**FORMATO REFERENCIAL PARA LA ELABORACIÓN DE LA**

**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (EGSI)**

**Tabla de contenido**

[1. Antecedentes 3](#_Toc160197509)

[2. Objetivo de la Política 3](#_Toc160197510)

[3. Política de Seguridad de la Información 3](#_Toc160197511)

[3.1. Descripción de la Política 3](#_Toc160197512)

[3.2. Declaración de los objetivos de seguridad de la información 4](#_Toc160197513)

[3.3. Roles y Responsabilidades 4](#_Toc160197514)

[3.4. Alcance y usuarios 5](#_Toc160197515)

[3.5. Comunicación de la Política 5](#_Toc160197516)

[3.6. Excepciones y sanciones 5](#_Toc160197517)

[4. Glosario de términos 6](#_Toc160197518)

[5. Documentos de referencia 6](#_Toc160197519)

[6. Firmas de responsabilidad 6](#_Toc160197520)

# Antecedentes

[INCLUIR EN CADA SECCIÓN, LA INFORMACIÓN QUE CORRESPONDE A SU INSTITUCIÓN; el texto del formato es una orientación para la elaboración de su propia documentación, que además requerirá de una investigación complementaria]

En esta sección se debe definir por qué se crea la 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.

El presente documento debe constituir una política de alto nivel, destinada a normar los aspectos más relevantes de la gestión de seguridad de la información, con una vigencia de largo plazo.

Recordar que la Política de Seguridad de la Información define los lineamientos y **compromiso** de las autoridades para proteger la información, garantizando en todo momento su confidencialidad, integridad y disponibilidad; además de prevenir y mitigar los riesgos que pueden afectarla.

**NOTA**: demostrar en todo el momento el compromiso que tienen las autoridades o máxima autoridad con el cumplimiento de esta política y con el Sistema de Gestión de Seguridad de la Información (EGSI). Tener presente que la máxima autoridad es la responsable de aprobar la política y dar vía libre para su publicación y difusión entre todos los funcionarios de la institución.

# Objetivo de la Política

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

Se debe especificar cuál es el objetivo principal de esta política, esto es el para qué la institución va a desarrollar e implementar esta Política de Seguridad de la Información.

*[Ejemplo:*

*[[1]](#footnote-1)Establecer los lineamientos y políticas que permitan a la institución garantizar la adecuada protección de todos sus activos de información y prevenir la materialización de riesgos que puedan afectar su confidencialidad, integridad y disponibilidad…]*

# Política de Seguridad de la Información

## 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 (…)][[2]](#footnote-2)*

## Declaración de los objetivos de seguridad de la información

En esta sección la institución debe declarar los objetivos de seguridad de la información alineados a la estrategia establecida en el “Plan Estratégico Institucional”. Estos objetivos deben ser:

* Coherentes con la política de seguridad de la información;
* Medibles, esto significa que es importante poder determinar si se ha cumplido o no un objetivo;
* Conectados con los requisitos de seguridad de la información aplicables y los resultados de la evaluación de riesgos y el tratamiento de riesgos;
* Comunicados y actualizados según corresponda.

*[Ejemplo:*

*Objetivo 1: Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, a todo el personal de la institución.*

*Objetivo 1: Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.*

*Objetivo 2: Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Institución.]*

**NOTA**: Se deberán crear indicadores alineados a los objetivos planteados y deben ser monitoreados. Considerando que se tiene que planificar como lograr estos objetivos, se debe determinar: qué se hará, qué recursos se requerirán, quién será el responsable, cuándo se completará y cómo se evaluarán los resultados.

## Roles y Responsabilidades

En esta sección cada institución debe incluir los diferentes roles y responsabilidades que considere pertinentes, con el fin de garantizar en todo momento el adecuado uso y protección de sus activos de información.

*[Ejemplo:*

*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.][[3]](#footnote-3)*

## 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.

*[Ejemplo: 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).]*

## 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, otros.

## Excepciones y sanciones

En esta sección se debe definir, en caso de existir, las **excepciones**, especificando en qué casos esta Política no sería aplicable.

De la misma manera, se debe definir las **sanciones** que la institución aplicará en caso de incumplimiento de alguno de los lineamientos establecidos y de lo descrito en la política.

# Glosario de términos

|  |  |
| --- | --- |
| Término | Definición |
| **Tipo de texto para describir el término** | Tipo de texto para incluir la definición del término |
| *Ejemplo:* |  |
| ***OSI*** | *Oficial de Seguridad de la Información* |
| ***Activos de información*** | *Cualquier elemento valioso para una organización que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso* |

# 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

*[Ejemplo:*

* *Ley Orgánica para la Transformación Digital y Audiovisual*
* *Ley Orgánica de Protección de Datos Personales*
* *Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024*
* *Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)*
* *Familia de Normas Técnicas ISO/IEC 27000*
* *Alcance del Esquema Gubernamental de Seguridad de la Información*
* *Plan estratégico institucional*
* *Otros.]*

# Firmas de responsabilidad

|  |  |  |
| --- | --- | --- |
|  | Nombre/Cargo | Firma |
| **Elaborado por:** | Nombres Apellidos/Oficial de Seguridad de la Información |  |
| **Revisado por:** | Nombres Apellidos/Presidente del Comité |  |
| **Aprobado por:** | Nombres Apellidos/Máxima Autoridad |  |

# Control de versiones del formato referencial

|  |  |
| --- | --- |
| **Versión**: | 1.0 |
| **Fecha de la versión**: | 01-03-2024 |
| **Creado por**: | Dirección de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil |
| **Aprobado por**: | Subsecretaría de Gobierno Electrónico y Registro Civil |
| **Nivel de confidencialidad**: | Bajo |

# Historial de cambios del formato referencial

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Detalle del cambio** |
| 1.0 | 01/03/2024 | Emisión inicial del documento |

1. ACADEMIA PIRANI, Guía para hacer una Política de Seguridad de la Información [↑](#footnote-ref-1)
2. MINTIC; Ministerio de Tecnologías de la Información y Comunicaciones de Colombia; Elaboración de la política general de seguridad y privacidad de la información. [↑](#footnote-ref-2)
3. CEUPE, Centro Europeo de Postgrado, Política de seguridad de la información y SGSI [↑](#footnote-ref-3)