



[Nombre de la Organización]

Política General de Seguridad de la Información y Ciberseguridad.

1. Propósito y Alcance

Esta política tiene como propósito establecer las directrices para proteger la información y los activos de información de **[Nombre de la Organización]** contra amenazas internas y externas, intencionales o accidentales.

Alcance:

- Se aplica a todos los empleados, contratistas y terceros que manejan información de **[Nombre de la Organización]**.
- Cubre todos los sistemas de información, redes, aplicaciones, ubicaciones y procesos de la organización.

2. Objetivos de Seguridad de la Información

Los objetivos principales son:

- **Confidencialidad:** Garantizar que la información sea accesible solo para personas autorizadas.
- **Integridad:** Mantener la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando lo requieran.

3. Compromiso de la Dirección

La alta dirección de **[Nombre de la Organización]** se compromete a:

- Apoyar la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).
- Proporcionar los recursos necesarios para cumplir con esta política y los objetivos establecidos.
- Cumplir con todas las leyes, regulaciones y requisitos contractuales aplicables.

Firma:

[Nombre del Director General]

[Título]

Fecha: ____ / ____ / ____

4. Roles y Responsabilidades

Alta Dirección:

- Proporcionar liderazgo y apoyo para el SGSI.
- Aprobar políticas y procedimientos relacionados con la seguridad de la información.

Responsable de Seguridad de la Información (CISO):

- Gestionar y supervisar el SGSI.
- Coordinar la evaluación y tratamiento de riesgos de seguridad.

Equipos de TI:

- Implementar y mantener controles técnicos de seguridad.
- Garantizar la disponibilidad y resiliencia de los sistemas de información.

Empleados y Colaboradores:

- Cumplir con las políticas y procedimientos establecidos.
- Participar en programas de formación en seguridad de la información.
- Reportar cualquier incidente o sospecha de violación de seguridad.

Audidores Internos:

- Evaluar la eficacia del SGSI y proponer mejoras.
- Realizar auditorías periódicas para asegurar el cumplimiento de las políticas.

5. Gestión de Riesgos de Seguridad de la Información

- **Identificación de Riesgos:** Se llevarán a cabo evaluaciones regulares para identificar amenazas y vulnerabilidades.
- **Análisis y Evaluación:** Los riesgos serán analizados en función de su probabilidad e impacto.

- **Tratamiento de Riesgos:** Se implementarán medidas para evitar, mitigar, transferir o aceptar riesgos según corresponda.
- **Revisión Periódica:** Los riesgos y controles serán revisados al menos una vez al año o cuando ocurra un cambio significativo.

6. Controles de Seguridad de la Información

6.1. Políticas y Procedimientos:

- Desarrollo y mantenimiento de documentos que guíen las prácticas de seguridad en la organización.

6.2. Control de Acceso:

- Implementación de medidas para asegurar que solo el personal autorizado pueda acceder a la información y sistemas.

6.3. Seguridad Física y Ambiental:

- Protección de las instalaciones y equipos contra accesos no autorizados, daños y perturbaciones.

6.4. Criptografía:

- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de la información sensible.

6.5. Seguridad en las Comunicaciones y Operaciones:

- Protección de la información durante su procesamiento, almacenamiento y transmisión.

6.6. Adquisición, Desarrollo y Mantenimiento de Sistemas:

- Integración de requisitos de seguridad en todo el ciclo de vida de los sistemas de información.

7. Gestión de Incidentes de Seguridad

- **Detección y Reporte:** Establecer mecanismos para identificar y reportar incidentes de seguridad.
- **Respuesta y Recuperación:** Procedimientos para contener y resolver los incidentes de manera eficiente.
- **Registro y Análisis:** Documentar todos los incidentes y analizar las causas para prevenir futuras ocurrencias.

8. Formación y Concientización

- Implementación de programas de capacitación periódicos para todos los empleados.

- Campañas de concientización para promover una cultura de seguridad en la organización.

9. Gestión de la Continuidad del Negocio

- Desarrollo de planes de continuidad y recuperación ante desastres.
- Realización de pruebas periódicas para asegurar la efectividad de los planes.
- Evaluación y actualización de los planes según sea necesario.

10. Cumplimiento Legal y Contractual

- Identificación y cumplimiento de todas las leyes, regulaciones y obligaciones contractuales aplicables.
- Establecimiento de procedimientos para garantizar el cumplimiento continuo.

11. Revisión y Mejora Continua de la Política

- La política será revisada al menos una vez al año o cuando ocurran cambios significativos en la organización o en el entorno regulatorio.
- Las revisiones serán coordinadas por el Responsable de Seguridad de la Información y aprobadas por la alta dirección.

12. Comunicación de la Política

- La política será comunicada a todos los empleados y estará disponible en la intranet corporativa.
- Se proporcionará a terceros relevantes según corresponda.

13. Sanciones por Incumplimiento

- El incumplimiento de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del empleo.
- Se investigarán todas las violaciones de manera justa y consistente.

14. Aprobación y Vigencia

Esta política entra en vigor a partir de la fecha de su aprobación y reemplaza cualquier política anterior relacionada con la seguridad de la información.

Firma:

[Nombre del Director General]

[Título]

Fecha: ____ / ____ / ____

Anexos

A. Glosario de Términos

- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **CISO:** Chief Information Security Officer o Responsable de Seguridad de la Información.

B. Referencias Normativas

- **ISO/IEC 27001:2022:** Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos.

C. Documentos Relacionados

- Manual del SGSI.
 - Procedimientos de Gestión de Incidentes.
 - Plan de Continuidad del Negocio.
 - Código de Conducta de la Organización.
-

Guía para Personalizar la Plantilla

1. **Información de la Organización:**
 - Reemplaza **[Nombre de la Organización]** con el nombre de tu empresa.
 - Actualiza los títulos y nombres de los responsables según la estructura de tu organización.
2. **Adaptación de Secciones:**
 - Añade, elimina o modifica secciones para reflejar las políticas y procedimientos específicos de tu organización.
 - Incorpora cualquier requisito legal o regulatorio aplicable a tu sector o ubicación geográfica.
3. **Detalles Específicos:**
 - Incluye detalles específicos en los controles de seguridad que tu organización implementa.
 - Personaliza los objetivos y compromisos para alinearlos con la visión y misión de tu empresa.
4. **Proceso de Revisión:**
 - Establece fechas reales y responsables para la revisión y actualización de la política.
 - Asegúrate de que la alta dirección revise y apruebe la política final.
5. **Comunicación:**

- Planifica cómo se comunicará esta política a todo el personal y terceros relevantes.
- Considera sesiones de formación o reuniones informativas para explicar el contenido y la importancia de la política.

Nota: Esta plantilla es una guía y debe ser adaptada para cumplir con los requisitos específicos de tu organización. Se recomienda consultar con profesionales en seguridad de la información para asegurar que la política sea completa y efectiva.