[Logo]

[Nombre de la institución]

FORMATO REFERENCIAL PARA LA ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Tabla de contenido

1. Antecedentes

En esta sección se debe definir por qué se crea una Política de Seguridad de la Información, su importancia, los riesgos de no contar con una o con su respectiva actualización.

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

2. Política de Seguridad de la Información

2.1. Descripción de la Política

Para las instituciones es importante contar con una Política de Seguridad de la Información, ya que a través de este documento se guiará el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la institución, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la institución.

[Ejemplo:

La máxima autoridad o el Comité de Seguridad de la Información de [nombre de institución], entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la institución.

Para el [nombre de la institución], la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo a lo expuesto, esta política aplica a la Institución según como se defina en el alcance, sus funcionarios, terceros, proveedores y la ciudadanía en general (…)[1]]

2.2. Objetivo

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.[3]

[Definir sus objetivos, los cuales deben contemplar los principios básicos a tener en cuenta dentro de la planeación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la institución.

Ejemplo:

- *Minimizar el riesgo en las funciones más importantes de la institución.*
- *Cumplir con los principios de seguridad de la información.*
- *Cumplir con los principios de la función administrativa.*

- *Mantener la confianza de sus clientes, socios y funcionarios.*
- *Apoyar la innovación tecnológica.*
- *Proteger los activos tecnológicos.*
- *Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.[1]]*

2.3. Roles y Responsabilidades

En esta sección se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la Política de Seguridad de la Información.

[La máxima autoridad a través del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la institución.

Cada funcionario líder de la unidad (NJS), es responsable de garantizar que los funcionarios que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la institución.

El Oficial de Seguridad de la Información (OSI) asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.

Cada uno de los funcionarios de la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.][2]

2.4. Alcance y usuarios

En esta sección se debe definir el alcance de la política en la institución. Además, se debe definir cuáles son sus usuarios: personas o grupos de personas que tendrán acceso a esta política y quienes deben acatarla.

[Esta Política se aplica a todo lo que contempla el Esquema Gubernamental de Seguridad de la Información (EGSI), según se define en el documento del Alcance del EGSI.

Los usuarios de este documento son todos los funcionarios de [nombre de la institución], como también terceros externos a la institución (todas las partes interesadas).]

2.5. Comunicación de la Política

En esta sección se debe detallar como se comunicará la Política de Seguridad de la Información a todos los servidores de la institución, mediante talleres/inducciones/propaganda y a través de que medio: correo electrónico, volantes, portal web.

3. Documentos de referencia

En esta sección se debe citar todos los documentos a los que se hace referencia en la Política. Además, se puede incluir las demás políticas de la institución referente a la Seguridad de la Información: como la Política de control de acceso, Política de seguridad para proveedores, entre otros.

- Acuerdo Ministerial 025-2019
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001
- Alcance del Esquema Gubernamental de Seguridad de la Información
- *[Enumerar otros documentos internos de la institución relacionados con esta Política; por ejemplo: el plan de desarrollo estratégico, plan de negocios, documento sobre gestión de riesgos, etc.]*

4. Terminología

En esta sección se debe definir todos los términos/palabras técnicas que se usarán en todo el documento.

[Ejemplo:

***Amenaza:** causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.*

***Confidencialidad:** Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.*

***Disponibilidad:** Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.*

***Integridad:** Propiedad de proteger la precisión y completitud de los activos.]*

Versión:	1.1
Fecha de la versión:	27-02-2020
Creado por:	Dirección Nacional de Interoperabilidad, Seguridad de la Información e Infraestructura
Aprobado por:	Subsecretaría de Estado - Gobierno Electrónico
Nivel de confidencialidad:	Bajo
Referencia:	**[1] MINTIC**; Ministerio de Tecnologías de la Información y Comunicaciones de Colombia; Elaboración de la política general de seguridad y privacidad de la información. **[2] CEUPE**, Centro Europeo de Postgrado, Política de seguridad de la información y SGSI **[3] 27001 ACADEMY**, Implement ISO 27001 and ISO 22301 effortlessly, www.iso27001standard.com

Historial de cambios

Versión	Fecha	Detalle de la modificación	Autor (es)
1.0	11/02/2020	Descripción básica del documento	Max Rohoden
1.1	27/02/2020	Modificación del documento	Luis Gualotuña