramientas como antivirus protege ante la infección de código malicioso salvaguardando los aplicativos críticos de la institución.*

Copias de respaldo de la información

[EGSI Hito 6.12 Controles: b, c]

La Unidad de Tecnologías de la Información asegurará la creación de copias de respaldo y almacenamiento de la información sensible, proporcionando los recursos tecnológicos adecuados, estableciendo procedimientos y controles necesarios para la ejecución de esta actividad. Las áreas designadas como custodios de la información, bajo el seguimiento de la Unidad de Tecnologías de la Información definirán la estrategia a seguir para la generación de copias de respaldo, considerando sus periodos de retención y condiciones de almacenamiento. El área responsable de la generación de los respaldos facilitará que los medios magnéticos que poseen la información crítica sean debidamente almacenados y cuenten con controles de seguridad física y medioambiental apropiados.

> ***Nota:*** *El respaldo de la información se priorizará en función de la criticidad de los activos considerando respaldos semanales de acuerdo a la disponibilidad de los sistemas de almacenamiento.*

Eventos y monitoreo de los recursos tecnológicos y los sistemas de información

[EGSI Hito 6.6 Controles: b, d]
[EGSI Hito 6.26 Controles: h, i, j, k]
[EGSI Hito 6.27 Controles: a, c, d]
[EGSI Hito 6.29 Controles: a, b, c, d]
[EGSI Hito 6.30 Controles: a, b, c]

La Unidad de Tecnología de la Información de la Institución pública deberá

monitorear continuamente el uso que dan los funcionarios y terceros a los recursos tecnológicos y sistemas de información de la institución.

Se garantizará el correcto manejo y custodia de los registros de auditoria cumpliendo con la retención de los registros establecidos.

Los Analistas y el Oficial de Seguridad de la Información, definirán las condiciones para el monitoreo y generación de archivos de auditoría en la plataforma tecnológica de la institución, lo cual deberá ser aplicado por las áreas responsables de administrar dicha plataforma.

> ***Nota:*** *La implementación de sistemas de monitoreo permitirá una constante revisión de las redes y aplicativos tecnológicos sobre las posibles amenazas o daños que se pueden suscitar en la institución, garantizando los registros de auditoría para determinar cualquier tipo de fraude tecnológico.*

Control al software operativo

El área de Tecnologías de la Información establecerá roles y perfiles, así como los procedimientos de control para la instalación de aplicaciones, sistemas y paquetes informáticos, se requiere contar con el soporte basado en acuerdos de niveles de servicio, garantizando la funcionalidad de las aplicaciones, sistemas, paquetes informáticos y software operativo.

> ***Nota:*** *La definición de roles y perfiles evita la creación y uso de usuarios genéricos, lo cual garantiza definir a los responsables de cada una de las aplicaciones críticas institucionales.*

Gestión de vulnerabilidades

[EGSI Hito 7.12 Controles: b]
[EGSI Hito 7.13 Controles: a]

La Unidad de Tecnologías de la Información revisará continuamente las vulnerabilidades informáticas en los activos tecnológicos de la institución, para lo cual se deberá realizar pruebas periódicas de escaneos y análisis de vulnerabilidades, con la finalidad de corregir los hallazgos identificados en las pruebas realizadas.

> ***Nota:*** *El análisis de vulnerabilidades de las aplicaciones mitigará posibles amenazas que puedan atentar contra la seguridad de la información institucional.*

Seguridad en las comunicaciones

Gestión y aseguramiento de las redes de datos

La Institución pública a través del área responsable de administrar la plataforma tecnológica, establecerá los controles adecuados para asegurar disponibilidad de redes de datos y servicios de se adhieren a las redes en mención, de igual manera facilitará los insumos necesarios que protejan la integridad y confidencialidad de la información que se transporta en las redes de datos institucionales.

Intercambio de información

[EGSI Hito 2.5 Controles: a, b, c, d, e]

[EGSI Hito 3.3 Controles: d]

La Institución pública deberá salvaguardar la información que se transfiera o intercambie con otras instituciones, generando los controles y procedimientos adecuados para el intercambio de información.

Se establecerán Acuerdos de Confidencialidad para el intercambio de información con terceros y de ser necesario se establecerá un acta de aceptación del riesgo que implique el traspaso de la información, suscritos por los involucrados.

La Unidad de Tecnología de la Información y la Unidad de Talento Humano custodiarán los acuerdos firmados y la información reposará en los expedientes físicos o digitales de cada funcionario. El acuerdo de confidencialidad deberá ser suscrito por los funcionarios al incorporarse a la institución.

Adquisición, desarrollo y mantenimiento de sistemas de información. Establecimiento de requisitos de seguridad

[EGSI Hito 8.1 Controles: a, b]

La Unidad de Tecnología de la Información garantizará que los paquetes y sistemas informáticos adquiridos y desarrollado a la interna de la institución o por parte de terceros, cumplirá con los lineamientos de seguridad definidos desde el área administrativa responsable de la seguridad de la información a través de la normativa y procedimientos vigentes para este fin. Las áreas propietarias de sistemas de información deberán acoger los lineamientos existentes y cuando lo consideren pertinente podrán apoyarse en las diferentes áreas técnicas y/o de gestión, para incluir requisitos de seguridad de la información básicos en la definición de requerimientos.

Los custodios de los sistemas de información deben asegurar que el software generado se encuentra acorde a los requerimientos de seguridad y en conformidad a las pruebas inherentes de desarrollo seguro de software.

> ***Nota:*** *El desarrollo o adquisición de software deberá ser cumplir con los requerimientos básicos de seguridad de la información y se promoverá el uso de herramientas de control de código.*

Desarrollo, aseguramiento de calidad, pruebas y soporte de los aplicativos, sistemas y paquetes informáticos

La Unidad de Tecnología de la Información asegurará que el desarrollo interno o externo de las aplicaciones, sistemas y paquetes informáticos cumpla con los requerimientos de seguridad establecidos, ajustándose a las buenas prácticas para desarrollo seguro, de igual manera se establecerá una metodología para la realización de pruebas de calidad orientadas a su funcionalidad y seguridad del software desarrollado.

Se debe garantizar que exista una adecuada transferencia tecnológica de las

aplicaciones, sistemas o paquetes informáticos desarrollados o adquiridos a la interna o externamente de la institución, asegurando un adecuado nivel de soporte.

> ***Nota:*** *La implementación de sistemas deberá pasar por un control previo de calidad.*

Protección de los datos de prueba

La Unidad de Tecnología de la Información ofuscará y cuidará los datos de prueba que se entregarán a los desarrolladores, asegurando la información determinada como confidencial en los ambientes de producción.

Relación con terceras partes (servicios previstos por terceros)

Condiciones de seguridad de la información para terceros

La Institución pública definirá los controles apropiados para terceras partes, para asegurar que la información institucional que se facilite a dichos actores y se cumpla con los procedimientos, normas y política establecida bajo los lineamientos de seguridad de la información. Los custodios o responsables deberán firmar convenios de confidencialidad que aseguraren la información de esta Cartera de Estado.

Prestación de servicios por terceros

La Institución pública deberá mantener los niveles de seguridad de la información definidos y acuerdos establecidos con proveedores, entidades gubernamentales locales y extranjeras.

Gestión de incidentes de seguridad

Reporte y tratamiento de incidentes de seguridad

[EGSI Hito 6.1 Controles: e]

[EGSI Hito 9.1 Controles: a, c]

La Unidad de Tecnologías de la Información dispondrá a los funcionarios y terceros que utilicen o trabajen con personas, equipos, aplicaciones, sistemas,

paquetes informáticos, medios físicos y de almacenamiento de la institución realicen el reporte de incidentes de seguridad de la información en el caso de presentarse algún incidente.

Se determinará responsables para el tratamiento de los incidentes de seguridad de la información facultados para investigar y solucionar los incidentes reportados, quienes deberán tomar las acciones necesarias para mitigar su reincidencia y realizar el debido escalamiento de acuerdo con su criticidad.

El responsable de tecnología de la información, Oficial de Seguridad o su delegado, serán los únicos autorizados para reportar incidentes de seguridad ante las autoridades competentes y serán el canal de comunicación establecido para hacer pronunciamientos oficiales a la Máxima Autoridad.

Seguridad de la información para garantizar la continuidad del negocio

Continuidad, contingencia y Rollback

La Unidad de Tecnología de la Información, facilitará los recursos adecuados para garantizar una respuesta de los funcionarios, procesos e infraestructura en caso de situaciones de contingencia, daños temporales o eventos catastróficos que atenten contra la seguridad de la información institucional y la continuidad de su operación.

Se deberá planificar el restablecimiento de las operaciones con el menor tiempo y costo, asegurando la información que se transporte o almacene dentro de la infraestructura tecnológica, estableciendo canales de comunicación idóneos entre funcionarios, proveedores y terceros.

Redundancia

El área de Tecnologías de la Información definirá una plataforma tecnológica redundante que cumpla con los parámetros básicos para salvaguardar la información crítica institucional.

Cumplimiento

Cumplimiento con requisitos legales y contractuales

La Unidad de Tecnología de la Información en conjunto con el Oficial de Seguridad de la Institución pública velarán por el cumplimiento de la normativa legal vigente con la seguridad de la información, el mismo que está definido por el Esquema Gubernamental de Seguridad de la Información, así también considerar los derechos de autor y propiedad intelectual de las aplicaciones, sistemas y paquetes informáticos instalados dentro de la institución cumpliendo con los requerimientos legales y de licenciamiento aplicables.

La Coordinación Jurídica en conjunto con el responsable de la seguridad de la información, identificarán, documentarán y actualizarán periódicamente los requisitos legales, contractuales y la regulación relacionada con la seguridad de la información que deba cumplir la institución pública .

Protección de datos personales

La Institución asegurará la protección y privacidad de los datos personales que almacene, procese y transmita de sus clientes, funcionarios y proveedores, acorde con la legislación, reglamentación y regulación aplicable para la institución pública.

3.3.2.11 Revisión y actualización de la política de seguridad de la información

Las políticas de seguridad de la información deberán revisarse como mínimo una vez al año o cuando ocurrieran cambios significativos en la institución que pudieran comprometer su aplicabilidad y eficacia.

3.3.2.12 Incumplimiento y excepciones

El incumplimiento de las presentes políticas se considerará una falta que será observada y considerada para proceder conforme a lo previsto en los reglamentos de la Institución pública y de ser el caso la aplicación de las penas previstas en las leyes

aplicables. No se contempla excepciones a la presente política.

3.3.2.13 Normativa secundaria

La Institución pública a través de la Unidad de Tecnología de la Información, dentro de su ámbito de competencia, instrumentará la Normativa Secundaria necesaria para el estricto cumplimiento de las Políticas de Seguridad de la Información de la institución pública con el fin de asegurar su correcta implementación y despliegue.

CAPÍTULO IV
CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se estableció una política de seguridad de la información para la Institución pública, considerando la criticidad de las aplicaciones para salvaguardar la confidencialidad, disponibilidad e integridad de la información y acorde a los lineamientos del Esquema Gubernamental de Seguridad de la Información.

La Institución pública, no tenía definida una metodología para tratamiento de riesgos y priorización de asignación de recursos, así como la mitigación mediante el uso de una política adecuada que permita brindar seguridad a las actividades de la institución.

Las aplicaciones críticas definidas en el estudio se alinearán a las definiciones establecidas en la política, considerando que los lineamientos propuestas aseguran la continuidad de las mismas y sobre soto resguardar la información ante cualquier tipo de amenaza interna o externa aplicada física o lógicamente.

La metodología aplicada se ajusta a la realidad de la Institución pública, por ende, a las instituciones públicas, considerando que varias no cuentan con una política de seguridad y de poseerla no se aplica, por lo cual con la metodología definida en esta investigación prioriza y categoriza la criticidad de los aplicativos e infraestructura y mantener la continuidad del negocio, así como el tratamiento de los riesgos tecnológicos.

El trabajo realizado permite replicar el modelo a instituciones públicas para

cumplimiento del acuerdo 166, Esquema Gubernamental de Seguridad de la Información, en función de la realidad institucional y volviendo a la política un documento funcional y no de archivo.

La política desarrollada cumple con los parámetros de confidencialidad, integridad y disponibilidad de la información aplicada a los activos críticos de la institución y se proyecta para una implementación y desarrollo de una política global orientada a los activos institucionales de acuerdo con la ponderación de su criticidad y riesgo para su tratamiento personalizado.

Con la ejecución de la política de seguridad de la información, la Institución pública, podrá cumplir a cabalidad con los hitos prioritarios definidos para la medición, conforme el acuerdo ministerial 166, patrocinado actualmente por el MINTEL.

4.2 Recomendaciones

Realizar el procedimiento para los aplicativos críticos de ponderación media y baja, de acuerdo con el tratamiento de riesgos para madurar la institución a nivel tecnológico y de esta manera cubrir todas las aristas que comprende la elaboración de una política de seguridad y su ejecución.

Aplicar políticas de control de seguridad de la información de acuerdo a un análisis de la criticidad y riesgo de sus activos aplicando la metodología desarrollada en este estudio para priorizar los activos y permitir la continuidad del servicio.

Revisar la política de seguridad una vez al año con la finalidad de mantener actualizada en función de las nuevas adquisiciones o desarrollos internos realizados y según la competencia de la institución mantener la ponderación establecida o actualizarla conforme a la metodología.

Definir un oficial de seguridad con conocimientos de tecnología, para el seguimiento y definición de nuevas directrices, ya que se debe contar con criterio técnico apropiado

BIBLIOGRAFÍA

Acosta, W. (29 de Febrero de 2016). *https://prezi.com/cuezzkaa1zcb/esquema-gubernamental-de-seguridad-egsi/*. Obtenido de https://prezi.com/cuezzkaa1zcb/esquema-gubernamental-de-seguridad-egsi/

Advisera Expert Solutions Ltd. (2018). *Qué es norma ISO 27001*. Obtenido de http://advisera.com/27001academy/es/que

Alvarado Peñaranda, M. (29 de Mayo de 2015). *Áreas principales de la norma ISO 27002.* Obtenido de http://maye139.blogspot.com/2015/05/areas-principales-de-la-norma-iso-27002.html

Bitcompany. (09 de Abril de 2015). *CobiT: Un marco de referencia para la información y la tecnología.* Obtenido de http://www.bitcompany.biz/que-es-cobit/#.WdaAzDVrzIU

Cibertec. (2016). *Que es COBIT.* Obtenido de https://www.cibertec.edu.pe/extension-profesional/certificaciones-internacionales/cursos-cobit/que-es-cobit/

Colegio Oficial de Ingenieros de Telecomunicaciones. (2009). *www.coit.es.* Obtenido de https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Congreso Nacional de Innovación y Servicios Públicos. (2018). *http://www.cnis.es.* Obtenido de http://www.cnis.es/glosario-seguridad/

Departamento Administrativo de la Función Pública . (2015). *Guía de Administración del Riesgo.* Obtenido de www.ufps.edu.co

Galán, M. (29 de Mayo de 2009). Obtenido de http://manuelgalan.blogspot.com/2009/05/la-entrevista-en-investigacion.html

Galán, Manuel. (29 de Mayo de 2009). *Entrevista.* Obtenido de http://manuelgalan.blogspot.com/2009/05/la-entrevista-en-investigacion.html

GES Consultor. (Julio de 2016). *ISO 27001 – Sistema de Gestión de la Seguridad de la Información*. Obtenido de http://www.gesconsultor.com/iso-27001.html

Gild, A. (2014). *Análisis del riesgo y el sistema de gestión de seguridad de la información.* Obtenido de http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf

Icontec. (16 de 02 de 2011). *Norma Técnica Colombiana ISO 31000*. Obtenido de https://www.slideshare.net/danielyand1/ntciso-310002011

ISACA. (10 de 07 de 2017). *COBIT 5 for Risk—A Powerful Tool for Risk Management*. Obtenido de http://www.isaca.org/COBIT/focus/Pages/cobit-5-for-risk-a-powerful-tool-for-risk-management.aspx

ISACA. (2017). *What is Cobit 5?* Obtenido de http://www.isaca.org/cobit/pages/default.aspx

ISO Tools. (20 de Febrero de 2015). *¿En qué consiste el ciclo PHVA de mejora continua?* Obtenido de https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

ISO TOOLS. (20 de febrero de 2015). *En qué consiste el ciclo PHVA de mejora continua.* Obtenido de https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

ISO Tools Excellence. (14 de 06 de 2016). *La norma ISO 27002 complemento para la ISO 27001*. Obtenido de https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

ISO27000. (10 de 9 de 2007). *http://www.iso27000.es.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Iso27000.es. (2012). *ISO/IEC 27002.* Recuperado el 19 de Agosto de 2017, de El portal de ISO 27001 en Español: http://www.iso27000.es/iso27000.html

iTTalent. (2015). *Buenas Prácticas de Gestión de Tecnología.* Obtenido de http://www.ittalent.com.co/buenas-pr-cticas-gesti-n-de-ti.html

Ladino, M. I., Villas, P. A., & López, A. M. (Abril de 2011). Fundamentos de la ISO 27001 y su aplicación en las empressas. *Scientia et Technica*, 3. Obtenido de http://www.redalyc.org/html/849/84921327061/

Malhorta, N. (24 de Marzo de 2004). *Investigación de Mercados (4ta ed.).* México: Pearson Educación. Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lad/arenas_m_a/capitulo3.pdf

Martínez Orencio, A. (17 de Junio de 2013). *La información en la organización, su gestión y auditoría.* Obtenido de Gestiopolis: https://www.gestiopolis.com/la-informacion-en-la-organizacion-su-gestion-y-auditoria/

Mesquida, A. L., Esperança Amengual, A. M., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. *Revista Española de Innovación, 6*(3), 21. Obtenido de http://www.redalyc.org/html/922/92218768002/

Padinas. (26 de Noviembre de 2005:89). *Técnicas de Levantamiento de Requerimientos.* Obtenido de https://monivela.wordpress.com/requerimientos/tecnicas-de-levantamiento-de-requerimientos/

Portal ISO 27000. (2013). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Ramírez, A. (2011). *Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios*. Obtenido de http://www.redalyc.org/html/4988/498850173005/

Registro Oficial 776. (15 de Junio de 2016). *Acuerdo Ministerial 166.* Obtenido de https://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

Secretaría Nacional de la Administración Pública. (2013). *Esquema Gubernamental de Seguridad de la Informacion - EGSI* . Obtenido de http://www.gobiernoelectronico.gob.ec/egsi

Institución pública. (2016, Octubre). *Plan Estratégico.* Retrieved from http://intranet.institucionpublica.gob.ec/documentacion/planestrategico

Institución pública. (2017). *Institución pública > > Organigrama* . Obtenido de http://www.institucionpublica.gob.ec/?p=633

Seguridad Informática. (11 de Junio de 2008). *Más información sobre ISO 27005:2008.* Obtenido de https://seguinfo.wordpress.com/category/iso/page/23/

Servicio Ecuatoriano de Normalización. (Febrero de 2015). *http://docplayer.es*. Obtenido de http://docplayer.es/48819724-Nte-inen-iso-iec-27002.html

SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. (3 de Agosto de 2017). *Norma ISO 27002: El dominio política de seguridad.* Obtenido de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Sistemas de Gestión de Seguridad de la Información SGSI. (14 de Junio de 2016). *La norma ISO 27002 complemento para la ISO 27001.* Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Informacióncerrojo: http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

Sistemas de Gestión de Seguridad de la Información SGSI. (14 de Junio de 2016). *La norma ISO 27002 complemento para la ISO 27001.* Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Informacióncerrojo.