UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para la Dirección General de Seguridad Ciudadana y Orden Público de la Comandancia General de la Policía Nacional - DGSCyOP.

Eduardo Sebastián Guacapiña Centeno

Ingeniería en Ciencias de la Computación

Proyecto integrador de fin de carrera presentado como requisito para la obtención del título de Ingeniero en Ciencias de la Computación

Quito, 18 de julio de 2022

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de ciencia e ingenierías

HOJA DE CALIFICACIÓN
DE TRABAJO DE FIN DE CARRERA

Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para la Dirección General de Seguridad Ciudadana y Orden Público de la Comandancia General de la Policía Nacional - DGSCyOP.

Eduardo Sebastián Guacapiña Centeno

Nombre del profesor, Título académico Noel Pérez Pérez, Ingeniero

Quito, 18 de julio de 2022

© DERECHOS DE AUTOR

Nombres y apellidos: Eduardo Sebastián Guacapiña Centeno

Código: 200620

Cédula de identidad: 1722306006

Lugar y fecha: Quito, 18 de julio de 2022

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

RESUMEN

El objetivo del proyecto es diseñar un sistema de seguridad de la información basado en la norma internacional ISO/IEC 27001 para la Dirección General de Seguridad Ciudadana y Orden Público de la Comandancia General de la Policía Nacional del Ecuador. El Sistema de Gestión de Seguridad de la Información, funcionará como metodología para establecer procedimientos, políticas y controles con el objeto de minimizar los riesgos que la Dirección pueda estar expuesta, como, por ejemplo: fraudes internos, robo y fuga de información, ataques de hackeo externo o penetración no autorizada a su infraestructura tecnológica. El sistema aportará de manera positiva al adecuado manejo y gestión de la información dentro de la Dirección General de Seguridad Ciudadana y Orden Público, garantizando la integridad, confidencialidad y disponibilidad de su información. Implementando así una estructura fuerte la cual pueda ser aplicada y mejorada en otras direcciones de la institución policial ecuatoriana.

Palabras clave: políticas, procedimientos, hackeo, confidencialidad, disponibilidad, información, seguridad.

ABSTRACT

The objective of the project is to design an information security system based on the international standard ISO/IEC 27001 for the General Directorate of Citizen Security and Public Order of the General Command of the National Police of Ecuador. The Information Security Management System will work as a methodology to establish procedures, policies and controls in order to minimize the risks that the Directorate may be exposed to, such as: internal fraud, theft and leakage of information, hacking attacks external or unauthorized penetration of its technological infrastructure. The system will contribute positively to the proper handling and management of information within the General Directorate of Citizen Security and Public Order, guaranteeing the integrity, confidentiality and availability of your information. Thus, implementing a strong structure which can be applied and improved in other Directorates of the Ecuadorian Police institution.

Keywords: policies, procedures, hacking, confidentiality, availability, information, security.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1: INTRODUCCIÓN

1.1. ANTECEDENTES

A nivel mundial, la gestión de riesgos y la seguridad de la información son áreas muy importantes dentro de las organizaciones, las cuales no se han desarrollado y administrado de manera adecuada.

Un caso especial son las instituciones públicas, más aún, considerando que en los últimos años han sido víctimas de fraudes internos, robo y fuga de información, ataques externos por personal no autorizado mediante técnicas de hackeo y penetración a su infraestructura tecnológica y ataques de ingeniería social dirigidos al personal que labora en estas instituciones.

De estos incidentes y riesgos relacionados con seguridad de la información mencionados anteriormente, la Dirección General de Seguridad Ciudadana y Orden Público de la Comandancia General de la Policía Nacional (en adelante DGSCyOP) no está exenta. Por el contrario, se convierte en un objetivo atractivo para los delincuentes informáticos.

Para la DGSCyOP la información es un recurso de vital importancia por la labor que desempeña a nivel del Distrito Metropolitano de Quito y del país. Debido a esto, se debe gestionar eficientemente la seguridad de la información, tomando en cuenta que en nuestro país son más frecuentes las amenazas sobre los sistemas informáticos y la infraestructura tecnológica que los soporta.

Esto genera que la información se encuentre en un riesgo constante de ser robada o usada inapropiadamente por personal no autorizado, por lo que, la elaboración e implantación de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI), basado en la norma internacional ISO 27001, generará un aporte sustancial para administrar de forma adecuada y segura la información en la DGSCyOP, la misma que a la presente fecha no cuenta con un SGSI que le asegure la integridad, disponibilidad y confidencialidad de la información.

Cuando se considera el área de seguridad de la información, existen diferentes estándares aplicables. Sin embargo, para el proyecto integrador de fin de carrera, se ha optado por la norma internacional ISO/IEC 27001, que establece los requisitos para la implementación de un SGSI, así como los objetivos de control y controles para cada uno de los dominios o procesos definidos en esta norma, los cuales se encuentran descritos en el Anexo A que

también es parte de la norma (El Anexo A forma parte del Anexo III – Declaración de Aplicabilidad de este documento); con lo cual se podrá cumplir con el objetivo de implementar un SGSI en la Dirección.

1.2. OBJETIVOS

El Objetivo principal de este proyecto es definir una propuesta de diseño de un SGSI inicial en la DGSCyOP, que permita proteger sus recursos y activos de información, así como la tecnología utilizada para el procesamiento de los mismos, para asegurar el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de la información.

La implementación del diseño del sistema propuesto permitirá:

- Gestionar la seguridad de la información como apoyo a la estrategia institucional.
- Establecer medidas y controles adecuados durante todo el ciclo de vida de la información (creación, tratamiento, almacenamiento, transmisión, eliminación y destrucción).
- Optimizar el desempeño de la Gestión de Seguridad de la Información aplicando mejores prácticas y controles.
- Dar cumplimiento al marco regulatorio y normativo de los organismos de control que tenga relación con la seguridad de la información a los que está sujeta la Comandancia General de la Policía Nacional.

1.3. ALCANCE

El alcance propuesto es el siguiente:

1. Realizar una evaluación y diagnóstico inicial en Gestión de Seguridad de la Información en la DGSCyOP. Este diagnóstico permitirá evaluar los mecanismos existentes para procesar información y controlar vulnerabilidades.

2. Diseñar una propuesta de un SGSI de acuerdo con las directrices de las normas internacionales ISO 27001 (Sistemas de Gestión de Seguridad de la Información-Requisitos) e ISO 27002 (Código de Prácticas para los Controles de Seguridad de la Información), que incluya:

    - Gestión de riesgos de seguridad de la información.

- Declaración de aplicabilidad de los dominios, objetivos de control y controles de acuerdo al Anexo A de la norma ISO 27001 (El Anexo A forma parte del Anexo III – Declaración de Aplicabilidad de este documento), que se implementarán como parte de la propuesta del SGSI en la DGSCyOP, que incluirá al menos:
    - Políticas de seguridad de la información.
    - Estructura y organización de la seguridad de la información.
    - Gestión de activos.
    - Seguridad física y ambiental.
    - Control de accesos.
    - Seguridad en las operaciones.
    - Seguridad en las comunicaciones.
    - Gestión de incidentes de seguridad de la información.

3. Levantamiento, valoración y clasificación de los activos informáticos y de soporte de la DGSCyOP.
4. Documentar los controles seleccionados para el SGSI de la Dirección.
5. Establecer la estructura de documentos para el SGSI.

CAPÍTULO 2: FUNDAMENTOS TEÓRICOS

En este capítulo, se incluirá todos los fundamentos teóricos sobre los temas tratados en este proyecto, con el objetivo de proporcionar una idea general sobre conceptos y metodologías aplicadas.

2.1. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se refiere a un conjunto de medidas de precaución y respuestas que permiten proteger y asegurar la información. Este tipo de seguridad es fundamental para que organizaciones o empresas puedan realizar sus operaciones sin correr demasiados riesgos, debido a que, para las instituciones anteriormente mencionadas, los datos que se manejan pueden ser esenciales y pueden marcar el presente o el futuro de las mismas (Areitio, 2008).

De acuerdo con la norma ISO 27001 existen tres definiciones o propiedades importantes y fundamentales para gestionar la información, que son:

- Confidencialidad: la propiedad de que la información esté siempre disponible y no sea divulgada sin autorización a personas u otras entidades.
- Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos.
- Disponibilidad: la propiedad de tener disponibilidad y ser usable en el momento que se necesite.

En general, seguridad es un concepto que se asocia con la falta de riesgos. Podemos entender la seguridad como el estado de cualquier sistema o información, sin importar que sea informático o no, que nos demuestre que está libre de riesgos o peligros. Podemos entender como riesgo a todo aquello que tenga posibilidad de afectar el funcionamiento o resultados obtenidos. (Definición del concepto de seguridad, 2020).

2.2. SGSI

La norma ISO 27001 define al SGSI como una parte del sistema gerencial general que se enfoca en riesgos empresariales para establecer, implementar, operar, monitorear y revisar. Es importante entender que en el sistema gerencial están incluidas políticas, estructura organizacional, responsabilidades, procedimientos, procesos, recursos y actividades.

Las principales ventajas que proporciona el SGSI son:

- Conocer a profundidad sobre la organización y su funcionamiento, proporcionando un plan de mejora continua para resolver posibles problemas y riesgos referentes a la seguridad de la información.
- Evaluar y analizar riesgos e identificar amenazas, vulnerabilidades y el impacto que pueden tener en las actividades de una institución.
- Crear e implementar planes de mejora continua para gestionar la seguridad de la información.
- Asegurar la disponibilidad y continuidad de las operaciones.
- Disminuir los costos relacionados con los eventos de seguridad de la información reportados.
- Aumentar el nivel de confianza con usuarios y clientes de los diferentes sistemas y aplicativos informáticos.
- Contribuir en el incremento del valor y calidad de los servicios y productos ofertados, mejorando la imagen institucional.
- Permite el cumplimiento de leyes, normas y regulaciones (nacionales como internacionales) de seguridad de la información, relacionadas con e-commerce, protección de datos personales, propiedad intelectual, etc.

2.3. METODOLOGÍA MAGERIT

MAGERIT son las siglas de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Su nombre define perfectamente esta metodología que consiste en analizar y gestionar los riesgos de los sistemas informáticos, desarrollada por el Consejo Superior de Administración Electrónica de España.

Es una metodología sistemática que facilita la evaluación y análisis de riesgos vinculados con las Tecnologías de la Información y Comunicación (TIC), la cual ha sido desarrollada para implementar medidas de control adecuadas y reducir el riesgo. MAGERIT recopila en un documento diferentes métodos y ejemplifica el cómo realizar análisis de riesgos (MHAP, 2012).

En general, MAGERIT se basa en un análisis del impacto que una brecha de seguridad podría tener en una empresa o institución, identificando diferentes amenazas que puedan afectar a una institución y diferentes vulnerabilidades que se puedan aprovechar por estas amenazas. Se obtiene una clara definición de cuáles son las medidas de prevención y corrección más adecuadas.

Esta metodología proporciona una guía completa para realizar un análisis de riesgo. Se divide en tres libros, el primero se refiere a la Metodología, que especifica la estructura que hay que tener en un modelo de gestión de riesgos. El libro se encuentra en línea con la ISO 31000 en términos de gestión de riesgos (Gutiérrez, 2013).

De acuerdo con MAGERIT, para realizar la gestión de riesgos de manera correcta se deben aplicar dos tareas importantes:

- Análisis de riesgos, el cual permite encontrar la situación general de la institución y realizar una estimación de lo que podría ocurrir.
- Tratamiento de los riesgos, el cual permite implementar o mejorar medidas y controles que minimizan el nivel de riesgo al mínimo posible o al aceptado por la organización.

La siguiente figura describe las etapas del proceso de gestión de riesgos que establece la metodología MAGERIT, el mismo que se aplicará para efectuar el análisis de riesgos de activos informáticos en la DGSCyOP:

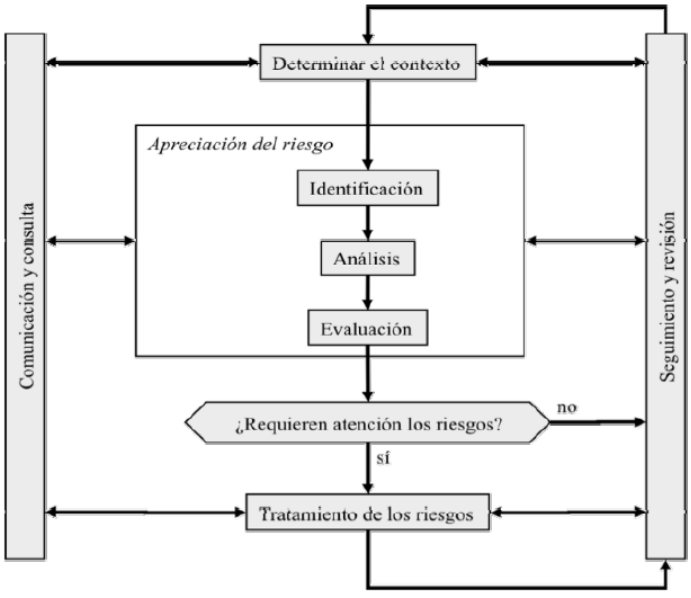

Figura 1. Etapas del proceso de gestión de riesgos metodología MAGERIT.

Fuente: MAGERIT vs3. Libro I, 2012.

Este proceso se alinea con la norma internacional ISO 31000, que establece las directrices y principios para gestionar el riesgo de las organizaciones.

2.4. NORMAS ISO

"Los estándares ISO son un grupo de normas reconocidas internacionalmente, definidas con el objetivo de ayudar a las organizaciones a mantener diversos grados de estandarización en términos de gestión, entrega y desarrollo de productos en la industria". (Gallego, 2021).

Las iniciales ISO significan "International Organization for Standardization". El origen de esta organización se remonta a 1946. La unión de varios organismos de relación y estandarización dieron como resultado la ISO. Desde entonces, se han creado más de veintitrés mil estándares hasta el día de hoy para una gran cantidad de áreas de tecnología, gestión y procesos de producción. Esta es una organización no gubernamental, de la que forman parte ciento sesenta y cuatro países, con setecientos ochenta y un comités y subcomités técnicos inmersos en el desarrollo de estándares. Su secretaría Central se encuentra en Ginebra, Suiza (Gallego, 2021).

2.5. NORMAS ISO 27000

ISO 27000 es un grupo de normas internacionales referentes a Seguridad de la Información que contiene un conjunto de buenas prácticas y guías para diseñar, implementar, mantener y mejorar el SGSI (ISO2700.ES, 2022).

Esta norma facilita un marco de seguridad de la información estandarizado para su uso dentro de una organización o empresa e incluye un conjunto de estándares (López, s. f.), que permiten:

- Establecer un SGSI.
- Evaluación de riesgos.
- Implementar controles.

"Un Sistema de Gestión de la Seguridad de la Información (SGSI), es un conjunto de políticas y procesos diseñados para crear un estándar en la gestión de la Seguridad de la

Información". (ISO2700.ES, 2022). Los principales estándares que conforman el conjunto de normas ISO 27000 son:

- ISO 27000: incluye el vocabulario que define toda la terminología utilizada en las diferentes normas que conforman la familia.
- ISO 27001: incluye un grupo de requerimientos para la implementación de un SGSI. Esta es la única norma de las mencionadas que se puede certificar, incluye una sección principal que se basa en un ciclo de mejora continua y el Anexo A, que detalla los objetivos y medidas de control propuestas por la norma.
- ISO 27002: cuenta con un grupo de buenas prácticas para la seguridad de la información las cuales describen los diferentes objetivos de control y controles de cada uno. En la actualidad se cuenta con 14 dominios, 35 objetivos de control y 114 controles.
- ISO 27003: es una guía para implementar un SGSI. Funciona como soporte para el estándar ISO 27001, que indica los lineamientos generales necesarios para una correcta implementación del SGSI. Incluyendo indicaciones para lograr implementar un SGSI de manera correcta.
- ISO 27004: contiene un conjunto de recomendaciones para medir y calcular datos sobre la gestión de la seguridad de la información. Define como establecer métricas, qué se debe medir, con qué frecuencia, cómo medir y cómo alcanzar los objetivos.
- ISO 27005: esta es una guía que brinda recomendaciones para gestionar riesgos de seguridad de la información que pueden dañar a las instituciones. No se incluye una metodología de gestión y análisis de riesgos específica, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.
- ISO 27006: es un grupo de requisitos para las instituciones certificadoras para que tengan la acreditación de la norma.
- ISO 27007: es una guía para realizar auditorías al SGSI. Define qué se debe auditar y el tiempo en el que hay que realizarlo, la asignación de auditores adecuados, planificar y ejecutar la auditoría, los procesos clave, etc.

2.6. ISO 27001

El estándar 27001 es el principal de toda la serie, este incluye los requerimientos para el diseño, implementación, mantenimiento y mejora continua de un SGSI. La inclusión de un

SGSI dentro de una institución es una decisión estratégica. Crear e implementar un SGSI dentro de una institución se debe a la necesidad de apoyar en el cumplimiento de los objetivos de la misma, los requerimientos de seguridad, los procedimientos organizacionales utilizados, el tamaño y la estructuración de la organización.

El estándar 27001 incluye un conjunto de normas para el control de la seguridad de la información. Según los principales criterios de esta serie de normas, la seguridad de la información es la protección de la integridad, confidencialidad y disponibilidad, así como la protección de los sistemas involucrados en su procesamiento (NTP-ISO/IEC Norma ISO 27001, 2014).

El modelo de sistema de gestión de seguridad de la información ISO 27001 se basa en una estructura PHVA (Planificar-Hacer-Verificar-Actuar). El proceso comienza con la planificación del alcance del SGSI, definiendo las áreas organizacionales a los que se aplicará el sistema (Normas ISO, s. f.).

El alcance debe definirse seleccionando las áreas más importantes o necesarias relacionadas con la gestión de seguridad de la información. Una vez que se define el alcance, se tiene que desarrollar una estrategia para gestionar la seguridad de la información que proporciona las directrices generales que la institución tiene que considerar ante las amenazas informáticas emergentes, teniendo en cuenta los requerimientos legales, establecidos y específicos de la misma.

La idea principal de la planificación del SGSI es determinar el riesgo de la información sobre amenazas y vulnerabilidades sensibles que las organizaciones pueden presentar, enfatizando los términos de confiabilidad, seguridad e información disponible (NTP-ISO/IEC Norma ISO 27001, 2014). Una vez se hayan identificado las amenazas y se haya realizado su análisis y evaluación, se desarrollará un plan de control de riesgos que incluye documentación y guías sobre los procesos que se deben seguir para aplicar los controles, además de capacitar y concientizar a los funcionarios sobre la seguridad informática en la institución y los controles que se deben aplicar. El Anexo A incluido en la norma ISO 27001 incluye un resumen de los controles por dominio, los cuales se detallan en la norma ISO 27002.

2.7. ISO 27002

Cuenta con un conjunto de buenas prácticas para la seguridad de la información las cuales describen los diferentes objetivos de control y controles de cada uno. En la actualidad se cuenta con 14 dominios, 35 objetivos de control y 114 controles. No es una norma certificable (UNE-ISO/IEC 27002, 2015).

Esta norma internacional tiene como objetivo ser una referencia para la selección de controles para el procedimiento de implementación del SGSI basado en la norma ISO 27001. Además, se puede utilizar como guía para la implementación de controles de seguridad de la información aceptables.

Esta norma se encuentra estructurada por 14 capítulos en los cuales se definen controles de seguridad, que abarcan 35 categorías de seguridad y 114 controles. El orden que tienen los capítulos de este estándar no define una mayor importancia u orden de aplicación. En algunas situaciones o contextos, todos los controles de seguridad pueden tener la misma importancia o criticidad, debido a esto, todas las instituciones que implementen este estándar deberán seleccionar los controles que requieran y que más se ajusten a sus objetivos de seguridad y a sus procesos. (UNE-ISO/IEC 27002, 2015).

Cada categoría de control contiene:

- Un objetivo de control define qué es lo que se desea cumplir.
- Se puede aplicar más de un control para cumplir el objetivo del control.
- Guía de implementación que da información con mayor detalle para apoyar la implementación del control y después del objetivo del control.
- Información extra que puede ser necesaria tomar en cuenta. Por ejemplo, consideraciones legales y referencias a otros estándares.

2.8. ÁREAS (DOMINIOS) DE LA ISO 27001

La norma ISO 27001, a través de su Anexo A, describe las áreas o dominios en los que se divide la gestión de seguridad de la información, estos son:

1. Políticas de seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad relativa a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.
7. Seguridad física y del entorno.
8. Seguridad de las operaciones.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de sistemas de información.
11. Relación con proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información para la gestión de continuidad del negocio.
14. Cumplimiento.

2.9. ESTRUCTURA DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA NORMA ISO 27001

De acuerdo con Atehortua, Bustamante & Valencia de los Ríos (2008), el modelo del SGSI de la norma ISO 27001 sigue una estructura PHVA (Planificar, Hacer, Verificar, Actuar), conocido como el ciclo Deming[1], que es un modelo para la implementación de estrategias de mejoramiento continuo en las organizaciones.

La siguiente figura representa el modelo del SGSI de la norma ISO 27001 basado en el ciclo de Deming (Atehortua, Bustamante & Valencia de los Ríos, 2008):

[1] El nombre proviene de Edwards Deming, el principal promotor, pero también es conocido como el ciclo PHVA que significa Planificar, Hacer, Verificar y Actuar, o PDCA en inglés (Plan, Do, Check, Act).

Figura 2: Modelo del SGSI de la norma ISO 27001.

El resumen de la descripción de las etapas del modelo del SGSI de la norma ISO 27001 (Ciclo de Deming: ejemplos, etapas, importancia, ventajas y desventajas, s. f.), es el siguiente:

1. Planificar: En esta etapa se realiza la planificación, diseño y establecimiento del SGSI, estructurando las políticas de seguridad que se aplicarán en la institución, se incluyen los objetivos a cumplir y su relación con los objetivos institucionales, los recursos requeridos, así como los procesos con sus activos (de información y de soporte).
2. Hacer: En esta etapa se despliega y opera el SGSI. Las políticas y los controles identificados para el cumplimiento son implementados por recursos técnicos, procedimientos o ambos, y funcionarios responsables son asignados a cada tarea.
3. Verificar: En esta etapa los resultados obtenidos se evalúan en base a indicadores para cada objetivo. Este análisis comprueba la eficacia y eficiencia de las acciones realizadas, así como, el cumplimiento de las políticas y procedimientos, y la identificación de fallos potenciales y su fuente, deben verificarse mediante evaluaciones y auditorías.
4. Actuar: Esta es la etapa en la que se realiza mantenimiento y mejoras al SGSI, se identifican e implementan las acciones preventivas y correctivas necesarias para corregir las deficiencias encontradas durante las evaluaciones y revisiones al SGSI, u otros aspectos relevantes que contribuyan con la mejora continua del SGSI.

CAPÍTULO 3: METODOLOGÍA

En este capítulo, se explica la metodología aplicada para la recolectar información y desarrollar del SGSI. La metodología incluye el proceso de investigación que se realizó, la población y la muestra escogida, el procesamiento y análisis de los datos y el plan de desarrollo para el SGSI.

3.1. METODOLOGÍA DE INVESTIGACIÓN

Para la investigación y el proceso de recolección de datos se optó por una metodología de campo y documental. De campo debido a que la investigación y recolección de información se realizará en el lugar del problema, es decir, en la DGSCyOP.

Documental debido a que la información teórica complementaria se recolecta de fuentes externas como libros, artículos, páginas web y bibliotecas. Finalmente, toda la información recolectada se utilizará para diseñar y documentar el SGSI.

3.2. POBLACIÓN Y MUESTRA

3.2.1. POBLACIÓN

La población que se tomó para el desarrollo del proyecto fue el personal responsable de los departamentos que conforman la DGSCyOP, que son: Planificación, Jurídico, Comunicación Organizacional, Análisis de la Información, Coordinación Operacional, Apoyo Operativo, Centro de Especialización Policial y Soporte Operativo. En total hay ocho funcionarios responsables de estos departamentos, quienes son los propietarios de la información que se registra, procesa y almacena en los mismos.

3.2.2. MUESTRA

La población que se requiere analizar de la DGSCyOP no es amplia, no es necesario calcular una muestra para la aplicación de entrevistas y levantamiento de información, por lo que la muestra es la misma población establecida en el punto anterior (8 funcionarios).

3.3. RECOLECCIÓN DE INFORMACIÓN

Para la parte teórica del proyecto se recolectó información de fuentes bibliográficas como: revistas, artículos e informes técnicos, libros, documentos oficiales de instituciones públicas, normas técnicas, páginas web, entre otras. Esta información debe ser acorde a los temas tratados en el proyecto para poder sustentar el marco teórico.

Para la investigación de campo y recolección de la información y documentación requerida de la DGSCyOP, se realizaron visitas a las oficinas de la Dirección para inspeccionar y evaluar los departamentos de Planificación, Jurídico, Comunicación Organizacional, Análisis de la Información, Coordinación Operacional, Apoyo Operativo, Centro de Especialización Policial y Soporte Operativo, en los cuales se registra y procesa información. Adicionalmente, a través de las visitas de campo a los departamentos de la Dirección, se recopilaron datos de los activos de información, infraestructura de red y la arquitectura de los sistemas informáticos implementados con su respectiva documentación.

Para complementar la recolección de información, se realizaron entrevistas al personal responsable de cada departamento de la Dirección mediante cuestionarios enfocados en seguridad de la información, con la finalidad de obtener información adecuada y relevante de las principales actividades y procesos que se realizan en la Dirección. Esta información representa un insumo importante para la elaboración y documentación del SGSI. El cuestionario aplicado se encuentra detallado en el Anexo I.

3.4. EVALUACIÓN Y ANÁLISIS DE DATOS

Para procesar, evaluar y analizar los datos obtenidos se realizó:

- Revisión de la información y documentos recopilados.
- Organización y clasificación de la información.
- Interpretación y análisis de los resultados.
- Desarrollo de la solución.

3.5. PLAN DE DESARROLLO

El desarrollo e implementación del SGSI se llevará a cabo aplicando las etapas y actividades que se describen en la siguiente tabla:

Etapa		Actividades	
I	Análisis de la situación actual basado en el tratamiento y seguridad de la información:		
		1.	Levantamiento de la estructura orgánica
		2.	Establecimiento de la misión y responsabilidades
		3.	Aplicación de entrevistas
		4.	Análisis de entrevistas y conclusiones
II	Desarrollar el SGSI alineado al estándar ISO 27001, siguiendo la estructura PHVA de la norma ISO 27001:		
	Planificar	1.	Definir el alcance
		2.	Establecer la organización del SGSI
		3.	Definir la política general de seguridad de la información
		4.	Establecer la metodología para la evaluación de riesgos
		5.	Realizar el levantamiento del inventario de activos
		6.	Identificar vulnerabilidades y amenazas
		7.	Valoración de activos
	Hacer	1.	Gestión de riesgos
		2.	Selección de controles a implementar
		3.	Declaración de aplicabilidad
		4.	Documentación de controles
		5.	Implementación de controles
		6.	Formar y concientizar
	Verificar	1.	Revisar el SGSI y eficacia de los controles
		2.	Realizar auditorías internas del SGSI
	Actuar	1.	Implementar mejoras al SGSI

Tabla 1. Etapas y actividades para el desarrollo e implementación del SGSI.

CAPÍTULO 4: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

En este capítulo, se realiza un diagnóstico de la situación actual de la DGSCyOP, en cuanto a su estructura organizacional, responsabilidades, activos e información procesada en los departamentos que la conforman. El diagnóstico se realizó mediante visitas a las oficinas de la Dirección y aplicación de entrevistas a los responsables de los departamentos.

4.1. ESTRUCTURA ORGÁNICA DE LA DGSCyOP

La DGSCyOP está liderada por el Director General de Seguridad Ciudadana y Orden Público, quien reporta y está bajo la supervisión del Subcomando General de Policía. Se encuentra conformada por los siguientes departamentos:

- Planificación
- Jurídico
- Comunicación Organizacional
- Análisis de la Información
- Coordinación Operacional
- Apoyo Operativo
- Centro de Especialización Policial
- Soporte Operativo

Adicionalmente, bajo la DGSCyOP se encuentran las siguientes direcciones:

- Dirección Nacional de Operaciones Especiales y Servicios Especializados
- Dirección Nacional de Coordinación Interinstitucional
- Dirección Nacional Preventiva y Comunitaria
- Dirección Nacional de Control de Fronteras
- Dirección Nacional de Control de Tránsito y Seguridad Vial

La siguiente figura describe la estructura orgánica de la DGSCyOP:

INSTRUMENTOS TÉCNICOS DE ORGANIZACIÓN DE TALENTO HUMANO		
Estructuras Posicionales	Registro Oficial No.911-2019 (A. M. 0080)	Versión: 1
Fecha de Elaboración: 09/01/2020		Pág. 30 de 114
DIRECCIÓN GENERAL DE SEG. CIUD. Y ORDEN PÚBLICO		Lámina No. 030

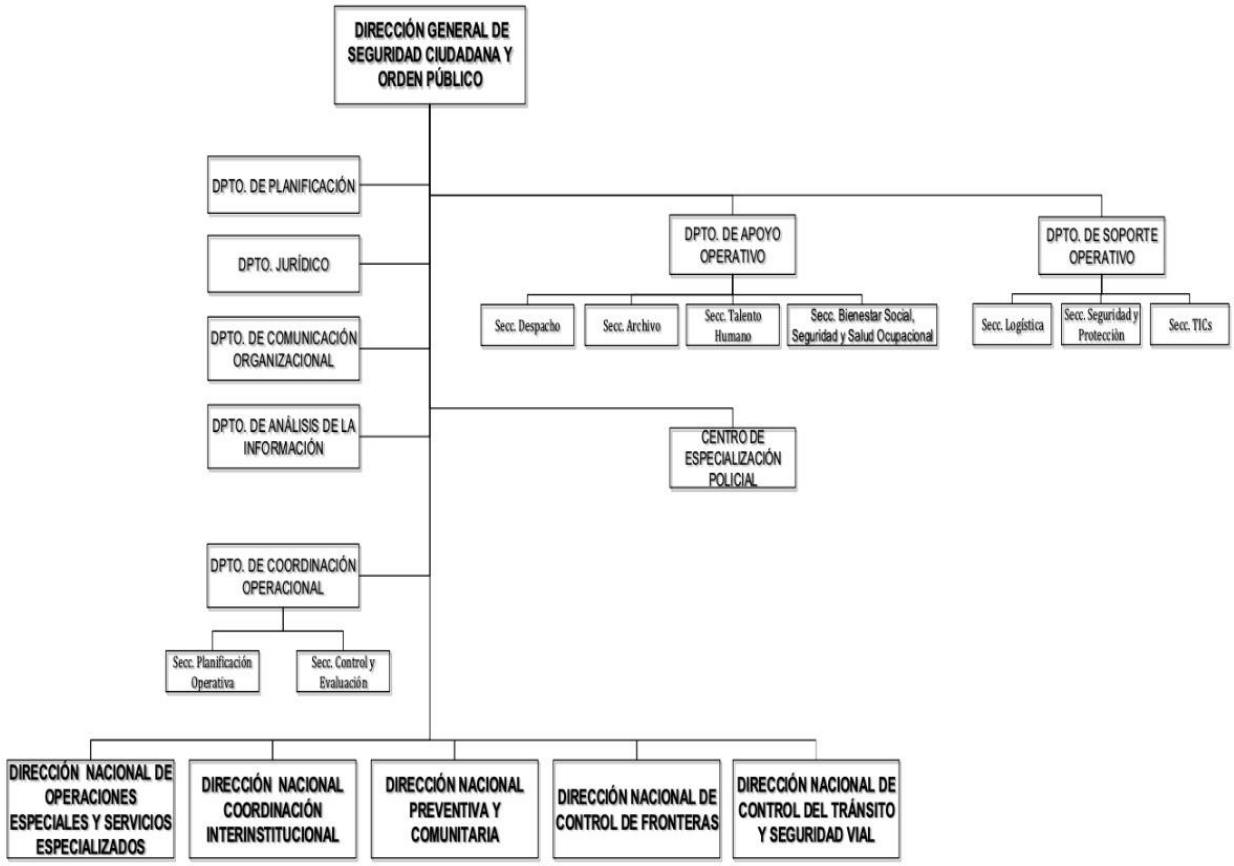

Figura 3. Estructura orgánica de la DGSCyOP.

Fuente: Departamento de Apoyo Operativo, Sección Talento Humano.

4.2. MISIÓN Y RESPONSABILIDADES

De acuerdo con el Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional del Ecuador la misión de la DGSCyOP es: "Dirigir las operaciones policiales del subsistema preventivo y coordinar con los subsistemas investigativo e inteligencia, para atender la seguridad ciudadana y el orden público".

Como se indicó en el punto anterior, el responsable es el Director General de Seguridad Ciudadana y Orden Público, quién tiene las siguientes responsabilidades:

- Ejecutar el mando y administración de recursos a su cargo en el ámbito de sus competencias.
- Coordinar las operaciones del subsistema preventivo, con el investigativo e inteligencia en el ámbito de su competencia.
- Emitir directrices operativas en base al estudio del delito a nivel nacional.
- Dirigir la planificación, coordinación y supervisión de las actividades administrativas, técnicas y operativas de las dependencias policiales bajo su mando.
- Asesorar al mando policial sobre las políticas públicas en materia de seguridad ciudadana y orden público, conforme a la misión institucional.
- Evaluar las operaciones policiales que ejecuten las direcciones nacionales y demás niveles desconcentrados de esta Dirección.
- Supervisar las operaciones policiales del subsistema preventivo con entidades públicas y privadas, nacionales e internacionales, en el ámbito de su competencia.
- Presentar el informe de gestión al Comando General conforme con la normativa legal establecida.
- Cumplir con las demás atribuciones y responsabilidades que señalen las leyes y reglamentos.

4.3. APLICACIÓN DE ENTREVISTAS

Para establecer la situación actual de la gestión de seguridad de la información en la DGSCyOP, así como levantar información relacionada con: procesos, activos, controles, infraestructura tecnológica y sistemas informáticos, se aplicó una entrevista a los jefes de los ocho departamentos que conforman la Dirección.

Las entrevistas se realizaron a través de un cuestionario con preguntas enfocadas en gestión de seguridad de la información, tomando como base las guías de la norma ISO 27001. El cuestionario compuesto de 15 preguntas se describe en el Anexo I.

El cuestionario de entrevistas se aplicó a los siguientes funcionarios de la Dirección (por solicitud de la Dirección, no se describe los nombres y apellidos de los funcionarios, solo su grado, iniciales y cargo):

No.	Grado e Iniciales	Cargo	Departamento
1.	TCNL. S. Z.	Jefe de Planificación	Planificación
2.	SBTE. D. O.	Jefe Jurídico	Jurídico
3.	MAYR. J. Z.	Jefe de Comunicación Organizacional	Comunicación Organizacional
4.	CPTN. A. M.	Jefe de Análisis de la Información	Análisis de la Información
5.	TCNL. D. V.	Jefe de Coordinación Operacional	Coordinación Operacional
6.	TCNL. E. M.	Jefe de Apoyo Operativo	Apoyo Operativo
7.	MAYR. M. V.	Jefe del Centro de Especialización Policial	Centro de Especialización Policial
8.	MAYR. R. R.	Jefe de Soporte Operativo (*)	Soporte Operativo

Tabla 2. Listado de personal entrevistado.

(*): El Jefe de Soporte Operativo delegó la entrevista al SGTO F. G., Analista de Datos, por estar a cargo de la Sección TIC's de la Dirección.

Las entrevistas cubrieron los siguientes aspectos:

- Políticas y controles relacionadas con gestión de seguridad de la información
- Responsabilidades en la gestión de seguridad de la información
- Identificación y registro de incidentes de seguridad de la información
- Gestión de riesgos
- Procesos y activos de información
- Capacitación en seguridad de la información

El resumen de los resultados obtenidos de las entrevistas aplicadas se describe en la siguiente tabla, en la que se presenta el porcentaje del total de entrevistados que respondió a cada pregunta, así como las respectivas justificaciones y respuestas.

Significado abreviaciones:

S: Si

N: No

D: Desconoce

P: Parcialmente

No.	PREGUNTA	Porcentajes (%)					JUSTIFICACIONES RESPUESTAS
		S	N	D	P	TOTAL	
1	¿Entiende la definición de seguridad de la información?	50.0	0.0	37.5	12.5	100.00	● Medidas necesarias para que la información se mantenga segura y sea confiable. ● Proteger la información de personas no autorizadas. ● Medidas para proteger la información para mantenerla íntegra. ● Controles lógicos y físicos que se aplican a la información. ● Asegurar la integridad y confidencialidad de la información.
2	¿En el departamento a su cargo o en la Dirección se han documentado formalmente y se aplican políticas para la a seguridad de la información?	25.0	75.0	0.0	0.0	100.00	● No existe una definición formal de políticas de seguridad de la información. ● Si, tenemos ciertas políticas en cuanto al control de la información: o Acceso a recursos informáticos con usuario y contraseña. o Restricción de acceso a equipos por personal no autorizado. o Restricción de instalación o modificación del software en equipos.
3	¿En la Dirección existe un responsable a cargo de la gestión de seguridad de la información?	0.0	100.0	0.0	0.0	100.00	
4	¿El personal a su cargo tiene definidas responsabilidades en cuanto al uso de recursos informáticos en la Dirección?	37.5	37.5	0.0	25.0	100.00	● Al entregarles las computadoras y recursos tecnológicos para el desarrollo de su trabajo asumen la responsabilidad de su custodia y cuidado. ● Todo el personal del departamento es responsable de los equipos que se les asigna. ● No se han establecido de manera formal estas responsabilidades. Se han establecido responsabilidades al personal, pero no existe un procedimiento formal. ● A cada funcionario se le da a conocer sus responsabilidades, pero no existe documentación que certifique esas responsabilidades.
5	¿Existe un procedimiento que el personal de la Dirección o de su departamento aplique para la identificación y reporte de incidentes de seguridad de la información?	0.0	87.5	12.5	0.0	100.00	
6	¿Se realizan simulacros de fallos o amenazas en los sistemas informáticos implementados en la Dirección o en su departamento?	0.0	50.0	50.0	0.0	100.00	
7	¿Existe algún control para el acceso de personal no autorizado a equipos, sistemas informáticos y áreas restringidas de la Dirección?	50.0	37.5	0.0	12.5	100.00	● Solo el personal autorizado de la Dirección. ● Al ingreso al edificio de la Comandancia el personal externo debe anunciarse para ingresar a la Dirección o a uno de sus departamentos. ● Solo personal que trabaja en la Comandancia o es miembro de la Policía Nacional. ● Si, solo el personal perteneciente al área o dirección en la que trabaja tiene acceso a los equipos de la misma.

No.	PREGUNTA	Porcentajes (%)					JUSTIFICACIONES RESPUESTAS
		S	N	D	P	TOTAL	
8	¿Conoce si se realizan mantenimientos periódicos a los equipos informáticos de la Dirección o de su departamento?	25.0	12.5	50.0	12.5	100.00	● No se han realizado en el departamento a mi cargo. ● Si, se realizan mantenimientos con periodicidad semestral.
9	¿Conoce si la Dirección tiene un plan de gestión de riesgos tecnológicos, de seguridad de la información o de otro tipo de riesgos?	12.5	25.0	50.0	12.5	100.00	● Se tienen planes de riesgos, pero relacionados con la gestión de la Policía Nacional, pero no para tecnología. ● Riesgos relacionados con las acciones operativas que coordina la Dirección. ● Esta Dirección no cuenta con plan para afrontar los riesgos y amenazas informáticas que se presenten.
10	¿Conoce los mecanismos y procedimientos de seguridad y control de acceso lógico que se aplican a los sistemas informáticos implementados en la Dirección o en su departamento?	25.0	50.0	12.5	12.5	100.00	● Contraseñas y cuentas de usuarios. ● Usuarios y claves. ● Asignación de una cuenta de usuario por parte del área de TICs. ● Clave y cuenta de usuario para acceso al sistema SIIPNE.
11	¿Conoce si la Dirección cuenta con un inventario de los activos de información?	12.5	0.0	62.5	25.0	100.00	● Se mantiene un inventario de hardware y software, y de archivos físicos, pero no es un inventario completo de activos de información.
12	¿Conoce de amenazas relacionadas con seguridad de la información a las que la Dirección o su departamento están expuestos?	75.0	12.5	12.5	0.0	100.00	● Ciberataques, robo de información, virus. ● Fuga de información, ataques cibernéticos, acceso no autorizado a información confidencial. ● No se cuenta con un responsable de seguridad de la información, virus informáticos. ● Acceso a la información por personal no autorizado (interno y externo).
13	¿En el último año ha recibido capacitación en temas de seguridad de la información?	0.0	100.0	0.0	0.0	100.00	
14	¿En el desarrollo de su gestión, qué servicios de TIC requiere? (Por ejemplo: correo electrónico, internet, sistemas informáticos, respaldos de información, mantenimiento y soporte técnico, red de datos, impresiones, etc.)						● Correo electrónico, computadoras, internet, sistemas. ● Red de datos, respaldos, soporte técnico.

No.	PREGUNTA	Porcentajes (%)					JUSTIFICACIONES RESPUESTAS
		S	N	D	P	TOTAL	
15	¿Qué procesos, activos tecnológicos y de información tiene a su cargo para el desempeño de sus funciones?						Procesos: planificación estratégica de la Dirección, planificación operativa, evaluación y análisis de resultados. Activos: computadores de los funcionarios del departamento, sistema Quipux, Sistema Integrado de la Policía Nacional (SIIPNE), equipo servidor asignado a la Dirección, información registrada en el correo electrónico institucional, Estatuto Policía Nacional, manuales e instructivos de la Dirección, documentación que se generan en el departamento: partes, memos, informes, planes, expedientes de casos, acuerdos ministeriales. Procesos: gestión de comunicación organizacional. Activos: información procesada en el departamento, equipos computacionales, sistema SIIPNE. Procesos: coordinación operativa, estadística operativa. Activos: computadoras, impresoras, sistema SIIPNE, sistema Quipux, información digital y física del departamento, archivo central de la Dirección. Procesos: coordinación operativa, soporte y apoyo operativo. Activos: computadores, SIIPNE, Quipux, información procesada en el departamento, archivo central de la Dirección. Procesos: coordinación de especializaciones para el personal policial. Activos: computadores, información del departamento. Procesos: soporte y mantenimiento de TIC, logística, seguridad y protección Activos: computadores, sistemas informáticos, información generada en el departamento, servidores de: archivos, respaldos, correo electrónico, equipos de comunicación, impresoras, equipos de seguridad.

Tabla 3. Resumen de resultados de entrevistas aplicadas.

4.4. ANÁLISIS DE LAS ENTREVISTAS Y CONCLUSIONES

Del análisis a las entrevistas realizadas se pueden establecer las siguientes conclusiones:

- El personal de la Dirección no tiene claro o desconoce la definición o concepto de seguridad de la información.
- En la Dirección no existen formalmente definidas políticas de seguridad de la información.
- En la Dirección no se tiene designado un funcionario responsable para gestionar la seguridad de la información.
- El personal de la Dirección no tiene asignadas de manera formal responsabilidades sobre el uso de los recursos informáticos a su cargo.
- No existe un procedimiento formal en la Dirección para que el personal realice la identificación y reportes de incidentes de seguridad de la información.

- No se realizan simulacros de fallas o amenazas en los sistemas informáticos implementados en la Dirección.
- Solo el personal que labora en la Dirección tiene la autorización para acceder a los equipos y sistemas informáticos implementados en la misma, y el único control que se mantiene para el acceso de personal externo es el registro y anuncio en el ingreso al edificio de la Comandancia.
- No se realizan mantenimientos periódicos de los equipos informáticos de la Dirección.
- En la Dirección no existe un plan de gestión de riesgos tecnológicos y tampoco de seguridad de la información.
- El principal control de acceso lógico a los sistemas informáticos de la Dirección es la asignación de una cuenta de usuario con clave.
- En la Dirección no se ha levantado ni documentado formalmente un inventario de activos informáticos.
- Las principales amenazas en relación con seguridad de la información que los jefes departamentales han identificado que podrían afectar a la Dirección son: ciberataques, robo y fuga de información, acceso sin autorización a la información, virus informáticos.
- El personal de la Dirección no ha recibido capacitación relacionada con seguridad de la información.
- Los principales servicios de TI que utiliza el personal de la Dirección son: correo electrónico, internet, sistemas informáticos, red de datos, respaldos de información y soporte técnico.
- Los principales procesos de la Dirección son: planificación estratégica, planificación operativa, evaluación y análisis de resultados, gestión de comunicación organizacional, coordinación operativa, estadística operativa, soporte y apoyo operativo, coordinación de especializaciones para el personal policial, soporte y mantenimiento de TIC, logística, seguridad y protección.
- Los principales activos tecnológicos y de información de la Dirección son: computadores (de escritorio y portátiles), sistema Quipux, Sistema Integrado de la Policía Nacional (SIIPNE), equipo servidor asignado a la Dirección, información registrada en el correo electrónico institucional, Estatuto Policía Nacional, manuales e instructivos de la Dirección, documentación que se generan en los departamentos: partes, memos, informes, planes, expedientes de casos, acuerdos ministeriales,

impresoras, documentación del archivo central de la Dirección, respaldos de información, equipos de seguridad.

Como conclusión final se puede indicar que en la DGSCyOP no existe una adecuada gestión de seguridad de la información, debido a que no se ha definido formalmente políticas para esta gestión, y no se han asignado responsabilidades a los funcionarios que manejan información en la Dirección. Esto conlleva a que no se pueda garantizar la disponibilidad, integridad y confidencialidad de la información, registrada, procesada y almacenada en la Dirección.

CAPÍTULO 5: DESARROLLO DEL SGSI

Con base en las conclusiones obtenidas sobre la situación actual en la Dirección, se desarrollará la propuesta de diseño del SGSI para hacer frente a las necesidades encontradas y cubrir las principales vulnerabilidades relacionadas con seguridad de la información. De acuerdo con el plan de desarrollo (definido en el Capítulo 2: Metodología), el SGSI se diseñará siguiendo la estructura PHVA del modelo de gestión de la norma ISO 27001 y sus respectivas actividades.

5.1. DEFINICIÓN DEL ALCANCE DEL SGSI

Como primer paso, se deben definir los límites para la implementación del SGSI en la DGSCyOP, con el objetivo de decidir qué activos tecnológicos y de información se quiere proteger. El alcance del SGSI permitirá establecer y garantizar la seguridad para los activos de información y tecnológicos que permiten el desempeño normal y exitoso de las funciones, servicios y actividades de la Dirección.

El alcance del SGSI establecido para la Dirección es el siguiente:

- Procesos: planificación estratégica, planificación operativa, evaluación y análisis de resultados, gestión de comunicación organizacional, coordinación operativa, estadística operativa, soporte y apoyo operativo, coordinación de especializaciones para el personal policial, soporte y mantenimiento de TIC, logística, seguridad y protección.
- Departamentos: Planificación, Jurídico, Comunicación Organizacional, Análisis de la Información, Coordinación Operacional, Apoyo Operativo, Centro de Especialización Policial y Soporte Operativo.
- Personal: aplica para todos los funcionarios de la Dirección, así como para el personal de apoyo y terceros no relacionados directamente a la Dirección, que tengan acceso a los activos de información y tecnológicos.
- Activos: incluye todos los activos de información y tecnológicos de la Dirección.
- Ubicaciones físicas: La DGSCyOP, se encuentra ubicada en el piso siete del edificio de la Comandancia General de la Policía Nacional del Ecuador, ubicado en la Av. Amazonas N. 53 – 113 y Japón.

5.2. ORGANIZACIÓN DEL SGSI

5.2.1. COMPROMISO DEL NIVEL DIRECTIVO

Como parte de los requisitos para la implementar un SGSI, de acuerdo a al estándar ISO 27001: 2013, debe existir el liderazgo y compromiso del nivel directivo, por lo que el Director de la DGSCyOP debe promover el establecimiento de un SGSI y cumplir con las Políticas de Seguridad de la Información aplicables y reafirmar su compromiso mediante:

- El cumplimiento de la normativa vigente interna y externa aplicable a la Dirección en materia de seguridad de la Información.
- Promover activamente una cultura de seguridad de la información dentro de la Dirección.
- Garantizar los recursos requeridos para implementar y realizar mantenimiento del SGSI en la Dirección.
- Mejorar continuamente el SGSI mediante buenas prácticas con el objetivo de cuidar la integridad, disponibilidad y confidencialidad de la información.

5.2.2. ORGANIZACIÓN

Para la gestión de la seguridad de la información en la Dirección se propone el establecimiento de la siguiente organización y estructura:

- Crear una Unidad de Seguridad de la Información, conformada por:
    - Un responsable de la seguridad u Oficial de Seguridad de la Información
    - Un Asistente de Seguridad de la Información

El responsable u Oficial de Seguridad de la Información deberá reportar y está bajo la supervisión del Director de la DGSCyOP y de un Comité de Seguridad de la Información.

5.3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de la política que se propone a continuación, es normar la gestión de seguridad de la información en la Dirección para proporcionar orientación y apoyar a esta gestión, de acuerdo con los requisitos y objetivos institucionales y las guías de la norma ISO 27001.

Los funcionarios, empleados externos, proveedores y todos los demás responsables de los activos informáticos y tecnológicos y recursos para procesar la información, deberán aplicar las pautas que se encuentran dentro de la política propuesta, con el objetivo de mantener la integridad, disponibilidad y confidencialidad de la información.

Política General de Seguridad de la Información:

- Es política de la Dirección con el apoyo del Comité de Seguridad de la Información generar normas para la Gestión de la Seguridad de la Información para:
    - Implementar un marco de gobierno (políticas, procedimientos, estructura) para empezar y monitorear la implementación de la gestión de seguridad de la información, así como definir roles y responsabilidades.
    - Organizar la gestión de activos informáticos para que tengan un nivel de protección adecuado.
    - Garantizar en una medida razonable, que todos los medios para procesar y/o conservar información cuenten con un resguardo físico y lógico, para evitar el acceso y/o uso indebido por parte de persona no autorizadas, así como permitir su operación continua.
    - Garantizar que los datos y las transacciones cumplan con su autorización correspondiente para poder ser utilizados y divulgados.
    - Asegurar una identificación y registro integral para todos los usuarios de los sistemas y aplicaciones informáticas que forman parte de la Dirección.
    - Definir una metodología para el análisis y evaluación de riesgos de seguridad de la información.

- Realizar revisiones y monitoreos periódicamente al SGSI con el objetivo de mantenerlo en una mejora continua.

5.4. METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para el establecimiento de la metodología para la evaluación de riesgos de Seguridad de la Información en la Dirección, se aplicarán las etapas establecidas en la metodología MAGERIT (definida en el punto 2.3 del Capítulo 2: Fundamentos Teóricos), que se describen a continuación:

- **Identificación:**

  Para la identificación se considerará que un riesgo es todo evento que ya se produjo o que se puede producir en la Dirección, relacionado con eventos de seguridad de la información o sobre un activo, que puede afectar a la continuidad operativa y tener alto impacto económico para la Dirección. Los responsables de la identificación de riesgos de seguridad de la información son todos los funcionarios de la Dirección.

  La identificación y reporte de los riesgos de seguridad de la información se realizará a través del correo electrónico institucional, por vía telefónica o por notificación directa al responsable de seguridad u Oficial de Seguridad de la Información. Los datos que se deben reportar son los siguientes:

  - Nombre y cargo de quién reporta el evento
  - Departamento / Sección
  - Detalle del evento de riesgo de seguridad de la información.
  - Periodicidad de ocurrencia del evento de riesgo (diaria, mensual, trimestral, semestral, anual).
  - Causa (si es factible determinarla)
  - Fecha de ocurrencia del evento de riesgo de seguridad de la información.

- **Análisis y Evaluación**

  El análisis de riesgos permitirá calificar (valorar) los riesgos de seguridad de la información identificados y establecer una prioridad para su evaluación y tratamiento. De acuerdo con la calificación de los riesgos se realizará la evaluación de los mismos, para decidir los riesgos que se aceptarán y cuáles no. Además, en qué situaciones se debe aceptar un riesgo o ejecutar un tratamiento para minimizarlo.

  Los riesgos serán analizados y valorados considerando la probabilidad de ocurrencia de una amenaza sobre el activo y el impacto que puede causar la pérdida de integridad, disponibilidad y confidencialidad del activo.

  La tabla de niveles de probabilidad definida para valorar los riesgos de seguridad de la información es la siguiente:

NIVEL	VALOR	DESCRIPCIÓN
Certeza	5	Ocurrencia en la mayoría de situaciones
Probable	4	Posible ocurrencia en la mayoría de situaciones
Moderado	3	Es posible que ocurra en algún momento
Improbable	2	Pudo ocurrir en alguna ocasión.
Muy Improbable	1	Puede ocurrir solo en situaciones extremas.

Tabla 4. Niveles de probabilidad de riesgos de seguridad de la información.

  La tabla de niveles de impacto definida para evaluar y valorar los riesgos de seguridad de la información es la siguiente:

NIVEL	VALOR	DESCRIPCIÓN
Catastrófico	5	El riesgo afecta totalmente a la confidencialidad, integridad y disponibilidad del activo.
Mayor	4	El riesgo afecta de forma importante a la confidencialidad, integridad y disponibilidad del activo.
Moderado	3	El riesgo afecta de forma moderada al activo.
Menor	2	El riesgo afecta en menor grado al activo.
Insignificante	1	No existe afectación al activo

Tabla 5. Niveles de impacto de riesgos de seguridad de la información.

Como se puede observar en las tablas anteriores, los niveles de impacto y probabilidad serán valorados utilizando una escala de Likert[2] de 1 al 5, siendo 1 el valor más bajo, y 5 el valor más alto. Para el cálculo del Nivel de Riesgo se aplica la siguiente fórmula:

Nivel de Riesgo = Probabilidad x Impacto

Con la combinación de estos valores se establecerá una matriz de riesgos de 5 x 5, en la que se definirán los siguientes niveles de valoración:

- No Aceptable (NA)
- Mayor (MY)
- Medio (MD)
- Menor (MR)

El resultado de la combinación de impacto por probabilidad y los niveles de valoración (zonas de riesgos), se describen en la siguiente tabla:

PROBABILIDAD		**IMPACTO**				
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
		1	**2**	**3**	**4**	**5**
Certeza	**5**	MD (5)	MY (10)	NA (15)	NA (20)	NA (25)
Probable	**4**	MD (4)	MY (8)	MY (12)	NA (16)	NA (20)
Moderado	**3**	MR (3)	MD (6)	MY (9)	MY (12)	NA (15)
Improbable	**2**	MR (2)	MD (4)	MD (6)	MY (8)	MY (10)
Muy Improbable	**1**	MR (1)	MR (2)	MR (3)	MD (4)	MD (5)

Tabla 6. Matriz de zonas de riesgos de seguridad de la información.

[2] La escala de Likert (que recibe el nombre del creador de la misma, el científico social estadounidense Rensis Likert), es una herramienta de medición que utiliza una escala de 3, 5 o 7 puntos, también se la conoce como escala de satisfacción, la cual incorpora un rango de opiniones que va de un extremo a otro.

.

Los niveles de valoración de riesgos de seguridad de la información y los rangos de valores que se aplicarán en la Dirección se describen a continuación en la tabla:

Niveles de Valoración de Riesgo	Rango
No Aceptable (NA)	15.00 – 25.00
Mayor (MY)	8.00 – 14.99
Media (MD)	3.01 – 7.99
Menor (MR)	0.00 – 3.00

Tabla 7. Niveles de valoración de riesgos y rangos.

Para evaluar los riesgos se propone que el límite de exposición a riesgos que la Dirección debe asumir es Medio, es decir, todos los riesgos con calificación igual o menor a 3.01 serán aceptados, y los que superen este valor deben ser tratados para minimizarlos.

- **Tratamiento**

  Una vez realizada la evaluación de los riesgos, se deberá tomar las siguientes acciones de tratamiento frente a los riesgos para poder mitigarlos (MAGERIT vs3. Libro I, 2012):

  - Asumir: Se debe solucionar el riesgo y su impacto económico con la utilización de recursos propios.
  - Mitigar: Implementación de controles y acciones para minimizar la probabilidad de ocurrencia de un riesgo.
  - Evitar: Decisión de no realizar la actividad que nos expone a un riesgo.
  - Transferir: Trasladar el riesgo a otras entidades, normalmente a través de un seguro.

  Los planes de acción para los tratamientos de los riesgos incluirán la siguiente información:

- El detalle del objetivo del plan de acción
- Los recursos necesarios para ejecutar el plan
- Responsables
- Detalle de las actividades que conforman el plan. Se debe incluir: descripción de la actividad, fecha en la que se empieza y finaliza la actividad, responsable de la actividad y el porcentaje de cumplimiento de la actividad.

Matriz de Riesgos de Seguridad de la Información

Finalmente, para completar la metodología planteada, la matriz de registro de riesgos de seguridad de la información de la Dirección estará compuesta por los siguientes campos:

- Descripción del activo o evento de seguridad de la información
- Amenazas
- Riesgo
- Nivel de Probabilidad
- Nivel de Impacto
- Nivel de Riesgo
- Nivel de Valoración
- Tratamiento

5.5. LEVANTAMIENTO DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN

Uno de los aspectos clave en el desarrollo del SGSI es la identificación y levantamiento de los activos de información y tecnológicos de la DGSCyOP. Los activos tienen un valor muy importante debido a que contienen o procesan información, por este motivo se les debe dar una gestión adecuada.

De acuerdo con la Norma Técnica Colombiana NTC-ISO 27005 – Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la Seguridad de la Información (Anexo B – Identificación y Valoración de los Activos y Valoración del Impacto), se tiene los siguientes tipos de activos:

- Activos primarios:
  - Información
  - Actividades y procesos del negocio
- Activos de soporte:
  - Hardware
  - Software
  - Redes
  - Personal
  - Ubicaciones físicas

Esta clasificación se asumió para realizar el inventario de activos de la Dirección, el mismo que incluye los siguientes campos:

- Código
- Nombre del activo
- Descripción del activo
- Tipo de activo
- Ubicación (área física en la Dirección)
- Responsable (propietario del activo)

El levantamiento de los activos se realizó a través de las entrevistas realizadas a los jefes departamentales de la Dirección, y mediante observación directa en sus instalaciones. La siguiente tabla detalla los activos de información levantados:

Cód.	Nombre Activo	Descripción	Tipo	Ubicación	Propietarios
A01	Plan estratégico institucional	Contiene las estrategias y objetivos de la Dirección para un período de tiempo.	Información	Departamento de Planificación	Jefe de Planificación
A02	Planes operativos	Contiene la información de los diferentes planes operativos policiales que se coordinan en la Dirección.	Información	Departamento de Coordinación Operativa	Jefe de Coordinación Operativa

Cód.	Nombre Activo	Descripción	Tipo	Ubicación	Propietarios
A03	Informes de evaluaciones	Contiene información del análisis y evaluación que se realiza de los diferentes operativos coordinados en la Dirección.	Información	Departamento de Análisis de Información	Jefe de Evaluación y Análisis de Resultados
A04	Comunicaciones	Contiene memos, partes, acuerdos ministeriales y comunicaciones generados en la Dirección o que llegan a la Dirección.	Información	Departamento de Gestión de Comunicación Organizacional	Jefe de Gestión de Comunicación Organizacional
A05	Expedientes personales	Contiene la información personal, laboral, seguridad y de salud ocupacional de los funcionarios que trabajan en la Dirección.	Información	Departamento de Apoyo Operativo, Sección Talento Humano	Jefe de Apoyo Operativo
A06	Informes Jurídicos	Contiene la información de los trámites y expedientes jurídicos generados en la Dirección.	Información	Departamento Jurídico	Jefe Jurídico
A07	Cursos y especializaciones	Contiene la información de los cursos, talleres y especializaciones realizados por el personal policial.	Información	Centro de Especialización Policial	Jefe del Centro de Especialización Policial
A08	Manuales de estatutos, políticas, procedimientos, reglamentos	Contiene la información de estatutos, normas, políticas, reglamentos y procedimientos de la Dirección	Información	Departamento de Apoyo Operativo	Jefe de Soporte Operativo
A09	Inventario de hardware y software	Contiene el inventario del hardware y software a cargo de la Dirección.	Información	Departamento de Soporte Operativo, sección TICs	Jefe de Soporte Operativo
A10	Informes soporte técnico	Contiene la información de los soportes técnicos y mantenimientos que realiza a través del personal de la sección TICs.	Información	Departamento de Soporte Operativo, sección TICs	Jefe de Soporte Operativo
A11	Respaldos información	Contiene los respaldos de información de las computadoras y servidor de archivos de la Dirección que se realizan en disco duro externo.	Información	Departamento de Soporte Operativo, sección TICs.	Jefe de Soporte Operativo
A12	Listado de cuentas y claves de usuarios administradores	Contiene la información de cuentas y claves de los usuarios requeridos para administrar el servidor de archivos, router y sistemas informáticos implementados en la Dirección.	Información	Departamento de Soporte Operativo, sección TICs	Jefe de Soporte Operativo

Cód.	Nombre Activo	Descripción	Tipo	Ubicación	Propietarios
A13	Información correo electrónico	Contiene correos electrónicos y archivos adjuntos del servicio de correo electrónico institucional.	Información	Computadoras asignadas al personal ubicadas en las instalaciones de la Dirección.	Funcionarios de la Dirección que tienen cuenta de correo electrónico institucional
A14	Computadores de escritorio y portátiles	Equipos que contienen la información que registran y procesan los funcionarios autorizados de la Dirección	Hardware	Instalaciones de la Dirección.	Funcionarios de la Dirección que tienen asignados computadores
A15	Servidor de archivos	Contiene información de toda la Dirección que se procesa y comparte a través de la red de datos.	Hardware	Área de equipos servidores y comunicaciones ubicada en la sección TICs.	Jefe de Soporte Operativo
A16	SIIPNE	Sistema Integrado de la Policía Nacional	Software	Plataforma de la Policía	
A17	Sistema Quipux	Sistema informático de gestión documental utilizado a nivel de la Policía Nacional y de las entidades gubernamentales.	Software	Plataforma del MINTEL.	Jefe de Soporte Operativo
A18	Discos duros externos	Contiene información de respaldo de los computadores y servidor de archivos de la Dirección.	Hardware	Área de equipos servidores y comunicaciones ubicada en la sección TICs	Jefe de Soporte Operativo
A19	Área de equipos servidores y comunicaciones	Contiene los equipos de comunicaciones, seguridad, servidor de archivos y discos duros externos.	Ubicación Física	Departamento de Soporte Operativo, sección TICs	Jefe de Soporte Operativo
A20	Archivo Central	Contiene la información histórica en medio físico (papel) de la Dirección.	Ubicación Física	Departamento de Apoyo Operativo, sección Archivo.	Jefe de Apoyo Operativo

Tabla 8. Listado de activos de información y soporte.

5.6. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Para realizar la identificación de amenazas y vulnerabilidades que pueden afectar a los activos de información y soporte identificados y registrados de la Dirección, se debe tener en cuenta los siguientes conceptos definidos en la norma ISO 27005 - Gestión del Riesgo en la Seguridad de la Información:

- Amenaza: es una causa potencial de una falla inesperada que podría dañar un sistema o un activo.
- Vulnerabilidad: es la debilidad de un activo que puede ser explotada por una o más amenazas.

Para la identificación y análisis de amenazas y vulnerabilidades relacionadas con los activos de la Dirección, se ha tomada como referencia los anexos C y D de la norma técnica colombiana ISO 27005 - Gestión del Riesgo en la Seguridad de la Información, así como los resultados de las entrevistas aplicadas a los funcionarios de la Dirección. En la siguiente tabla, se presentan las vulnerabilidades y amenazas identificadas con sus riesgos asociados por tipo de activo:

Tipo Activo	Amenaza	Vulnerabilidades	Riesgos
Información	Robo de información	Ausencia de controles físicos y lógicos en los sistemas y equipos que procesan y almacenan información.	Falta de disponibilidad o ausencia de información y posible uso de la misma con fines malintencionados.
	Accesos no autorizados	Sistema de autenticación inadecuado, deficiente configuración, aplicaciones no protegidas contra accesos lógicos y físicos.	Falta de confidencialidad de la información.
	Alteración de información	Ausencia de protección de la información, registro y respaldos (copias), y de controles de entrada de datos.	Informes no confiables e íntegros de la Dirección por manipulación de la información.
	Códigos maliciosos o virus informáticos	No ejecución de actualizaciones periódicas de antivirus	Daño a los sistemas informáticos, equipo computacional e información
	Errores de usuario	Registro y mantenimiento de datos incorrecto, ausencia de controles en el ingreso de información, ausencia de procesos disciplinarios.	Falta de integridad de la información procesada y generada en la Dirección.
	Hackers – espionaje	Arquitectura de red insegura, falta de equipos de seguridad perimetral y ausencia de un SGSI formalmente implementado	Ingreso a los sistemas informáticos y equipos computacionales por personal no autorizado con fines maliciosos que pueden dañar la imagen institucional y pérdida y/o secuestro de información.
Hardware	Falla y/o daño en equipo computacional (servidor y computadores)	No ejecución de mantenimientos preventivos periódicos, ausencia de controles ambientales adecuados y procedimientos de revisión	Falta de disponibilidad de la información almacenada en los equipos y paralización de las actividades de la Dirección.

Tipo Activo	Amenaza	Vulnerabilidades	Riesgos
		y mantenimiento inadecuados.	
	Robo	Inadecuadas seguridades y controles físicos, ausencia de un seguro vigente para el equipo computacional	Pérdidas económicas y de información que podría asumir la Dirección.
	Políticas y procedimientos para administración de hardware no definidos	Uso inadecuado del hardware	Evasión de responsabilidades en el uso del hardware por el personal de la Dirección
Software	Mal funcionamiento del software	Software obsoleto o no actualizado	Falta de integridad de la información procesada a través del software implementado en la Dirección.
	Robo y/o daño del software	Falta de copias periódicas de respaldo y de controles de acceso lógico y procedimientos de revisión y mantenimiento inadecuados.	Fata de disponibilidad del software de la Dirección.
	Uso de software no licenciado	Ausencia de controles de instalaciones de software no autorizado	Riesgos legales por uso de software no licenciado que pueden afectar a la Dirección.
	Falsificación de credenciales de acceso al software	Administración y custodia inadecuada de cuentas y claves de acceso	Acceso no autorizado a datos e información confidencial.
	Políticas y procedimientos para administración de software no definidos	Uso inadecuado del software	Evasión de responsabilidades en el uso del software por el personal de la Dirección.
Ubicación Física	Accesos no autorizados	Falta de registro y control físico a las ubicaciones físicas	Ausencia de controles de acceso a personal no autorizado a las ubicaciones críticas de la Dirección.
	Fuego	Sistemas de extinción de incendios no implementados o con mal funcionamiento por falta de revisiones y mantenimientos periódicos.	Daños de equipos sensibles, pérdidas de información, pérdidas financieras y paralización de las actividades normales de la Dirección.
	Políticas y procedimientos para administración de ubicaciones físicas críticas no definidos	Uso inadecuado a las ubicaciones físicas críticas	Evasión de responsabilidades por parte del personal de la Dirección que está a cargo de las ubicaciones físicas.

Tabla 9. Amenazas, vulnerabilidades y riesgos por activo.

5.7. VALORACIÓN DE LOS ACTIVOS

De acuerdo con la norma ISO 27001, la valoración de los activos de información y de soporte de la Dirección, se realizará considerando los criterios de integridad, disponibilidad y confidencialidad de la información. Para establecer la valoración de los activos se aplicarán los niveles y valores descritos en la siguiente tabla:

Requisito	Niveles de Valoración					
	Bajo	**Valor**	**Medio**	**Valor**	**Alto**	**Valor**
Confidencialidad	El activo es **público** y su divulgación no ocasiona impacto en la Dirección en caso de que llegue a manos o sea conocido por personal no autorizado.	1	El activo es considerado de **uso interno** y si es accedido por personal no autorizado de la Dirección, el impacto sería importante.	2	El activo es considerado **privado**, su uso o acceso por personal no autorizado de la Dirección el impacto sería crítico.	3
Integridad	La falta de integridad del activo ocasiona un bajo impacto en la Dirección.	1	La falta de integridad del activo ocasiona un impacto significante en la Dirección.	2	El daño o modificación no autorizada es de alto impacto para la Dirección. .	3
Disponibilidad	Si el activo no está disponible para la Dirección por más de dos (2) días, no existe impacto o es muy bajo.	1	El activo puede estar no disponible para la Dirección hasta dos (2) días.	2	El activo no puede superar un (1) día de indisponibilidad para no afectar a la Dirección.	3

Tabla 10. Niveles de valoración de criterios de integridad, disponibilidad y confidencialidad.

Al igual que en la metodología de evaluación de riesgos de seguridad de la información (descrita en el punto 5.4), para valorar los niveles de cada requisito se utiliza una escala de Likert de 1 al 3, siendo 1 el valor más bajo, y 3 el valor más alto. Para el cálculo del valor del activo se aplica la siguiente fórmula:

Valor Activo = valor confidencialidad + valor integridad + valor disponibilidad

El valor más alto que un activo puede tener es 9, y el valor mínimo es 3. Para la gestión de riesgos se considerarán los activos con valor igual o mayor a 5, que se considera son los de

mayor importancia dentro de la Dirección y requieren de controles adecuados y eficientes para garantizar su integridad, disponibilidad y confidencialidad.

En la siguiente tabla, se describen los resultados obtenidos de la valoración realizada a los activos de información y de soporte de la Dirección, aplicando los niveles y valores descritos:

Cód.	Activo	Tipo	Confiden-cialidad	Integridad	Disponi-bilidad	Valor Total
A01	Plan estratégico institucional	Información	2	3	1	6
A02	Planes operativos	Información	3	3	3	9
A03	Informes de evaluaciones	Información	3	3	1	7
A04	Comunicaciones	Información	3	3	3	9
A05	Expedientes personales	Información	3	3	1	7
A06	Informes Jurídicos	Información	2	3	1	6
A07	Cursos y especializaciones	Información	1	2	1	4
A08	Manuales de estatutos, políticas, procedimientos, reglamentos	Información	1	3	1	5
A09	Inventario de hardware y software	Información	2	3	2	7
A10	Informes soporte técnico	Información	2	2	1	5
A11	Respaldos información	Información	3	3	3	9
A12	Listado de cuentas y claves de usuarios administradores	Información	3	3	3	9
A13	Información correo electrónico	Información	2	2	2	6
A14	Computadores de escritorio y portátiles	Hardware	2	3	3	8
A15	Servidor de archivos	Hardware	3	3	3	9
A16	SIIPNE	Software	2	3	3	8
A17	Sistema Quipux	Software	2	3	2	7
A18	Discos duros externos	Hardware	3	3	3	9
A19	Área de equipos servidores y comunicaciones	Ubicación Física	3	3	3	9
A20	Archivo Central	Ubicación Física	2	2	1	5

Tabla 11. Valoración de activos de información y soporte.

La siguiente tabla describe los activos ordenados por su valor de mayor a menor:

Cód.	Activo	Tipo	Valor Total
A02	Planes operativos	Información	9
A04	Comunicaciones	Información	9
A11	Respaldos información	Información	9
A12	Listado de cuentas y claves de usuarios administradores	Información	9
A15	Servidor de archivos	Hardware	9
A18	Discos duros externos	Hardware	9
A19	Área de equipos servidores y comunicaciones	Ubicación Física	9
A14	Computadores de escritorio y portátiles	Hardware	8
A16	SIIPNE	Software	8
A03	Informes de evaluaciones	Información	7
A05	Expedientes personales	Información	7
A09	Inventario de hardware y software	Información	7
A17	Sistema Quipux	Software	7
A01	Plan estratégico institucional	Información	6
A06	Informes Jurídicos	Información	6
A13	Información correo electrónico	Información	6
A08	Manuales de estatutos, manuales, reglamentos	Información	5
A10	Informes soporte técnico	Información	5
A20	Archivo Central	Ubicación Física	5
A07	Cursos y especializaciones	Información	4

Tabla 12. Activos de información y soporte ordenados de menor a mayor por su valor.

De los resultados obtenidos después de valorar de los activos, se puede concluir que de los 20 activos de información y de soporte levantados, únicamente el activo Cursos y Especializaciones, no será considerado para la gestión de riesgos por su calificación igual a 4, es decir, el 95% de los activos levantados serán considerados en la evaluación y análisis de riesgos.

5.8. GESTIÓN DE RIESGOS

Los riesgos se analizarán basándonos en los activos valorados, la probabilidad de ocurrencia del riesgo (amenaza) y el impacto que puede ocasionar la falta de integridad, disponibilidad y confidencialidad.

Mediante la evaluación y análisis de riesgos de los activos de información la Dirección podrá realizar:

- Identificación objetiva de los activos de información y de soporte críticos que afectan en la continuidad de las operaciones.
- Evaluar la efectividad de los procedimientos y controles de seguridad establecidos.

- Optimización de las inversiones relacionadas con seguridad de la información.
- Monitoreo del aumento o disminución de los niveles de riesgo.

En el Anexo II, se presenta la matriz de riesgos de los activos de información y de soporte seleccionados para el análisis y evaluación, la misma que se elaboró aplicando la metodología de riesgos de seguridad de la información descrita en el punto 5.4.

En la tabla 13, se muestra un resumen de la matriz de riesgos, en la que se puede evidenciar el Nivel de Valoración establecido para cada activo de la Dirección:

No.	Datos del Activo			Descripción Riesgo	Nivel de Riesgo	Nivel de Valoración	Tratamiento
	Cód.	Nombre	Tipo				
R1	A01	Plan estratégico institucional	Información	Acceso no autorizado al Plan Estratégico Institucional que ocasione su pérdida o alteración y uso indebido y falta de confidencialidad, integridad y disponibilidad del Plan.	12	MY	Mitigar
R2	A02	Planes operativos	Información	Acceso no autorizado a los Planes Operativos que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los planes.	15	NA	Mitigar
R3	A03	Informes de evaluaciones	Información	Acceso no autorizado a los Informes de Evaluaciones que ocasione su pérdida o alteración, y uso indebido y falta de confidencialidad, integridad y disponibilidad de los informes.	12	MY	Mitigar
R4	A04	Comunicaciones	Información	Acceso no autorizado a las Comunicaciones que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de las comunicaciones.	15	NA	Mitigar
R5	A05	Expedientes personales	Información	Acceso no autorizado a los Expedientes Personales que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los expedientes.	12	MY	Mitigar
R6	A06	Informes Jurídicos	Información	Acceso no autorizado a los Informes Jurídicos que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los informes.	12	MY	Mitigar
R7	A08	Manuales de estatutos, políticas, procedimientos, reglamentos	Información	Acceso no autorizado a los Manuales, Estatutos, Políticas, Procedimientos, Reglamentos, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad en los mismos.	6	MD	Asumir
R8	A09	Inventario de hardware y software	Información	Acceso no autorizado al Inventario de hardware y Software, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad en el inventario.	12	MY	Mitigar

No.	Datos del Activo			Descripción Riesgo	Nivel de Riesgo	Nivel de Valoración	Tratamiento
	Cód.	Nombre	Tipo				
R9	A10	Informes soporte técnico	Información	Acceso no autorizado a los Informes de Soporte Técnico, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los informes.	9	MY	Mitigar
R10	A11	Respaldos de información	Información	Acceso sin autorización a los respaldos de información que ocasionaría en mayor nivel pérdida de su disponibilidad, así como de su confidencialidad e integridad.	20	NA	Mitigar
R11	A12	Listado de cuentas y claves de usuarios administradores	Información	Acceso no autorizado al Listado de Cuentas y Calves de Usuarios Administradores, que ocasione su pérdida o alteración y uso indebido, y falta de integridad, disponibilidad y confidencialidad del listado.	15	NA	Mitigar
R12	A13	Información correo electrónico	Información	Acceso no autorizado a la Información del Correo Electrónico, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de esta información.	15	NA	Mitigar
R13	A14	Computadores de escritorio y portátiles	Hardware	Falta de disponibilidad de la información almacenada en las computadoras y paralización de las actividades de la Dirección, pérdidas económicas y uso indebido de la información almacenada en estos equipos.	16	NA	Mitigar
R14	A15	Discos duros externos	Hardware	Falta de disponibilidad de la información almacenada en los discos duros, pérdidas económicas y uso indebido de la información almacenada en estos dispositivos.	15	NA	Mitigar
R15	A16	Servidor de archivos	Hardware	Falta de disponibilidad de la información y datos almacenados en el servidor de archivos y paralización de las actividades de la Dirección, pérdidas económicas y uso indebido de la información almacenada en el servidor.	15	NA	Mitigar
R16	A17	SIIPNE	Software	Falta de integridad de la información procesada a través del sistema SIIPNE, falta de disponibilidad del sistema SIIPNE, riesgos legales por uso de software no licenciado y evasión de responsabilidades del personal que utiliza este sistema.	10	MY	Mitigar
R17	A18	Sistema Quipux	Software	Falta de integridad de la información procesada a través del sistema Quipux, falta de disponibilidad del sistema Quipux, riesgos legales por uso de software no licenciado y evasión de responsabilidades del personal que utiliza este sistema.	6	MD	Asumir
R18	A19	Área de equipos servidores y de comunicaciones	Ubicación Física	Control de acceso físico inadecuado a la oficina de equipos servidores y de comunicaciones, daños y/o pérdidas de estos equipos y de la información que almacenan.	10	MY	Mitigar
R19	A20	Archivo Central	Ubicación Física	Control de acceso físico inadecuado al archivo central, pérdida o robo de la información almacenada en esta área.	8	MY	Mitigar

Tabla 13. Resumen matriz de riesgos de activos de información y de soporte.

Luego del análisis y evaluación de riesgos de los activos de información y de soporte de la Dirección, se obtuvo los siguientes resultados:

- Se han registrado y evaluado 19 riesgos relacionados con los activos de la Dirección.
- 8 activos tienen un Nivel de Valoración No Aceptable.
- 9 activos tienen un Nivel de Valoración Mayor.
- 2 riesgos están dentro del Nivel de Valoración aceptado por la Dirección (menor o igual a 7.99), y 17 requieren tratamiento para mitigar su efecto.
- Los activos con mayor nivel de riesgo y que requieren de mayor prioridad para su tratamiento son:
    - Planes operativos
    - Comunicaciones
    - Respaldos de información
    - Listado de cuentas y claves de usuarios administradores
    - Información correo electrónico
    - Computadores de escritorio y portátiles
    - Discos duros externos
    - Servidor de archivos

Para poder realizar la mitigación de los riesgos, se necesita verificar, seleccionar e implementar controles, buscando siempre un equilibrio en el costo beneficio de su implementación.

5.9. SELECCIÓN DE CONTROLES A IMPLEMENTAR

La selección de controles para los activos que requieren mitigación, es el insumo principal para el plan de tratamiento de riesgos que se debe aplicar en la Dirección. Esta selección se realizará utilizando como referencia el Anexo A del estándar ISO 27001 (que forma parte del Anexo III de este documento), en el que para cada dominio se definen objetivos de control, que de acuerdo con el nivel de riesgo de cada activo serán seleccionados, para posteriormente incluir los controles requeridos en la declaración de aplicabilidad.

La siguiente tabla describe los Dominios y Objetivos de Control seleccionados para cada activo que requiere un plan de mitigación, considerando sus amenazas, vulnerabilidades y nivel de valoración del riesgo:

Cód.	Nombre	Amenazas	Vulnerabilidades	Nivel de Valoración Riesgo	Dominio	Objetivo de Control
A01	Plan estratégico institucional	• Robo de información • Acceso no autorizado • Alteración de información • Virus informáticos • Errores de usuario • Hackers – espionaje	• Ausencia de controles físicos y lógicos • Sistema de autenticación deficiente. • Falta de protección de la información. • No ejecución de actualizaciones periódicas de antivirus • Incorrecto ingreso, controles de entrada de datos no efectivos. • Arquitectura de red insegura, falta de equipos de seguridad perimetral. • Ausencia de políticas de seguridad de la información formalmente definidas	MY	A.5 Políticas de Seguridad de la Información	• A.5.1 Directrices de la gestión de seguridad de la información
A02	Planes operativos			NA	A.6 Organización de la seguridad de la información	• A.6.1 Organización interna
A03	Informes de evaluaciones			MY	A.8 Gestión de activos	• A.8.1 Responsabilidad por los activos • A.8.2 Clasificación de la información
A04	Comunicaciones			NA	A.9 Control de acceso	• A.9.1 Requisitos de la empresa para el control de acceso • A.9.2 Gestión de acceso de usuario • A.9.4 Control de acceso a sistema y aplicación
A05	Expedientes personales			MY	A.11 Seguridad física y ambiental	• A.11.1 Áreas seguras • A.11.2 Equipos
A06	Informes Jurídicos			MY	A.12 Seguridad de las operaciones	• A.12.1 Procedimientos y responsabilidades operativas • A.12.3 Respaldo
A09	Inventario de hardware y software			MY	A.13 Seguridad de las comunicaciones	• A.13.1 Gestión de seguridad de la red • A.13.2 Transferencia de información
A10	Informes soporte técnico			MY	A.16 Gestión de incidentes de seguridad de la información	• A.16.1 Gestión de incidentes de seguridad de la información y mejoras
A11	Respaldos información			NA		
A12	Listado de cuentas y claves de usuarios administradores			NA		
A13	Información correo electrónico			NA		

Cód.	Nombre	Amenazas	Vulnerabilidades	Nivel de Valoración Riesgo	Dominio	Objetivo de Control
A14	Computadores de escritorio y portátiles	• Falla y/o daño en equipo computacional (servidor y computadores) • Robo • Políticas y procedimientos para administración de hardware no definidos	• No ejecución de mantenimientos preventivos periódicos, ausencia de controles ambientales • Inadecuadas seguridades y controles físicos • Uso inadecuado del hardware	NA	A.5 Políticas de Seguridad de la Información	A.5.1 Directrices de la gestión de seguridad de la información
A15	Discos duros externos			NA	A.11 Seguridad física y ambiental	• A.11.1 Áreas seguras • A.11.2 Equipos
A16	Servidor de archivos			NA		
A17	SIIPNE	• Funcionamiento incorrecto de software • Robo y/o daño • Uso de software no licenciado • Falsificación de credenciales de acceso al software • Políticas y procedimientos para administración de software no definidos	• Software obsoleto o no actualizado • Ausencia de copias periódicas de respaldo y falta de controles de acceso lógico • Ausencia de controles de instalaciones de software no autorizado • Administración inadecuada de cuentas y claves de acceso • Uso inadecuado del software	MY	A.5 Políticas de Seguridad de la Información	A.5.1 Directrices de la gestión de seguridad de la información
					A.9 Control de acceso	• A.9.1 Requisitos de la empresa para el control de acceso • A.9.2 Gestión de acceso de usuario A.9.4 Control de acceso a sistema y aplicación
					A.12 Seguridad de las operaciones	• A.12.1 Procedimientos y responsabilidades operativas • A.12.2 Protección contra códigos maliciosos • A.12.3 Respaldo de información
A19	Área de equipos servidores y de comunicaciones	• Accesos no autorizados • Fuego • Políticas y procedimientos para administración de ubicaciones físicas críticas no definidos	• Falta de registro y control físico a las ubicaciones físicas • No se tiene implementados sistemas de control de incendios • Uso inadecuado de las ubicaciones físicas críticas	MY	A.5 Políticas de Seguridad de la Información	A.5.1 Directrices de la gestión de seguridad de la información
A20	Archivo Central			MY	A.11 Seguridad física y ambiental	• A.11.1 Áreas seguras • A.11.2 Equipos

Tabla 14. Selección de dominios y objetivos de control para los activos de acuerdo a amenazas, vulnerabilidades y nivel de riesgo.

5.10. DECLARACIÓN DE APLICABILIDAD

Una vez que se han seleccionado los objetivos de control para cada activo de acuerdo con sus amenazas, vulnerabilidades y nivel de valoración del riesgo, se elabora la Declaración de Aplicabilidad que es parte del SGSI de la Dirección. Para este fin, se considera lo establecido en la norma ISO 27001, que indica: diseñar una Declaración de Aplicabilidad que cuente con controles necesarios y se debe justificar los que se incluyen y los que se excluyen, refiriéndonos a los controles del Anexo A de esta norma.

Los controles descritos en el Anexo A de la norma ISO 27001, se explican con mayor detalle en la norma ISO 27002 - Código de Prácticas para los Controles de Seguridad de la Información, en la que se establece la siguiente estructura para cada categoría de control:

- Categoría principal de cada control de seguridad (Dominio), que contiene:
    - Un objetivo del control; y
    - Uno o más controles.

El formato establecido para la Declaración de Aplicabilidad de la Dirección General de Seguridad Ciudadana y Orden Público es el siguiente:

- Sección: número secuencial para el dominio, objetivo de control y control.
- Descripción del control: de acuerdo con el Anexo A de la norma ISO 27001.
- Estado Actual del Control: implementado, parcialmente implementado, por implementar.
- Aplica Si/No: indica si el control se selecciona para implementar o no.
- Justificación de la Selección (Si) o de la Exclusión (No): se debe indicar la justificación de la selección del control o, por el contrario, la justificación de la exclusión del control.

La Declaración de Aplicabilidad definida para la Dirección se encuentra detallada en el Anexo III. El resumen de los dominios, objetivos de control y controles seleccionados y que se deben implementar se describe en la siguiente tabla:

Nro.	Descripción Dominio – Objetivo de Control - Controles
	Políticas de Seguridad de la Información
	Dirección de gestión de seguridad de la información
1.	Políticas de Seguridad de la Información
2.	Revisión de las políticas para la seguridad de la información
	Organización de la Seguridad de la Información
	Organización interna
3.	Roles y responsabilidades para la seguridad de la información
4.	Separación de funciones
	Gestión de activos
	Responsabilidad de los activos
5.	Inventario de activos
6.	Propiedad de los activos
7.	Uso aceptable de los activos
8.	Devolución de activos
	Clasificación de la información
9.	Directrices de Clasificación de la información
10.	Etiquetado de la información
11.	Manejo de los activos
	Control de acceso
	Requisitos institucionales para el control de acceso
12.	Política de control de acceso
13.	Acceso a redes y servicios de red
	Gestión de acceso de los usuarios
14.	Registro y retiro de usuarios
15.	Provisión de accesos a usuarios
16.	Revisión de los derechos de acceso de usuario
17.	Retiro o adaptación de los derechos de acceso
	Control de acceso a sistemas y aplicaciones
18.	Restricción del acceso a la información
19.	Procedimientos seguros de inicio de sesión
	Seguridad física y ambiental
	Áreas seguras
20.	Controles físicos de entrada
21.	Seguridad de oficinas, despachos e instalaciones
	Seguridad de los Equipos
22.	Ubicación y protección de equipos
23.	Mantenimiento de los equipos
24.	Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento
25.	Equipo informático de usuario desatendido
26.	Política de puesto de trabajo despejado y pantalla limpia
	Seguridad de las operaciones
	Procedimientos y responsabilidades operacionales
27.	Documentación de procedimientos de operación

Nro.	Descripción Dominio – Objetivo de Control - Controles
28.	Gestión de cambios
29.	Gestión de capacidades
	Protección contra códigos maliciosos
30.	Controles contra malware
	Respaldo de información
31.	Copias de seguridad de la información
	Seguridad de las comunicaciones
	Gestión de la seguridad de redes
32.	Controles de red
33.	Seguridad de los servicios de red
34.	Separación en las redes
	Transferencia de información
35.	Políticas y procedimientos de transferencia de información
36.	Mensajería electrónica
	Gestión de incidentes de seguridad de la información
	Gestión de los incidentes de seguridad de la información y mejoras
37.	Responsabilidades y procedimientos
38.	Reporte de los eventos de seguridad de la información
39.	Reporte de debilidades de seguridad de la información
40.	Apreciación y decisión sobre los eventos de seguridad de la información
41.	Respuesta a incidentes de seguridad de la información
42.	Aprendizaje de los incidentes de seguridad de la información
43.	Recopilación de evidencias

Tabla 15. Resumen de controles seleccionados en la Declaración de Aplicabilidad.

5.11. DOCUMENTACIÓN DE CONTROLES PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Después de seleccionar los controles que se propondrán para que se implementen como parte del SGSI de la Dirección General de Seguridad Ciudadana y Orden Público, se debe realizar su documentación tomando como referencia las guías de la norma ISO 27002, para su posterior implementación. A continuación, se documentan los controles seleccionados en la Declaración de Aplicabilidad.

5.11.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de las políticas de seguridad de la información es proporcionar orientación y apoyo para la seguridad de la información en la Dirección, en concordancia con sus objetivos estratégicos y cumplimiento de leyes y normas relacionadas.

5.11.1.1. DOCUMENTACIÓN DE LAS POLÍTICAS

En el punto 5.3, de acuerdo a la metodología que se está aplicando para el desarrollo del SGSI en la Dirección, se definió la Política General de seguridad de la información, para complementar, se proponen las siguientes políticas de seguridad de la información:

- El Oficial de Seguridad de la Información o responsable de seguridad, debe garantizar la socialización de las políticas de seguridad de la información y capacitación a los empleados de la Dirección.
- La clasificación de los activos de información de la Dirección, se basa en los criterios de integridad, disponibilidad y confidencialidad de cada uno de los activos, y contempla el impacto que puede causar en la Dirección la pérdida de alguna de estas propiedades.
- La información generada en la Dirección a través de los diferentes sistemas, aplicaciones y equipo computacional es de uso exclusivo para las actividades que realicen los funcionarios de la Dirección, por lo que está estrictamente prohibido divulgarla, transferirla o modificarla sin autorización del propietario de la información.
- Todos los empleados de la Dirección están en la obligación de informar al Oficial de Seguridad de la Información la existencia de incidentes o amenazas que puedan perjudicar a la integridad, confidencialidad y disponibilidad de la información institucional.
- Queda prohibido a todos los funcionarios generar copias de archivos o información de otras personas; hacerse pasar por otra persona en una comunicación que no le pertenece, o enviar información en nombre de otra persona sin su consentimiento.
- No está permitido usar recursos tecnológicos y de telecomunicaciones para actividades que no se encuentren relacionadas con lo laboral y funciones asignadas al personal de la Dirección.
- Está prohibido conceder permisos de uso de los sistemas y aplicativos informáticos de la Dirección a personas sin la autorización respectiva.
- Para el servicio de correo electrónico institucional se establecen las siguientes restricciones:
    - Enviar contenidos con fines publicitarios y comerciales en beneficio de familiares, terceros o propio.
    - Envío de spam, es decir, que tenga relación con virus, publicidad corporativa, mensajes en cadena, entre otros.

  - Usar el correo electrónico de otro usuario.
  - Falsificación de correos electrónicos.
  - Dar lectura, borrar, realizar una copia o una modificación a correos electrónicos de otros usuarios, sin autorización.
  - Transferir archivos que tengan virus o cualquier tipo de programa que pueda ser perjudicial.
- Está prohibido el uso de equipos computacionales que sean de propiedad de los funcionarios de la Dirección, en la red de datos de la Dirección.
- Si no se cumplen las políticas de Seguridad de la Información definidas, los funcionarios recibirán sanciones de acuerdo al Reglamento Interno de la Comandancia General de Policía.

El SGSI de la Dirección también debe considerar el cumplimiento de las normas y disposiciones establecidas en:

- Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público
- Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional
- Decretos Ejecutivos, Reglamentos y Leyes que rigen a la Policía Nacional del Ecuador.

5.11.1.2. REVISIÓN DE LAS POLÍTICAS

Las políticas de seguridad de la información deben ser verificadas de forma anual o cuando se realicen cambios significativos en la infraestructura tecnológica y de los funcionarios de la Dirección, con el objetivo de garantizar que se mantenga su vigencia y aplicabilidad. Esta revisión debe ser coordinada a través del Oficial de Seguridad de la Información o responsable de seguridad.

5.11.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo es definir una estructura organizativa para la seguridad de la información para dar inicio y tener un control de la implementación y operación de la gestión de seguridad de la información en la Dirección.

5.11.2.1. ROLES Y RESPONSABILIDADES

Se propone los siguientes niveles y roles de responsabilidad para la Gestión de Seguridad de la información en la Dirección:

- Comité de Seguridad de la Información:
  - Planificar, coordinar y supervisar el SGSI.
  - Revisar y aprobar las políticas y procedimientos de seguridad de la información.
  - Revisión y aprobación del plan anual de Seguridad de la Información.
  - Recibir, analizar y aprobar los informes presentados por la Unidad de Seguridad de la Información y, de ser el caso, dar recomendaciones y resoluciones pertinentes.
- Director de la DGSCyOP:
  - Promover la cultura de seguridad de la información dentro de la Dirección.
  - Difundir e implementar las políticas de seguridad de la información al interior de la Dirección.
  - Cumplir y hacer cumplir las políticas y procedimientos para la gestión de seguridad de la información aprobadas por el Comité de Seguridad de la Información.
  - Designar recursos, la infraestructura tecnológica, física y los funcionarios necesarios para gestionar de manera adecuada la seguridad de la información en la Dirección
- Oficial de Seguridad de la Información o responsable de seguridad:
  - Desarrollar y proponer políticas de gestión de la seguridad de la información en la Dirección y establecer controles lógicos, técnicos, físicos y administrativos para tratar riesgos que se encuentren relacionados con la seguridad de la información.
  - Dar soporte a los funcionarios de la Dirección en la identificación de la información sensible y sus riesgos asociados, levantamiento y clasificación de activos de información, identificación e implementación de las medidas y controles de seguridad necesarias para los activos de información.
  - Analizar, monitorear e informar cualquier evento o incidente que quebrante la seguridad de la información en la Dirección.

- Asignar identificadores de usuario, claves y accesos lógicos a los distintos sistemas informáticos de la Dirección, así como también la creación de roles de usuarios.
- Gestionar la evaluación periódica del desempeño del SGSI, a fin de tomar acciones orientadas a mejorarlo.
- Actualizar las políticas y procedimientos de seguridad de la información y verificar su cumplimiento.
- Socializar las políticas y procedimientos de seguridad de la información al personal de la Dirección.

- Responsable de TICs:
  - Garantizar el cumplimento de los requisitos y políticas de seguridad de la información establecidos para el funcionamiento, gestión y comunicación de los aplicativos informáticos e infraestructura tecnológica de la Dirección.
  - Garantizar que los sistemas y aplicaciones informáticas de la Dirección incluyan medidas de seguridad y controles de acceso lógico.
  - Aplicar buenas prácticas para garantizar la seguridad de la información en los servicios y procedimientos de la Sección de TICs.
- Jefaturas Departamentales:
  - Cumplir y controlar la aplicación de las políticas y procedimientos de seguridad de la información por parte del personal a su cargo.
  - Solicitar al área de Talento Humano y al Oficial de Seguridad de la Información la creación, cambio o modificación de usuarios, roles (perfiles), accesos, a los sistemas de información y otros recursos tecnológicos de la Dirección del personal a su cargo.
  - Solicitar la remoción de derechos de acceso a los sistemas y aplicativos informáticos de los usuarios que no los requieran para desempeñar sus tareas.
  - Reportar incidentes relacionados con la seguridad de la información al Oficial de Seguridad de la Información.
- Usuarios finales (de los activos de información y de soporte):

- Dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información.
- Participar en los cursos de capacitación y eventos de concientización que el Oficial de Seguridad de la Información organice como parte de su gestión.
- Dar lectura a los documentos publicados en la intranet o comunicados por correo electrónico sobre temas de seguridad de la información.

La conformación del Comité de Seguridad de la Información propuesta es la siguiente:

- Un representante del Subcomando General de Policía
- Director de la DGSCyOP
- Oficial de Seguridad de la Información
- Un representante de las jefaturas departamentales

5.11.2.2. SEGREGACIÓN DE TAREAS (FUNCIONES)

Para una adecuada segregación o separación de funciones se deben aplicar los siguientes controles:

- Ningún funcionario de la Dirección deberá tener privilegios para registrar, autorizar y cancelar una transacción, esto como mecanismo de protección para los mismos funcionarios y la Dirección.
- Cada transacción debe pasar por las etapas de: aprobación, autorización, ejecución y registro. Estas etapas deben ser gestionadas por un funcionario independiente en el departamento responsable de la transacción.
- Los cargos que se establezcan en la Dirección deben estar definidos en la estructura orgánica y funcional de la Dirección.

5.11.3. GESTIÓN DE ACTIVOS

El propósito de la gestión de activos es el siguiente:

- Identificar todos los activos de la Dirección y establecer responsabilidades para una buena protección de los activos.

- Garantizar que toda información cuente con un nivel correcto de protección respecto al nivel de importancia y clasificación para la Dirección.
- No permitir que la información se divulgue, modifique, elimine o destruya, sin la autorización del propietario o responsable de la misma, independientemente del medio de almacenamiento en el que se almacene.

5.11.3.1. INVENTARIO DE ACTIVOS

Los controles propuestos son:

- Los activos de información y de soporte deben estar identificados de manera única en el inventario de activos de información de la Dirección.
- El Oficial de Seguridad de la Información tiene la responsabilidad de levantar y registrar un inventario de activos de información conjuntamente con los propietarios de los mismos, con los siguientes datos: código, descripción, tipo, ubicación, propietario, calificación y clasificación.

5.11.3.2. PROPIEDAD DE LOS ACTIVOS

Los controles propuestos son:

- Todos los activos de soporte e información que forman parte de la Dirección deben tener asignado un propietario.
- El inventario de activos de información deberá incluir los propietarios designados, así como los funcionarios responsables de custodiarlos.

5.11.3.3. USO ACEPTABLE DE LOS ACTIVOS

Los controles propuestos son:

- Los funcionarios y directivos de la Dirección, así como el personal externo, tienen la responsabilidad de cumplir con las políticas y directrices dispuestas por la Dirección

para el uso de la información, para garantizar su confidencialidad, integridad y disponibilidad.

- Todas las plataformas y aplicaciones informáticas en las que se procese y/o conserve información sensible deberán tener implementado un sistema automático de control de acceso, tales como: claves de acceso o credenciales de acceso, registro de pistas de auditoría (logs), control de horarios de acceso, siempre tomando en cuenta la parte técnica y de costo beneficio sea factible tener estas funcionalidades.
- Los propietarios de la información son los únicos autorizados para transmitir o compartir información de la Dirección que sea confidencial o de uso interno.

5.11.3.4. DEVOLUCIÓN DE ACTIVOS

Los controles propuestos son:

- Todos los funcionarios de la Dirección deben realizar la devolución de los activos que se les ha asignado para el desarrollo de su trabajo, una vez que terminen sus funciones en la Dirección o sean trasladados a otra dependencia.
- La devolución de los activos debe realizarse a través de un acta de entrega recepción formalmente firmada y aceptada por el funcionario que entrega los activos y el que los recibe.

5.11.3.5. DIRECTRICES DE CLASIFICACIÓN DE LA INFORMACIÓN

Los controles propuestos son:

- Se tiene que diseñar una metodología para analizar, calificar y clasificar los activos de Información de la Dirección, la misma que incluya:
    - Reglas para valorar y clasificar los activos de información de acuerdo a los criterios de integridad, disponibilidad y confidencialidad.
    - Formato para etiquetar los activos de información y de soporte alineado a la clasificación establecida.

5.11.3.6. ETIQUETADO DE LA INFORMACIÓN

Los controles propuestos son:

- Para el etiquetado de los activos registrados en el inventario, se utilizará la siguiente clasificación: privado, uso interno y público.
- El Oficial de Seguridad de la Información, con el apoyo de los propietarios de los activos de información y de soporte, debe gestionar el etiquetado de los activos de la Dirección.

5.11.3.7. MANEJO DE LOS ACTIVOS

Los controles propuestos son:

- Implementación y desarrollo de controles y prohibiciones para un adecuado manejo de la información, especialmente la clasificada como privada y de uso interno de la Dirección.
- Cuando un funcionario de la Dirección requiera realizar una impresión, copia, almacenamiento, envío e intercambio de información, debe estar autorizado por el responsable de la misma, y cuando sea necesario el Oficial de Seguridad de la Información verificará el adecuado tratamiento a la información de acuerdo a las políticas de seguridad de la información de la Dirección.

5.11.4. CONTROL DE ACCESO

El control de acceso tiene como objetivos:

- Restringir los accesos de todos recursos tecnológicos de la Dirección, por medio de los cuales se almacena y procesa la información que es propiedad de la Dirección.
- De acuerdo con los criterios de confidencialidad y disponibilidad de la información, asegurar que únicamente se registren funcionarios y usuarios autorizados para el acceso a los activos de información y de soporte.

5.11.4.1. POLÍTICAS DE CONTROL DE ACCESO

Los controles propuestos son:

- En el punto 5.11.1 se incluye todas las políticas propuestas para el control de accesos a los recursos tecnológicos y activos de información y de soporte de la Dirección.
- El cumplimiento de las políticas de seguridad de la información es obligatorio para todos los funcionarios de la Dirección, y también para personal externo que por razones laborales y de relación con la Dirección podría tener acceso a estos recursos.
- A los funcionarios y usuarios de la Dirección se les asignarán los permisos de acceso (lógicos y físicos), estrictamente requeridos para el desarrollo de sus funciones.

5.11.4.2. ACCESO A REDES

Los controles propuestos son:

- Los funcionarios de la Dirección (usuarios autorizados), únicamente tienen acceso a la red de datos y a servicios de red que se autoricen a usar para el cumplimiento de sus funciones.
- Todas las computadoras y equipos conectados a una red de datos de la Dirección deben tener asignada una dirección IP válida, asignada por el área de TICs.

5.11.4.3. ADMINISTRACIÓN DE CUENTAS Y ROLES DE USUARIOS

Los controles propuestos son:

- Cuando se requiera efectuar asignación de claves y roles de acceso a los funcionarios y usuarios de la Dirección, se realizará a través del Oficial de Seguridad de la Información o responsable de seguridad, previo requerimiento formal del jefe inmediato.
- El Oficial de Seguridad de la Información o responsable de seguridad debe verificar que la generación de contraseñas de acceso a los sistemas y aplicaciones considere, siempre que sea factible, lo siguiente:
    - Tener una longitud mínima definida por el fabricante o proveedor del software.
    - Usar combinación de letras y números no asociados a fechas, o nombres fácilmente identificables.

- Contar con un período de vigencia obligando al usuario a modificarla periódicamente.

- El Oficial de Seguridad de la Información o responsable de seguridad puede revocar los permisos de acceso de un funcionario de la Dirección en los casos que se detecte que se ha incumplido con las políticas de seguridad de la información, con la autorización del director o jefes departamentales.
- La sección TICs realizará los trabajos de mantenimiento en aplicaciones/servidores y base de datos, mediante usuarios con perfiles restringidos para el efecto.

5.11.4.4. CONTROLES DE ACCESO A SISTEMAS Y APLICACIONES

Los controles propuestos son:

- La sección TICs que tiene a cargo la gestión de los aplicativos informáticos implementados en la Dirección, deben velar que los mismos cuenten con controles de acceso lógicos de acuerdo a las políticas de seguridad de la información establecidas en la Dirección.
- Los funcionarios responsables de los activos de información y de soporte (designados en el inventario de activos de información de la Dirección), establecerán las restricciones y controles de acceso, de la información procesada a través de las aplicaciones y sistemas informáticos de la Dirección.
- Todo el software y/o aplicativo informático que se implemente en la Dirección, debe contar con licencia de uso respectiva, con la finalidad de evitar problemas legales por el uso y acceso a software no licenciado.

5.11.4.5. ACCESO A SERVIDORES

Los controles propuestos son:

- El acceso a servidores de archivos se asigna únicamente a los funcionarios de la sección TICs, responsables de la administración de los mismos, con perfiles autorizados para realizar las labores propias del cargo, por lo tanto, se debe tener en cuenta los siguientes aspectos:

    - Proteger la seguridad y confidencialidad de la información almacenada en los servidores de archivo.

- Evitar compartir el servidor o dar acceso a funcionarios no autorizados al servidor de archivos.

5.11.5. SEGURIDAD FÍSICA Y AMBIENTAL

La seguridad física y ambiental tiene los siguientes objetivos:

- Asegurar el buen funcionamiento de los recursos y equipos tecnológicos de la Dirección, para que su vida útil se alargue lo máximo posible.
- Evitar el acceso físico sin previo control o autorización a los espacios físicos de mayor importancia y criticidad de la Dirección, así como la implementación de controles físicos y ambientales en el área de servidores y de los dispositivos de comunicación, para minimizar riesgos relacionados con pérdida, fallas o daños de estos equipos y la información que almacenan.
- Garantizar la seguridad ambiental para los activos de información y de soporte, a través de controles de temperatura, humedad, sensores, alarmas, y que se encuentren en áreas físicas limpias para su adecuado funcionamiento.
- Establecer una política de pantalla limpia para los equipos computacionales asignados a los funcionarios de la Dirección.

5.11.5.1. ÁREAS SEGURAS

Las áreas seguras que la Dirección posee, en la que se almacena información y documentos son:

- Archivo central
- Cuarto de servidores y comunicaciones
- Archivadores ubicados en los departamentos

Los controles propuestos son:

- El Oficial de Seguridad de la Información o responsable de la seguridad, tiene que implementar controles de seguridad perimetral sobre las áreas físicas críticas de la Dirección, como, por ejemplo: cámaras de seguridad, puertas con control de acceso electrónico o llaves, alarmas, protección de ventanas, entre otras.

- Los funcionarios de la Dirección que tienen la responsabilidad sobre las áreas seguras, deben contribuir con el control de acceso a las mismas, para garantizar que únicamente personal autorizado acceda a las mismas.
- El Oficial de Seguridad de la Información o responsable de la seguridad, debe garantizar que en las áreas seguras no se almacenen materiales de fácil combustión o que tengan amenazas relacionadas con inundaciones o incendios.
- Las áreas seguras deben contar con sistemas o dispositivos de extinción de incendios, complementados con alarmas para la detección oportuna de condiciones inadecuadas en las mismas.
- Para el ingreso de funcionarios de la Dirección o de personal externo a las áreas seguras, se debe mantener un registro de acceso que incluya: nombres de la persona que acceda, fecha y hora de acceso, motivó, datos del funcionario que autoriza y firmas.

5.11.5.2. SEGURIDAD EN OFICINAS

Los controles propuestos son:

- Los funcionarios de la Dirección deben llevar de manera obligatoria su credencial visible en todo momento.
- Para el personal externo a la Dirección, se debe contar con tarjetas de visitantes que se le entregará al ingreso a la Dirección, y de igual forma este personal debe llevar la identificación de visitante durante el tiempo que permanezca en las oficinas de la Dirección.
- Queda estrictamente prohibido cualquier tipo de actividad de comercio dentro de las instalaciones de la Dirección, esto incluye comerciantes externos o que los propios funcionarios ejerzan diferentes actividades de comercio dentro de las instalaciones.
- Los funcionarios que deban ingresar a las instalaciones de la Dirección en días no laborables, tienen que realizar una solicitud previa, al jefe inmediato, con copia al Oficial de Seguridad de la Información o responsable de seguridad, donde se especifique su nombre, la fecha en la que se va a acceder, departamento al que pertenece, y las razones por la cuales ingresará a las instalaciones en días no laborales.
- Los funcionarios de la Dirección, así como los visitantes o personas externas que necesiten ingresar computadoras o dispositivos tecnológicos personales a las instalaciones de la Dirección, estos equipos tienen que ser registrados en el momento de su ingreso y salida.

5.11.5.3. ESCRITORIOS LIMPIOS

Los controles propuestos son:

- Todos los funcionarios, al dejar su área de trabajo, tienen que realizar un bloqueo de la computadora, y guardar de manera segura cualquier tipo de documento o dispositivo que contenga información importante.
- De igual forma, los funcionarios de la Dirección al terminar su horario de trabajo deberán guardar de manera segura cualquier tipo de documento o dispositivo que contenga información importante, y apagar el equipo tecnológico que está a su cargo.
- La información o documentos institucionales considerados como privados y de uso interno, y que está a cargo de los funcionarios de la Dirección o propietarios de la misma, en todo momento deben ser almacenados en archivadores, armarios o cajones bajo llave.

5.11.5.4. EQUIPOS DE USUARIOS

Los controles propuestos son:

- Para reducir los riesgos relacionados con pérdidas y/o daños de las computadoras asignadas a los funcionarios de la Dirección, deben ser ubicados dentro de oficinas o áreas seguras.
- Los equipos servidores, computadoras de escritorio y equipos de comunicación deben contar con fuentes alternas de energía (UPS), para minimizar riesgos relacionados con cortes de energía eléctrica.
- El usuario que requiera instalación de software adicional al proporcionado en su computador para el cumplimiento de sus funciones, gestionará esta solicitud al Jefe de Soporte Operativo justificando la necesidad del nuevo software.
- Para el traslado de servidores, computadores, equipos y dispositivos fuera de las instalaciones de la Dirección, se debe contar con la justificación y autorización del jefe inmediato y/o Jefe de Soporte Operativo, y se deberá comunicar al Oficial de Seguridad de la Información o responsable de seguridad, para el registro y control correspondiente.

5.11.5.5. MANTENIMIENTO DE EQUIPOS

Los controles propuestos son:

- Los funcionarios de la sección TICs deben efectuar como mínimo una vez al año, mantenimientos preventivos a los equipos servidores y computadoras de la Dirección, y en el caso de existir problemas o fallas con estos equipos se realizarán mantenimientos correctivos. Cuando sea requerido con autorización del director, se contratará proveedores externos calificados para realizar el mantenimiento.
- El funcionario responsable de TICs, dentro de la planificación anual de su Sección, deberá incluir el mantenimiento preventivo del equipo computacional de la Dirección.
- Todos los mantenimientos realizados al equipo computacional de la Dirección, deben tener un registro con toda la información relacionada a los mismos, y el responsable de llevar este registro es el funcionario de la sección TICs.
- Será responsabilidad de los funcionarios autorizados de la sección TICs, realizar el formateo de las computadoras que se donen o se den de baja, con el objetivo de eliminar todo tipo de información confidencial de la Dirección.
- Si para efectuar un mantenimiento preventivo o correctivo de un equipo de cómputo es requerido su traslado hacia las instalaciones de un proveedor externo autorizado, se deben realizar con la autorización del Jefe de Soporte Operativo.

5.11.6. SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones tiene como objetivos:

- Garantizar el funcionamiento y operatividad correcta y segura de los recursos y activos informáticos y de soporte de la Dirección.
- Establecer responsabilidades y controles al momento de ejecutar operaciones en las instalaciones de tratamiento de información.

5.11.6.1. RESPONSABILIDADES DE OPERACIÓN

Los controles propuestos son:

- Se debe contar con documentación y procedimientos actualizados de la operación realizada a través del equipo computacional de la Dirección.

- Garantizar que los funcionarios de la Dirección no realicen ningún tipo de cambio en las configuraciones de software de antivirus, ni en herramientas que sean parte de la seguridad de los equipos.
- Almacenar o archivar en forma segura en medios físicos o digitales la documentación funcional y técnica de los sistemas y aplicativos informáticos.
- Usar y acceder a la información institucional contenida en los repositorios centrales de almacenamiento (carpetas compartidas), debe estar restringido según el nivel de autorización establecido por el responsable o propietario de la información, quien será el único habilitado para autorizar el acceso al repositorio.
- Prohibir la instalación de aplicaciones o software no autorizadas. En caso de existir excepciones se debe emitir un informe de los riesgos que implica la nueva instalación, en conjunto con el Oficial de Seguridad de la Información o responsable de seguridad.
- Mantener actualizados los sistemas operativos y sistemas de procesamiento de información con los últimos parches de seguridad que se encuentren a disposición por parte de sus proveedores. En caso de excepciones, se debe documentar explicando porque las actualizaciones no son posibles y dar un detalle del riesgo que conlleva.
- El Oficial de Seguridad de la Información o responsable de seguridad, en coordinación con la sección TICs, realizará un análisis de vulnerabilidades sobre la infraestructura tecnológica de la Dirección para identificar posibles brechas de seguridad y tomar las acciones correctivas necesarias.

5.11.6.2. CONTROLES CONTRA VIRUS Y MALWARE

Los controles propuestos son:

- En todos los equipos computacionales de la Dirección se debe implementar software antivirus para minimizar riesgos relacionados con virus informáticos, Estas herramientas deben tener en orden todas las licencias de uso requeridas.
- El Oficial de Seguridad de la Información o responsable de seguridad, debe garantizar que la información almacenada en servidores, computadoras y medios de almacenamiento, sean revisados y escaneados de manera permanente por el software antivirus implementado.

5.11.6.3. RESPALDOS DE INFORMACIÓN

Los controles propuestos son:

- La información almacenada y procesada a través de la infraestructura tecnológica de la Dirección, deberá mantener copias de respaldo, incluyendo su periodo de retención, rotación y métodos apropiados para su restauración. Estas copias de seguridad deben mantenerse en lugares con condiciones físicas, ambientales y de seguridad adecuadas, bajo custodia del responsable de la sección TICs, para garantizar su integridad y disponibilidad.
- Los medios en los que se respalda la información de la Dirección deben ser verificados de manera periódica para asegurar que la información contenida en los mismos se pueda recuperar y ser utilizada cuando se requiera.
- Las copias de respaldo de todos los sistemas y/o aplicativos contenidos en los servidores de la Dirección debe ser realizado por el personal de la sección TICs.

5.11.6.4. GESTIÓN DE CAMBIOS Y CAPACIDAD

Los controles propuestos son:

- El responsable de TICs deberá controlar y registrar todos los cambios o modificaciones que se realicen a los componentes de la infraestructura tecnológica de la Dirección, como son: computadoras, servidores, equipos de comunicación, sistemas informáticos.
- Cualquier cambio o modificación a un elemento de la infraestructura tecnológica de la Dirección debe ser autorizado por el Jefe de Soporte Operativo.
- Es responsabilidad de la sección TICs monitorear de manera permanente la capacidad de los equipos tecnológicos de la Dirección, para solicitar las actualizaciones o mantenimientos requeridos, y garantizar que los mismos se encuentren operativos y con la capacidad requerida para un funcionamiento adecuado.

5.11.7. SEGURIDAD DE LAS COMUNICACIONES

Los objetivos de la seguridad en las comunicaciones son:

- Garantizar que la información transmitida y procesada mediante la red de datos de la Dirección se encuentre protegida.

- Asegurar la confidencialidad e integridad de la información enviada y recibida a través de la red de datos de la Dirección.

5.11.7.1. CONTROLES DE RED

Los controles propuestos son:

- La sección TICs definirá procedimientos de control indispensables para asegurar la disponibilidad de la red de datos de la Dirección y de los servicios asociados a la misma, e implementará controles de seguridad que mantengan la confidencialidad e integridad de la información que se transmite por la red.
- La Dirección a través de los funcionarios de la sección TICs, implementará herramientas, equipos y dispositivos de seguridad, para controlar accesos sin autorización a la red de datos de personal interno o externo.
- Únicamente los equipos propiedad de la Dirección, deberán estar conectados a la red de datos.
- La sección TICs tendrá la responsabilidad de asignar usuarios y claves de acceso a la red de datos institucional, y si es necesario se solicitará autorización al Oficial de Seguridad de la Información.
- El acceso lógico a los servidores y equipos de comunicación a través de la red de datos institucional será administrado por la sección TICs, para lo cual deberá diseñar el esquema de redes, subredes de acuerdo con la criticidad de la información manejada en los diferentes departamentos.
- Los recursos a disposición mediante la red de datos institucional, serán de uso exclusivo para asuntos relacionados con actividades laborales.

5.11.7.2. INTERCAMBIO DE INFORMACIÓN

Los controles propuestos son:

- Para el intercambio de información privada o de uso interno con entidades que no formen parte de la Dirección, la sección TICs debe implementar controles y herramientas que garanticen la confidencialidad e integridad de la información que se intercambia, como por ejemplo software para cifrado de información.
- Para el establecimiento de acuerdos de intercambio de información entre la Dirección y entidades externas, el jefe del departamento que establezca este convenio, coordinará

con el Jefe Jurídico la definición de Acuerdos de Confidencialidad entre la Dirección y la entidad externa, incluyendo los compromisos adquiridos y las penalidades por incumplir estos acuerdos.

- Los Acuerdos de Confidencialidad deben incluir de forma obligatoria las responsabilidades legales que adquieren las entidades externas, por posibles divulgaciones de la información recibida sin previa autorización de la Dirección.
- El servicio de Internet asignado a los funcionarios de la Dirección será utilizado únicamente para tareas relacionadas con funciones laborales.
- El Oficial de Seguridad de la Información o responsable de seguridad en colaboración con el encargado de la sección TICs, establecerá las restricciones de acceso para el uso del servicio de Internet por parte de los funcionarios de la Dirección, y realizará el control y monitoreo del uso que se dé a este servicio.
- Los funcionarios de la Dirección tienen la responsabilidad de:
    - Utilizar el Internet de forma responsable, evitando navegar en sitios web no seguros o descargar archivos o contenido peligroso que pudiera afectar a la información de la Dirección.
    - No acceder a sitios web con contenido de pornografía, drogas o páginas que atenten a los principios éticos y morales que persigue la Dirección y la Policía Nacional.
    - No utilizar sin autorización del Oficial de Seguridad de la Información o jefe inmediato servicios de mensajería o redes sociales como: Facebook, Hotmail, Instagram, Whatsapp o similares.

5.11.7.3. SEGURIDAD DEL CORREO ELECTRÓNICO

Los controles propuestos son:

- A través de la sección TICs se debe implementar herramientas y software antivirus para protección de los mensajes y archivos recibidos a través del servicio de correo electrónico y minimizar riesgos relacionados con spam, virus, intercepción, entre otros.
- Para dar protección a la confidencialidad e integridad de los correos electrónicos, se deben utilizar técnicas de cifrado para mensajes o correos electrónicos que contienen información clasificada como privada o restringida.

- Para el funcionamiento estable del servicio de correo electrónico de la Dirección, el responsable de la sección TICs debe parametrizar el uso del mismo, para que exista un control sobre el tamaño de los archivos adjuntos a transmitir, envió o no a cuentas de correo electrónico personales o fuera del dominio de la Dirección, cantidad de destinatarios, espacio del buzón del correo, etc.
- Los funcionarios de la Dirección utilizarán el correo electrónico institucional sólo para fines laborales.
- Los funcionarios de la Dirección no están autorizados a suscribirse a boletines de tipo comercial o de entretenimiento utilizando el correo electrónico institucional, las únicas suscripciones serán las que son netamente competentes a su trabajo.

5.11.8. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad de la información tiene como objetivos:

- Asegurar una gestión oportuna y eficiente para responder ante riesgos o incidentes de seguridad de la información que pueden ocurrir en la Dirección.
- Minimizar el impacto si llegara a materializarse un riesgo o incidente de seguridad de la información.

5.11.8.1. RESPONSABILIDADES Y PROCEDIMIENTOS

Los controles propuestos son:

- Los incidentes que tengan relación con seguridad de la información deben ser administrados a través de un procedimiento formal, el mismo que debe ser documentado e implementado por el Oficial de Seguridad de la Información o responsable de seguridad.
- Es responsabilidad de los funcionarios de la Dirección ante la identificación de un incidente de seguridad de la información, reportarlo inmediatamente al Oficial de Seguridad de la Información o responsable de seguridad, a través del procedimiento establecido.

5.11.8.2. EVALUACIÓN Y ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los controles propuestos son:

- El Oficial de Seguridad de la Información o responsable de seguridad debe capacitar y dar a conocer a todos los funcionarios de la Dirección el procedimiento para gestión de Incidentes de Seguridad de la Información, así como los medios disponibles para que puedan informar sobre los incidentes (correo electrónico, llamada telefónica, comunicación directa, software de apoyo).
- De acuerdo con el análisis de amenazas y vulnerabilidades realizado en la Dirección, los tipos de incidentes de seguridad de la información para que los funcionarios puedan identificarlos y reportarlos son:
    - Robo y/o alteración de información
    - Accesos no autorizados
    - Virus informáticos
    - Hackeos
    - Falla, daño o robo de equipo computacional
    - Errores en el funcionamiento de software
    - Utilización de software sin licencia
    - Falsificación de credenciales de acceso al software
    - Ingeniería social
    - Incumplimiento de políticas de seguridad de la información
- Se debe mantener un registro de los incidentes de seguridad de la información reportados y solucionados a través del Oficial de Seguridad de la Información o responsable de seguridad, como soporte de esta gestión y para informar al nivel directivo.
- Los reportes relacionados con incidentes de seguridad y análisis de vulnerabilidades deben ser clasificados como privados y serán custodiados por el Oficial de Seguridad de la Información o responsable de seguridad.

5.12. IMPLEMENTACIÓN DE CONTROLES

Antes de desarrollar este punto y los siguientes, es importante aclarar que el alcance del proyecto de diseño de una propuesta de SGSI para la Dirección General de Seguridad Ciudadana y Orden Público, no incluye la implementación de los controles seleccionados y documentados, ya que esto depende, en primer lugar, de la aprobación del SGSI propuesto por parte de las autoridades de la Dirección, además de la disponibilidad de recursos financieros y humanos, y la asignación del tiempo requerido para la implementación.

De igual forma, el alcance no incluye las actividades de las fases de Verificar y Actuar, establecidas en la metodología para desarrollar el SGSI, ya que para ejecutarlas primero se debe hacer una implementación de los controles de seguridad de la información seleccionados. Sin embargo, como un aporte de este trabajo de investigación, se desarrollan de manera general las actividades que la Dirección debe realizar, una vez que se realice la implementación.

Una vez que se han documentado los controles que se aplicarán para el SGSI de la Dirección, se debe establecer un cronograma para su implementación, para lo cual se requiere como ya se indicó anteriormente, de la aprobación del SGSI por parte de las autoridades de la Dirección y la disponibilidad de recursos humanos y financieros, así como la concienciación y participación de todos los funcionarios de la Dirección.

5.13. FORMAR Y CONCIENTIZAR

La norma ISO 27001 establece que la Dirección debe garantizar que todos los funcionarios con responsabilidades definidas en el SGSI, debe ser capacitado en temas relacionados a seguridad de la información para fortalecer sus capacidades en esta gestión, y al resto de funcionarios de la Dirección se debe concientizar y capacitar en las políticas y controles de seguridad de la información que se implementen, para su adecuada aplicación.

De la misma manera, se debe tener el apoyo total de los directivos y jefaturas de la Dirección, para definir las estrategias que contribuyan en el proceso de implementación del SGSI, asignando recursos para planes de capacitación y concienciación permanente en gestión de seguridad de la información.

5.14. REVISAR EL SGSI

La Norma ISO 27001 como parte de la revisión gerencial del SGSI, recomienda que la misma se realice en periodos planeados de tiempo (al menos una vez al año), para garantizar su continua validez, conveniencia y efectividad. Esta revisión permite el análisis y evaluación del SGSI, además de la detección de fortalezas y debilidades para implementar oportunidades de mejora en el SGSI.

En el caso de la Dirección, la verificación del SGSI la debe realizar el Comité de Seguridad de la Información (propuesto como parte de la estructura organizacional del SGSI), por medio de informes entregados por el Oficial de Seguridad de la Información o responsable de seguridad. A continuación, se detalla algunos soportes que se requieren para el proceso de verificación:

- Informes de auditorías internas o externas del SGSI.
- Sugerencias y recomendaciones de los funcionarios de la Dirección.
- Revisión del registro de incidentes de seguridad de la información y de las soluciones adoptadas.
- Cambios organizacionales y de procesos en la Dirección que afecten directamente al SGSI.

La norma ISO 27001 en su apartado “Monitorear y Revisar el SGSI”, establece los siguientes procedimientos que se deben llevar a cabo para realizar el seguimiento al SGSI:

- Realizar procedimientos de monitoreo y revisión; y, otros controles.
- Ejecutar revisiones regulares de la efectividad del SGSI.
- Evaluar la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
- Revisar las evaluaciones de riesgo de manera periódica y sus niveles de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios presentados a nivel de la organización, tecnología y objetivos institucionales.
- Ejecutar auditorías internas al SGSI a intervalos de tiempo planificados.
- Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso del SGSI.
- Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

- Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

Teniendo en cuenta la anterior información, la Dirección debe establecer:

- Mejoramiento del SGSI a través de planes de acción.
- Mantener el análisis y evaluación de riesgos actualizada.
- Actualización, cambio o implementación de nuevos controles.
- Asignación de más recursos para el cumplimiento de los objetivos del SGSI.
- Revisión periódica de los niveles de riesgo aceptados por la Dirección.
- Implementación de estrategias para medir la efectividad de los controles.
- Mejora del procedimiento para la gestión de incidentes de seguridad de la información.

5.15. REALIZAR AUDITORÍAS INTERNAS DEL SGSI

De acuerdo con el estándar ISO 27001, la Dirección debe realizar auditorías internas al SGSI de manera periódica con el fin de evaluar qué los objetivos de control, controles y procesos incluidos en el SGSI cumplan con las necesidades requeridas de seguridad de la información identificadas, además de implementar y dar mantenimiento de manera eficaz, haciéndolo en base a lo esperado.

Para la ejecución de las auditorías internas del SGSI se debe contar con personal certificado y calificado en este tipo de auditorías, debido a que se debe aplicar procedimientos de evaluación y verificación de los controles y procedimientos implementados como parte del SGSI. Se recomienda utilizar personal de auditoría de la Comandancia General.

Como resultado de las revisiones de auditoría, se debe presentar al director un informe de auditoría que incluya:

- Objetivo y alcance de la auditoría
- Periodo de la auditoría y fecha de ejecución
- Metodología y procedimientos de auditoría aplicados
- Los hallazgos, observaciones y conclusiones de la auditoría con sus respectivos soportes y evidencias

5.16. IMPLEMENTAR MEJORAS AL SGSI

De acuerdo a la norma ISO 27001 la Dirección debe realizar una mejora continua para la efectividad del SGSI basándose en el uso y aplicación de la política de seguridad de la información, objetivos de control, análisis de los eventos monitoreados, resultados de auditorías internas o externas, acciones correctivas y preventivas y revisiones gerenciales.

Producto de esta mejora continua se deben implementar las medidas correctivas requeridas para eliminar las observaciones y no conformidades con los requerimientos del SGSI.

Los involucrados en esta etapa por parte de la Dirección son: director, jefaturas y funcionarios, que tiene la responsabilidad de realizar e implementar las acciones de mejora propuestas como resultado de la revisión del SGSI, lo cual permitirá mantener los objetivos del SGSI.

5.17. ESTRUCTURA DE DOCUMENTOS DEL SGSI

De acuerdo con el estándar ISO 27001 los documentos que un SGSI debe incluir son:

- Enunciados documentados de la política SGSI y los objetivos
- El alcance del SGSI
- Procedimientos y controles de soporte del SGSI
- Descripción de la metodología de evaluación de riesgos
- Resultados de la evaluación de riesgos
- Plan de tratamiento de riesgos
- Registros requeridos por el estándar internacional (si se va a optar por la certificación)
- Enunciado de Aplicabilidad.

Para la estructura de los documentos del SGSI propuesto para la DGSCyOP, se recomienda considerar como guía la norma ISO 9001 Estándar de los Sistemas de Gestión de Calidad, la misma que divide a la documentación en cuatro niveles; que adaptados al modelo propuesto del SGSI de la Dirección son:

- Nivel 1: Manual de Gestión de Seguridad de la Información

Es el principal documento del SGSI que incluye los objetivos, alcance, organización, responsabilidades, políticas y procedimientos establecidos para el SGSI propuesto para la Dirección.

- Nivel 2: Procedimientos del SGSI

Incluyen todos los procedimientos formalmente documentados y aprobados por el nivel directivo para la gestión de seguridad de la información y que permite la operatividad del SGSI.

- Nivel 3: Instrucciones, checklists y formularios

Son todos los documentos requeridos para el registro y soporte de las actividades realizadas como parte de la gestión de seguridad de la información en la Dirección.

- Nivel 4: Registros

Son todas las evidencias y soportes a través de los cuales se verifica el cumplimiento de los requisitos del SGSI en la Dirección.

CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES:

Al finalizar el proyecto se obtienen las siguientes conclusiones:

- La Dirección General de Seguridad Ciudadana y Orden Público actualmente no cuenta con un modelo de SGSI para la gestión de la seguridad de la información. Todos los procedimientos que se realizan relacionados con la seguridad, no se ejecutan con base en políticas, lineamientos o estándares, simplemente se basan en normativas generales definidas por la Comandancia General, las cuales no garantizan la seguridad de la información. Por otra parte, los encargados de la sección TICs y de los otros departamentos de la Dirección, no tienen el conocimiento necesario sobre seguridad de la información y normas o estándares relacionados.
- Los activos de información y de soporte de la Dirección no son administrados adecuadamente, debido a que los funcionarios no tienen asignadas formalmente responsabilidades sobre los mismos. Esta situación indica que no se cumplen los controles planteados por la norma ISO 27001, generándose riesgos sobre la información que se registra y procesa en la Dirección.
- Los controles de seguridad lógica y física que se mantienen en la Dirección, están enfocados en aspectos relacionados con evitar robos de equipos, pero se descuidan aspectos como: administración de cuentas, roles y claves de usuarios, acceso a redes de datos, mantenimientos preventivos periódicos, accesos a áreas críticas por personal autorizado y la seguridad en los equipos.
- El modelo de SGSI propuesto para la Dirección General de Seguridad Ciudadana y Orden Público, basado en la Norma ISO 27001 y su guía de buenas prácticas ISO 27002, le permitirá planificar, diseñar, implementar y administrar de manera sistemática y adecuada el SGSI para garantizar la confidencialidad, integridad y disponibilidad de la información que se registra, procesa y almacena en la Dirección.
- Con la metodología aplicada basada en la norma ISO 27001, y el desarrollo y documentación de las etapas correspondientes, se ha cumplido con los objetivos y alcance establecidos para el presente proyecto. Se aporta de forma significativa en mejorar la gestión de seguridad de la información en una institución pública como la Dirección General de Seguridad Ciudadana y Orden Público.

6.2. RECOMENDACIONES:

- Se recomienda implementar el SGSI propuesto en la Dirección, aplicando la metodología establecida basada en la norma internacional ISO 27001; para reducir las brechas de seguridad de la información detectadas. Una vez que se implemente el SGSI, debe ser monitoreado periódicamente para verificar su eficiencia y vigencia.
- Es necesario que todos los funcionarios de la Dirección cuenten con una adecuada y permanente capacitación orientada a los aspectos de seguridad de la información, además de una permanente concientización y conocimiento sobre las políticas y procedimientos y buenas prácticas establecidos en el SGSI, con la finalidad de disminuir el riesgo de ocurrencia de incidentes o eventos que comprometan la seguridad informática en la Dirección.
- El modelo propuesto para el SGSI de la Dirección le permitirá al nivel directivo mantener una visión adecuada del estado de los activos de información y de soporte implementados en la Dirección, por lo que se recomienda que una vez que se implemente el SGSI, se propongan estrategias de cambio y mejora del sistema, se verifiquen las medidas de seguridad aplicadas y los resultados obtenidos. Esto permitirá tomar decisiones de manera objetiva, argumentada y documentada sobre gestión de seguridad de la información, involucrando a todos los funcionarios de la Dirección.
- Finalmente, se recomienda que el modelo de SGSI propuesto para la Dirección, una vez que sea implementado, verificado y monitoreado, sea replicado al resto de Direcciones y dependencias de la Comandancia General de la Policía Nacional.

REFERENCIAS BIBLIOGRÁFICAS

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Paraninfo. https://books.google.com.ec/books?id=_z2GcBD3deYC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Arévalo, M. C. (2020, 13 octubre). *¿Cuántos controles tiene la norma ISO 27001?* Pirani. Recuperado 13 de marzo de 2022, de https://www.piranirisk.com/es/blog/cuantos-controles-tiene-la-norma-iso-27001

Atehortua, F. A., Bustamante, R. E., & Valencia de los Ríos, J. A. (2008). *Sistema de gestión integral. Una sola gestión, un solo equipo*. Universidad de Antioquía. https://books.google.com.co/books?id=15nVyh1Fn6MC&printsec=frontcover&hl=es&source=gbs_atb#v=onepage&q&f=false

Ciclo de Deming: ejemplos, etapas, importancia, ventajas y desventajas. (s. f.). *beetrack.* Recuperado 13 de marzo de 2022, de https://www.beetrack.com/es/blog/ciclo-de-deming-etapas-ejemplos.

Definición del concepto de seguridad. (2020). INSPQ. Recuperado 13 de marzo de 2022, de https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad.

Gallego, D. (2021, 29 diciembre). *¿Qué son las normas ISO?* GlobalSuite Solutions. Recuperado 13 de marzo de 2022, de https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:%7E:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

Estándar Internacional ISO/IEC 27001 (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos*. International Organization for Standardization.

Gutiérrez, C. (2013, 14 mayo). *MAGERIT: metodología práctica para gestionar riesgos. We Live Security*. Recuperado 15 de mayo de 2022, de https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

ISO2700.ES (2022). *Serie 27000. Normas y Descripción.* Recuperado 13 de maro de 2022, de https://www.iso27000.es/iso27000.html

López, A. (s. f.). *Serie 27k*. ISO27000. Recuperado 13 de marzo de 2022, de https://www.iso27000.es/iso27000.html

MAGERIT - versión 3.0. Libro I – Método. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Gobierno de España - Ministerio de Hacienda y Administraciones Públicas (MHAP).

Normas ISO. (s. f.). *ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002*. Recuperado 13 de marzo de 2022, de https://www.normas-iso.com/iso-27001/

NTP-ISO/IEC Norma ISO 27001. (2014). *TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.* (2.a ed.). INDECOPI.

NTC-ISO/IEC Norma ISO 27005. (2009). *Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información*. INCONTEC.

UNE-ISO/IEC 27002. (2015). *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información*. AENOR.

ANEXOS

Anexo I: Cuestionario de entrevistas

Dirección General de Seguridad Ciudadana y Orden Público			
Encuesta sobre Gestión de Seguridad de la Información			
Nombre y Apellido Entrevistado:		**Cargo:**	
Departamento:		**Fecha:**	

Nro.	**Pregunta**
1.	¿Entiende la definición de seguridad de la información? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Si su respuesta es Si, describa esta definición. ....
2.	¿En el departamento a su cargo o en la Dirección se han documentado formalmente y se aplican políticas referentes a seguridad de la información? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta ....
3.	¿En la Dirección existe un responsable a cargo de la gestión de seguridad de la información? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta ....
4.	¿El personal a su cargo tiene definidas responsabilidades en cuanto al uso de recursos informáticos en la Dirección? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta ....
5.	¿Existe un procedimiento que el personal de la Dirección o de su departamento aplique para la identificación y reporte de incidentes de seguridad de la información?

Dirección General de Seguridad Ciudadana y Orden Público			
Encuesta sobre Gestión de Seguridad de la Información			
Nombre y Apellido Entrevistado:		**Cargo:**	
Departamento:		**Fecha:**	

Nro.	Pregunta
	Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta. ....
6.	¿Se realizan simulacros de fallos o amenazas en los sistemas informáticos implementados en la Dirección o en su departamento? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta. ....
7.	¿Existe algún control para el acceso de personal no autorizado a equipos, sistemas informáticos y áreas restringidas de la Dirección? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta. ....
8.	¿Conoce si se realizan mantenimientos periódicos a los equipos informáticos de la Dirección o de su departamento? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta. ....
9.	¿Conoce si la Dirección tiene un plan de gestión de riesgos tecnológicos, de seguridad de la información o de otro tipo de riesgos? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta. ....

Dirección General de Seguridad Ciudadana y Orden Público			
Encuesta sobre Gestión de Seguridad de la Información			
Nombre y Apellido Entrevistado:		**Cargo:**	
Departamento:		**Fecha:**	

Nro.	Pregunta
	.....
10.	¿Conoce los mecanismos y procedimientos de seguridad y control de acceso lógico que se aplican a los sistemas informáticos implementados en la Dirección o en su departamento? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Si su respuesta es Si detalle los mecanismos. ....
11.	¿Conoce si la Dirección cuenta con un inventario de los activos de información? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Justifique su respuesta. ....
12.	¿Conoce de amenazas relacionadas con seguridad de la información a las que la Dirección o su departamento están expuestos? Si ( ) No ( ) Parcialmente ( ) Desconoce ( ) Si su respuesta es Si describa las amenazas. ....
13.	¿En el último año ha recibido capacitación en temas de seguridad de la información? Si ( ) No ( ) Parcialmente ( ) Si su respuesta es Si, describa los cursos o capacitaciones recibidas. ....
14.	¿En el desarrollo de su gestión, qué servicios de TIC requiere? (Por ejemplo: correo electrónico, internet, sistemas informáticos, respaldos de información, mantenimiento y soporte técnico, red de datos, impresiones, etc.)

Dirección General de Seguridad Ciudadana y Orden Público			
Encuesta sobre Gestión de Seguridad de la Información			
Nombre y Apellido Entrevistado:		**Cargo:**	
Departamento:		**Fecha:**	

Nro.	Pregunta
	....
15.	¿Qué procesos, activos tecnológicos y de información tiene a su cargo para el desempeño de sus funciones? Procesos: .... Activos: .....

Anexo II: Matriz de Riesgos de los Activos de Información y de Soporte

No.	Datos Activos				Amenazas	Descripción Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Nivel de Valoración	Tratamiento
	Cód.	Nombre	Tipo	Vlr.							
R1	A01	Plan estratégico institucional	Información	6	● Robo de información ● Acceso no autorizado ● Alteración de información ● Virus informáticos ● Errores de usuario ● Hackers – espionaje	Acceso no autorizado al Plan Estratégico Institucional que ocasione su pérdida o alteración y uso indebido y falta de confidencialidad, integridad y disponibilidad del Plan.	3	4	12	MY	Mitigar
R2	A02	Planes operativos	Información	9		Acceso no autorizado a los Planes Operativos que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los planes.	3	5	15	NA	Mitigar
R3	A03	Informes de evaluaciones	Información	7		Acceso no autorizado a los Informes de Evaluaciones que ocasione su pérdida o alteración, y uso indebido y falta de confidencialidad, integridad y disponibilidad de los informes.	3	4	12	MY	Mitigar
R4	A04	Comunicaciones	Información	9		Acceso no autorizado a las Comunicaciones que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de las comunicaciones.	3	5	15	NA	Mitigar
R5	A05	Expedientes personales	Información	7		Acceso no autorizado a los Expedientes Personales que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los expedientes.	3	4	12	MY	Mitigar
R6	A06	Informes Jurídicos	Información	6		Acceso no autorizado a los Informes Jurídicos que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los informes.	3	4	12	MY	Mitigar
R7	A08	Manuales de estatutos, políticas, procedimientos, reglamentos	Información	5		Acceso no autorizado a los Manuales, Estatutos, Políticas, Procedimientos, Reglamentos, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad en los mismos.	3	2	6	MD	Asumir
R8	A09	Inventario de hardware y software	Información	7		Acceso no autorizado al Inventario de hardware y Software, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad en el inventario.	3	4	12	MY	Mitigar
R9	A10	Informes soporte técnico	Información	5		Acceso no autorizado a los Informes de Soporte Técnico, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de los informes.	3	3	9	MY	Mitigar

No.	Datos Activos				Amenazas	Descripción Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Nivel de Valoración	Tratamiento
	Cód.	Nombre	Tipo	Vlr.							
R10	A11	Respaldos información	Información	9		Acceso no autorizado a los respaldos de información que ocasionaría en mayor nivel pérdida de su disponibilidad, así como de su confidencialidad e integridad.	4	5	20	NA	Mitigar
R11	A12	Listado de cuentas y claves de usuarios administradores	Información	9		Acceso no autorizado al Listado de Cuentas y Calves de Usuarios Administradores, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad del listado.	3	5	15	NA	Mitigar
R12	A13	Información correo electrónico	Información	6		Acceso no autorizado a la Información del Correo Electrónico, que ocasione su pérdida o alteración y uso indebido, y falta de confidencialidad, integridad y disponibilidad de esta información.	3	5	15	NA	Mitigar
R13	A14	Computadores de escritorio y portátiles	Hardware	8	• Falla y/o daño en equipo computacional (servidor y computadores) • Robo • Políticas y procedimientos para administración de hardware no definidos	Falta de disponibilidad de la información almacenada en las computadoras y paralización de las actividades de la Dirección, pérdidas económicas y uso indebido de la información almacenada en estos equipos.	4	4	16	NA	Mitigar
R14	A15	Discos duros externos	Hardware	9		Falta de disponibilidad de la información almacenada en los discos duros, pérdidas económicas y uso indebido de la información almacenada en estos dispositivos.	3	5	15	NA	Mitigar
R15	A16	Servidor de archivos	Hardware	9		Falta de disponibilidad de la información almacenada en el servidor de archivos y paralización de las actividades de la Dirección, pérdidas económicas y uso indebido de la información almacenada en el servidor.	3	5	15	NA	Mitigar
R16	A17	SIIPNE	Software	8	• Mal funcionamiento del software • Robo y/o daño • Uso de software no licenciado • Falsificación de credenciales de acceso al software • Políticas y procedimientos para administración de software no definidos	Falta de integridad de la información procesada a través del sistema SIIPNE, falta de disponibilidad del sistema SIIPNE, riesgos legales por uso de software no licenciado y evasión de responsabilidades del personal que utiliza este sistema.	2	5	10	MY	Mitigar
R17	A18	Sistema Quipux	Software	7		Falta de integridad de la información procesada a través del sistema Quipux, falta de disponibilidad del sistema Quipux, riesgos legales por uso de software no licenciado y evasión de responsabilidades del personal que utiliza este sistema.	2	3	6	MD	Asumir

No.	Datos Activos				Amenazas	Descripción Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Nivel de Valoración	Tratamiento
	Cód.	Nombre	Tipo	Vlr.							
R18	A19	Área de equipos servidores y de comunicaciones	Ubicación Física	9	• Accesos no autorizados • Fuego • Políticas y procedimientos para administración de ubicaciones físicas críticas no definidos	Control de acceso físico inadecuado al área de equipos servidores y de comunicaciones, daños y/o pérdidas de estos equipos y de la información que almacenan.	2	5	10	MY	Mitigar
R19	A20	Archivo Central	Ubicación Física	5		Control de acceso físico inadecuado al archivo central, pérdida o robo de la información almacenada en esta área.	2	4	8	MY	Mitigar

Anexo III: Declaración de Aplicabilidad del SGSI

La estructura de la Declaración de Aplicabilidad es la siguiente:

LEYENDA	
COLOR	DESCRIPCIÓN
	Dominio
	Objetivo de control
	Control de seguridad

A continuación, se describe la Declaración de Aplicabilidad establecida para la Dirección, de acuerdo a los dominios y objetivos de control seleccionados en el punto 7.9:

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.5	**Políticas de Seguridad de la Información**			
A.5.1	**Dirección de gestión de seguridad de la información**			
A.5.1.1	Políticas de Seguridad de la Información	Por Implementar	Si	Es indispensable para la Dirección contar con políticas de seguridad de la información, formalmente aprobadas y socializadas e informadas a los funcionarios.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Por Implementar	Si	Es necesario revisar las políticas de seguridad de la información periódicamente para mantenerlas actualizadas y vigentes.
A.6	**Organización de la Seguridad de la Información**			
A.6.1	**Organización interna**			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Por Implementar	Si	Es necesario que se definan los roles y responsabilidades para la gestión de seguridad de la información en la Dirección.
A.6.1.2	Separación de funciones	Por Implementar	Si	Las responsabilidades en la Dirección deben ser segregadas para reducir las modificaciones no autorizadas o el mal uso de los activos.
A.6.1.3	Contacto con las autoridades		No	Por pertenecer a la Policía Nacional la Dirección está en contacto permanente con todas las autoridades del país.
A.6.1.4	Contacto con los grupos de interés especial		No	La Dirección cuenta con grupos especiales con los cuales está en contacto permanente.
A.6.1.5	Seguridad de la Información en la gestión de proyectos		No	La Dirección no gestiona proyectos, otra área de la Comandancia General tiene esta responsabilidad.
A.6.2	**Dispositivos móviles y teletrabajo**			
A.6.2.1	Política de dispositivos móviles		No	

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.6.2.2	Teletrabajo		No	En la selección de controles a implementar el objetivo de control Dispositivos móviles y teletrabajo no fue seleccionado.
A.7	**Seguridad de los recursos humanos**			
A.7.1	**Antes del empleo**			
A.7.1.1	Selección		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Seguridad de los Recursos Humanos y sus controles.
A.7.1.2	Términos y condiciones laborales		No	
A.7.2	Durante el empleo			
A.7.2.1	Responsabilidades de la Máxima Autoridad o su delegado		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Seguridad de los Recursos Humanos y sus controles.
A.7.2.2	Concienciación, educación y formación en seguridad de la información		No	
A.7.2.3	Proceso disciplinario		No	
A.7.3	Finalización o cambio de empleo			
A.7.3.1	Responsabilidades ante la finalización o cambio de empleo		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Seguridad de los Recursos Humanos y sus controles.
A.8	**Gestión de activos**			
A.8.1	Responsabilidad de los activos			
A.8.1.1	Inventario de activos	Por Implementar	Si	Es indispensable dentro del SGSI de la Dirección mantener un inventario de activos de información y de soporte.
A.8.1.2	Propiedad de los activos	Por Implementar	Si	Todos los activos incluidos en el inventario deben tener asignado un propietario o responsable.
A.8.1.3	Uso aceptable de los activos	Por Implementar	Si	El uso aceptable de los activos de información y de soporte es importante en la Dirección debido a que siempre existe limitaciones en el presupuesto para la renovación o actualización de activos.
A.8.1.4	Devolución de activos	Por Implementar	Si	Debido a la alta rotación de personal policial en la Dirección es importante gestionar adecuadamente la devolución de activos.
A.8.2	Clasificación de la información			
A.8.2.1	Directrices de Clasificación de la información	Por Implementar	Si	Los activos de información deben ser clasificados de acuerdo a sus criterios de confidencialidad, integridad y disponibilidad.
A.8.2.2	Etiquetado de la información	Por Implementar	Si	Una vez que los activos de información se clasifican, deben ser etiquetados de acuerdo a su clasificación.

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.8.2.3	Manejo de los activos	Por Implementar	Si	El manejo adecuado de los activos por parte de los propietarios y funcionarios de la Dirección es importante para garantizar su confidencialidad, integridad y disponibilidad.
A.8.3	Manejo de los soportes de almacenamiento – medios			
A.8.3.1	Gestión de medios extraíbles		No	En la selección de controles a implementar el objetivo de control Manejo de los soportes de almacenamiento no fue seleccionado.
A.8.3.2	Eliminación de los medios		No	
A.8.3.3	Transferencia de medios físicos		No	
A.9	**Control de acceso**			
A.9.1	Requisitos institucionales para el control de acceso			
A.9.1.1	Política de control de acceso	Por Implementar	Si	Es importante contar con una política de control de accesos a los recursos y activos de la Dirección.
A.9.1.2	Acceso a redes y servicios de red	Por Implementar	Si	Debido a que en la Dirección se tiene una red local para la transmisión de información y acceso al servidor de archivos, de debe tener un control de acceso para este recurso
A.9.2	Gestión de acceso de los usuarios			
A.9.2.1	Registro y retiro de usuarios	Por Implementar	Si	Se debe mantener un procedimiento para la administración de cuentas de usuarios en la Dirección.
A.9.2.2	Provisión de accesos a usuarios	Por Implementar	Si	Es importante contar con un control para otorgamiento de roles y derechos de acceso a los usuarios de la Dirección.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales		No	En la Dirección no existen funcionarios con privilegios de acceso especiales, únicamente cuentas de usuarios y claves de acceso a los recursos y activos de la Dirección.
A.9.2.4	Gestión de la información de autenticación secreta de usuarios		No	No existe información secreta a nivel de usuarios en la Dirección.
A.9.2.5	Revisión de los derechos de acceso de usuario	Por Implementar	Si	Se debe realizar una revisión periódica de las cuentas y claves de acceso otorgados a los funcionarios de la Dirección.
A.9.2.6	Retiro o adaptación de los derechos de acceso	Por Implementar	Si	Debido a la rotación de personal policial que existe en la Dirección es importante contar con un control para el retiro o cambios de los derechos de acceso de los usuarios.
A.9.3	Responsabilidades del usuario			
A.9.3.1	Uso de la información confidencial para la autenticación		No	En la selección de controles a implementar el objetivo de control Manejo de los soportes de almacenamiento no fue seleccionado.

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.9.4	Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción del acceso a la información	Por Implementar	Si	Es importante contar en la Dirección con controles de acceso a la información y sistemas informáticos.
A.9.4.2	Procedimientos seguros de inicio de sesión	Por Implementar	Si	Es importante contar con controles para el inicio de las sesiones en los computadores, sistemas informáticos y otros activos de la Dirección.
A.9.4.3	Sistema de gestión de contraseñas		No	En la Dirección no se cuenta con un sistema de gestión de contraseñas, lo que se implementará es un procedimiento de administración de cuentas y roles de usuarios.
A.9.4.4	Uso de herramientas de administración de sistemas		No	En la Dirección no se administran sistemas.
A.9.4.5	Control de acceso al código fuente del programa		No	En la Dirección no se mantiene código fuente de aplicaciones o sistemas informáticos.
A.10	**Criptografía**			
A.10.1	Controles criptográficos			
A.10.1.1	Política de uso de los controles criptográficos		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Criptografía y sus controles.
A.10.1.2	Gestión de Claves		No	
A.11	**Seguridad física y ambiental**			
A.11.1	Áreas seguras			
A.11.1.1	Perímetro de seguridad física		No	La Dirección se encuentra ubicada en el séptimo piso del edificio de la Comandancia General de Policía y no requiere un perímetro de seguridad física.
A.11.1.2	Controles físicos de entrada	Por Implementar	Si	A pesar que el dominio Seguridad Física y del Entorno no está considerado en el alcance del SGSI, en la selección de controles fue escogido por las amenazas y riesgos relacionados con seguridad física y accesos físicos.
A.11.1.3	Seguridad de oficinas, despachos e instalaciones	Por Implementar	Si	Se debe implementar controles para el acceso físico a las instalaciones de la Dirección y a sus áreas críticas.
A.11.1.4	Protección contra las amenazas externas y ambientales		No	La Dirección se encuentra ubicada en el séptimo piso del edificio de la Comandancia General de Policía y existen controles para amenazas externas desde el ingreso al edificio.
A.11.1.5	Trabajo en áreas seguras		No	
A.11.1.6	Áreas de carga y entrega		No	En la Dirección no se tiene áreas de carga y entrega.
A.11.2	Seguridad de los Equipos			

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.11.2.1	Ubicación y protección de equipos	Por Implementar	Si	Dentro de las oficinas de la Dirección se debe contar con controles para la ubicación y protección de los equipos y dispositivos tecnológicos.
A.11.2.2	Instalaciones de suministro		No	La Dirección se encuentra ubicada en el séptimo piso del edificio de la Comandancia General de Policía, y otra área es responsable de las instalaciones de suministro en el edificio.
A.11.2.3	Seguridad del cableado		No	El mantenimiento y soporte técnico del cableado de datos es realizada por otra área de la Comandancia.
A.11.2.4	Mantenimiento de los equipos	Por Implementar	Si	En la Dirección se debe normar el mantenimiento de los equipos ya que se determinó en el diagnóstico que no se realiza de manera periódica.
A.11.2.5	Salida de los activos fuera de las instalaciones de la institución		No	En la Dirección no salen equipos fuera de sus instalaciones.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones		No	
A.11.2.7	Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento		Si	Para el control de los discos duros externos de respaldo se debe mantener este control.
A.11.2.8	Equipo informático de usuario desatendido	Por Implementar	Si	Para las computadoras de la Dirección se debe implementar estos controles, para garantizar su disponibilidad.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Por Implementar	Si	
A.12	**Seguridad de las operaciones**			
A.12.1	Procedimientos y responsabilidades operacionales			
A.12.1.1	Documentación de procedimientos de operación	Por Implementar	Si	En la Dirección únicamente se realizan actividades de soporte técnico a usuarios y administración de los equipos tecnológicos y sistemas informáticos implementados, y estos deben ser documentados.
A.12.1.2	Gestión de cambios	Por Implementar	Si	Se debe realiza un control a los cambios que se realicen únicamente a los activos y recursos informáticos implementados en la Dirección.
A.12.1.3	Gestión de capacidades	Por Implementar	Si	Debido a la limitación de recursos y equipos tecnológicos en la Dirección, es importante controlar las capacidades de los mismos.
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción		No	En la Dirección no es requerido mantener estos ambientes, debido a que no se realiza desarrollo y mantenimiento de sistemas.
A.12.2	Protección contra códigos maliciosos			

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.12.2.1	Controles contra malware	Por Implementar	Si	Se debe contar con controles para la protección de virus u otro código malicioso, en los equipos tecnológicos de la Dirección.
A.12.3	Respaldo de información			
A.12.3.1	Copias de seguridad de la información	Parcialmente Implementado	Si	Se de tener un procedimiento periódico para respaldar la información generada en la Dirección.
A.12.4	Registro y monitoreo			
A.12.4.1	Registro de eventos		No	En la selección de controles a implementar el objetivo de control Registro y Monitoreo no fue seleccionado.
A.12.4.2	Protección de los registros de información		No	
A.12.4.3	Registros de administración y operación		No	
A.12.4.4	Sincronización de relojes		No	
A.12.5	Control del software en producción			
A.12.5.1	Instalación del software en sistemas en producción		No	En la selección de controles a implementar el objetivo Control de Software en Producción no fue seleccionado.
A.12.6	Gestión de la vulnerabilidad técnica			
A.12.6.1	Gestión de las vulnerabilidades técnicas		No	En la selección de controles a implementar el objetivo de control Gestión de Vulnerabilidad Técnica no fue seleccionado.
A.12.6.2	Restricciones en la instalación de software		No	
A.12.7	Consideraciones sobre la auditoría de sistemas de información			
A.12.7.1	Controles de auditoría de sistemas de información		No	En la selección de controles a implementar el objetivo de control Consideraciones sobre Auditoría de Sistemas de Información no fue seleccionado.
A.13	**Seguridad de las comunicaciones**			
A.13.1	Gestión de la seguridad de redes			
A.13.1.1	Controles de red	Por Implementar	Si	La red de datos implementada en la Dirección debe ser controlada y administrada para proteger la información que se transmite a través de la misma.
A.13.1.2	Seguridad de los servicios de red	Por Implementar	Si	Se debe controlar la compartición de archivos y carpetas que se tiene en el servidor de archivos y en las computadoras de la Dirección.
A.13.1.3	Separación en las redes	Por Implementar	Si	Se debe controlar que la red de datos de la Dirección sea exclusiva y no esté compartida por otras áreas o pisos del edificio de la Comandancia.
A.13.2	Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de información	Por Implementar	Si	Deben existir políticas y procedimientos formalmente documentados para las

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
				transferencias de información que se realiza en la Dirección hacia otras dependencias.
A.13.2.2	Acuerdos de transferencia de información		No	Los acuerdos son gestionados por otra área de la Comandancia.
A.13.2.3	Mensajería electrónica	Por Implementar	Si	Deben existir controles para el uso del servicio de correo electrónico institucional.
A.13.2.4	Acuerdos de confidencialidad o no revelación		No	El establecimiento de acuerdos
A.14	**Adquisición, desarrollo y mantenimiento de los sistemas**			
A.14.1	Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas y sus controles, y adicionalmente en la Dirección se realizan actividades de mantenimiento y desarrollo de aplicaciones.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas		No	
A.14.1.3	Controles de transacciones en línea		No	
A.14.2	Seguridad en el desarrollo y en los procesos de soporte			
A.14.2.1	Política de desarrollo seguro		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas y sus controles, y adicionalmente en la Dirección no se realizan actividades de mantenimiento y desarrollo de aplicaciones.
A.14.2.2	Procedimientos de control de cambios en sistemas		No	
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		No	
A.14.2.4	Restricciones a los cambios en los paquetes de software		No	
A.14.2.5	Principios de ingeniería de sistemas seguros		No	
A.14.2.6	Ambiente de desarrollo seguro		No	
A.14.2.7	Desarrollo externalizado		No	
A.14.2.8	Pruebas de seguridad del sistema		No	
A.14.2.9	Pruebas de aceptación de sistemas		No	
A.14.3	Datos de prueba			
A.14.3.1	Protección de los datos de prueba		No	En el alcance del SGSI de la Dirección, no se consideró este dominio.
A.15	**Relaciones con proveedores**			
A.15.1	Seguridad de la información en relación con los proveedores			
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Relaciones con Proveedores y sus controles.
A.15.1.2	Requisitos de seguridad en contratos con terceros		No	
A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones		No	
A.15.2	Gestión de la provisión de servicios del proveedor			
A.15.2.1	Monitoreo y revisión de los servicios de proveedores		No	

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.15.2.2	Gestión de cambios en los servicios de proveedores		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Relaciones con Proveedores y sus controles.
A.16	**Gestión de incidentes de seguridad de la información**			
A.16.1	Gestión de los incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos	Por Implementar	Si	La gestión de incidentes de seguridad de la información está considerada en el alcance del SGSI de la Dirección y los controles de este Dominio son importantes la detección de incidentes o eventos que afecten a la confidencialidad, integridad y disponibilidad de los activos de información y de soporte.
A.16.1.2	Reporte de los eventos de seguridad de la información	Por Implementar	Si	
A.16.1.3	Reporte de debilidades de seguridad de la información	Por Implementar	Si	
A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Por Implementar	Si	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Por Implementar	Si	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Por Implementar	Si	
A.16.1.7	Recopilación de evidencias	Por Implementar	Si	
A.17	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**			
A.17.1	Continuidad de seguridad de la información			
A.17.1.1	Planificación de la continuidad de seguridad de la información		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Aspectos de la Seguridad de la Información para la Gestión de la Continuidad del Negocio y sus controles.
A.171.2	Implementación de la continuidad de seguridad de la información		No	
A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información		No	
A.17.2	Redundancias			
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información		No	En el alcance del SGSI de la Dirección, no se consideró este dominio y sus controles.
A.18	**Cumplimiento**			
A.18.1	Cumplimiento de los requisitos legales y contractuales			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Cumplimiento y sus controles.
A.18.1.2	Derechos de propiedad intelectual		No	
A.18.1.3	Protección de los registros		No	
A.18.1.4	Protección y privacidad de la información de carácter personal		No	
A.18.1.5	Reglamentos de controles criptográficos		No	
A.18.2	Revisiones de seguridad de la información			

Sección	ANEXO A ISO27001 Descripción	Estado actual del Control	Aplica Si/No	Justificación de la selección (Si) o de la exclusión (No)
A.18.2.1	Revisión independiente de seguridad de la información		No	En el alcance del SGSI de la Dirección, no se consideró el dominio Cumplimiento y sus controles.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad		No	
A.18.2.3	Comprobación del cumplimiento técnico		No	