[logo de la organización]

[nombre de la organización]

Commented [20A1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [20A2]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	20000Academy	Plantilla básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El propósito de este documento es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Este documento se aplica a todos los procesos y actividades del SGS.

Los usuarios de este documento son todos los empleados de [nombre de la organización], como también todos los participantes externos que cumplan algún rol en el SGS.

Commented [20A3]: Por favor, incluye el nombre de la organización.

2. Documentos de referencia

- ISO/IEC 20000-1:2018, apartados 8.7.3, 7.5.4.e)
- Proceso de gestión de la seguridad de la información
- Proceso de gestión de continuidad del servicio TI
- Proceso de gestión de disponibilidad del servicio
- Proceso de gestión de incidentes
- Proceso de gestión de cambios

Commented [20A4]: Puedes encontrar una plantilla para este documento en la carpeta "11_Procesos_Aseguramiento_del_Servicio / 11.2_Gestion_de_continuidad_del_servicio_de_TI".

Commented [20A5]: Puedes encontrar una plantilla para este documento en la carpeta "11_Procesos_Aseguramiento_del_Servicio / 11.1_Gestion_de_disponibilidad".

Commented [20A6]: Puedes encontrar una plantilla para este documento en la carpeta "10_Procesos_de_Resolucion_y_Ejecucion / 10.1_Gestion_de_incidentes".

Commented [20A7]: Puedes encontrar una plantilla para este documento en la carpeta "09_Procesos_Diseño_Construccion_y_Transicion_de_Servicios / 09.1_Gestion_de_cambios".

3. Definiciones

[redacted] - característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad - característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

[redacted] - característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información - es la preservación de la confidencialidad, integridad y accesibilidad de la información.

[redacted] - parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Objetivo

El objetivo de la gestión de la seguridad de la información es proporcionar confidencialidad, integridad y accesibilidad de los activos de información y de los activos y servicios de la organización.

El Gerente de Seguridad de la Información es responsable de revisar los objetivos de gestión de la seguridad de la información y de determinar nuevos [redacted].

Commented [20A8]: [redacted]

4.1 Política de Seguridad de la Información

La Política de seguridad de la información es una directriz que proporciona reglas sobre el uso y mal uso de la seguridad de la información de [nombre de la organización].

[redacted]

[lista]

4.2 Requisitos para la seguridad de la información

Los requerimientos legales y normativos y las obligaciones contractuales importantes para la organización en el ámbito de la seguridad de la información, a los que las actividades de seguridad de la información dan cumplimiento, están detallados en el Plan de SGS.

Los requerimientos de servicios que cumplen las actividades de seguridad de la información están detallados en los Requerimientos de nivel de servicios.

4.3 Gestión de riesgos

[redacted]

4.4 Controles de seguridad de la información

[Nombre de la organización] ha implementado y utiliza controles de seguridad físicos, administrativos y técnicos. El Gerente de Seguridad de la información es responsable de lo garantizar que:

- [redacted]

La efectividad de los controles es revisada durante la auditoría interna de seguridad. El Informe de auditoría interna contiene las acciones necesarias.

[redacted]

- [redacted]

4.5 Auditoría interna

Commented [20A9]: [redacted]

Commented [20A10]: [redacted]

Commented [20A11]: Puedes encontrar una plantilla para este documento en la carpeta "04_Plan_de_SGS".

Commented [20A12]: Puedes encontrar una plantilla para este documento en la carpeta "07_Procesos_de_Relacion_y_Acuerdo / 07.2_Gestion_de_niveles_de_servicio".

Commented [20A13]: Si usted ha implementado ISO 27001 consulte la metodología de gestión de riesgos que está usando en función de esa norma.

Commented [20A14]: Puedes encontrar una plantilla para este documento en la carpeta "05_Gestion_de_riesgos".

Commented [20A15]: [redacted]

Commented [20A16]: Puedes encontrar una plantilla para este documento en la carpeta "12_Auditoria_Interna".

Commented [20A17]: [redacted]

Commented [20A18]: Estos puntos son obligatorios, pero puedes incluir elementos adicionales de acuerdo a las prácticas de tu organización.

[Una vez al año] se realiza un auditoría interna de seguridad de la información. El [cargo] designa un auditor.

El Auditor Interno asegura que los resultados de la auditoría sean incluidos en el informe de auditoría interna. El Gerente de mejora continua de servicios revisa los resultados de la auditoría y define oportunidades de mejora.

El Gerente de seguridad de la información es el responsable de seguir y gestionar la resolución de los hallazgos de auditoría interna, quedando registradas en el Formulario de Acciones Correctivas y Preventivas.

4.6 Comunicación de la Política

El Gerente de Seguridad de la Información debe asegurarse de que todos los empleados de (nombre de la organización), como también los participantes externos correspondientes (incluyendo a clientes, usuarios, proveedores externos, y otras partes interesadas relevantes), sean familiarizados con esta Política y con la importancia de dar cumplimiento a la misma.

Después de un cambio relevante en la política, y como mínimo [una vez al año], el Gerente de Seguridad de la Información [mediante un email] al personal apropiado del proveedor del servicio, clientes, y otros proveedores relacionados, indicando la nueva versión del documento, y recordando la importancia de cumplir con la política.

4.7 Gestión de los incidentes de seguridad

Los incidentes de seguridad son gestionados por el proceso de Gestión de Incidentes. Los incidentes de seguridad de la información son clasificados como [...]. El Gerente de Seguridad de la Información define las prioridades para los incidentes de seguridad de la información y los informa al Gerente de Incidentes.

El Gerente de Seguridad de la información analiza los tipos, volúmenes e impactos de los incidentes de seguridad de la información.

El Gerente de seguridad de la información revisa los incidentes de seguridad de la información e identifica mejoras.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

[cargo] aprueba esta política.

Commented [20A19]: Puedes adaptar la frecuencia de acuerdo a las prácticas de tu organización.

Commented [20A20]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo_ CEO, CIO, Director RI, Responsable TI, Responsable del Servicio, etc

Commented [20A21]: Puedes encontrar una plantilla para este documento en la carpeta "14_Mantenimiento_y_mejora".

Commented [20A22]: Puedes ajustarlo de acuerdo a las prácticas de tu organización.

Commented [20A23]: [redacted]

Commented [20A24]: [redacted]

Commented [20A25]: Introduce la categoría de los incidentes de seguridad de la información

[redacted]

Commented [20A26]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo: CEO, CIO, Director TI, Gerente TI, etc.

Commented [20A27]: Esto es sólo una recomendación; ajustar la frecuencia según sea necesario.

Commented [20A28]: [redacted]

[cargo]
[nombre]

_____
[firma]

Commented [20A29]: Sólo es necesario si el Procedimiento para control de documentos establece que los documentos en papel deben ser firmados.