[logo de la organización]

[nombre de la organización]

Commented [AES1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

PROCEDIMIENTOS DE SEGURIDAD PARA EL DEPARTAMENTO DE TI

Commented [AES2]: Las partes de este documento para las que se necesita realizar una especificación más detallada, pueden ser redactas como documentos separados (políticas/procedimientos).

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

Commented [AES3]: 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	Advisera	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación relacionada dentro del alcance del SGSI.

Los usuarios de este documento son empleados de [unidad organizativa de tecnología de la información y de la comunicación].

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31 y A.8.32
- Política de seguridad de la información
- [Plan de recuperación ante desastres]
- [Política sobre dispositivos móviles, tele-trabajo y trabajo desde casa]
- [Política de clasificación de la información]
- [Inventario de activos]
- [Política de seguridad para proveedores]
- [Política de desarrollo seguro]
- [Política de control de acceso]

Commented [AES4]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

3. Procedimientos de seguridad para el departamento de TI

3.1. Gestión de cambios

Cualquier cambio sobre sistemas operativos o de producción debe ser realizado de la siguiente forma:

1. Los cambios pueden ser propuestos por [indicar los cargos].
2. Los cambios deben ser autorizados por el [cargo], que debe evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]

Commented [AES5]: Para obtener más información sobre este tema, lea este artículo:

[redacted]

Commented [AES6]: Eliminar este punto si la Política de gestión [redacted]

Commented [AES7]: Eliminar todo este punto si el control [redacted]

Commented [AES8]: Se puede especificar qué es y qué no se [redacted]

Commented [AES9]: Otra forma de formular los pasos, puede [redacted]

El [cargo] es responsable de actualizar los documentos (políticas, procedimientos, planes, etc.) que se han visto afectados por el cambio.

3.2. Gestión de configuración

El [cargo] es responsable de documentar los ajustes de configuración de hardware, software, servicios y redes que se deben aplicar para garantizar

3.3. Gestión de capacidad

El [cargo] es responsable de monitorear el uso de los activos de TIC

3.4. Protección antivirus

El [nombre del software antivirus] debe instalarse en cada plataforma (p. ej., servidores físicos, virtuales o en la nube)

3.5. Copias de seguridad

3.5.1. Procedimiento para copias de seguridad

Se deben crear copias de seguridad para todos los sistemas identificados en la [Estrategia de continuidad de negocio] y con la frecuencia especificada en dicho documento.

Se crean automáticamente registros del proceso de creación de copias de seguridad en los sistemas sobre los que se realiza la copia de seguridad.

3.5.2. Prueba de las copias de seguridad

Las copias de seguridad y el proceso de restauración deben ser probados al menos [una vez cada tres meses] mediante la implementación del proceso de recuperación de datos en [identificar el servidor en el cual se realiza la recuperación de datos] y la verificación de que todos los datos han sido recuperados satisfactoriamente.

Commented [AES10]: Elimine todo este elemento si el control

Commented [AES11]: Eliminar este elemento si el control A.8.6

Commented [AES12]: Eliminar este elemento si el control A.8.7

Commented [AES13]: Eliminar todo este punto si el control

Commented [AES14]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES15]: Eliminar este punto si la Política de

Commented [AES16]: En caso que no exista este documento,

Commented [AES17]: Las copias de seguridad deben ser

Commented [AES18]: Adaptar la frecuencia de acuerdo

3.6. Gestión de seguridad de red

El [cargo] es el responsable de gestionar y controlar las redes de computación, de garantizar la seguridad de la información en las redes, de prevenir la fuga de datos y de proteger los servicios conectados a la red desde accesos no autorizados. Por lo tanto, es necesario:

- Separar la responsabilidad operativa de las redes de la responsabilidad sobre aplicaciones sensible y demás sistemas.
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Garantizar la disponibilidad de los servicios en red [describir los controles que asegurarán la disponibilidad].
- Filtrar el acceso a sitios web con contenido potencialmente malicioso o ilegal, o que puedan utilizarse para la fuga de datos.
- Garantizar que los relojes del sistema en todos los ordenadores estén sincronizados [describa cómo están sincronizados y con qué fuente horaria precisa].

[redacted]

3.7. Servicios de red

El [cargo] debe definir las características de seguridad y el nivel de servicio deseado para todos los servicios en red, si estos servicios son prestados por la organización o son tercerizados. Se deberán documentar estos servicios con los proveedores.

[redacted]

3.8. Eliminación de datos

Todos los datos almacenados en aplicaciones, bases de datos, servidores y redes deben ser eliminados por el propietario del activo cuando ya no se necesiten.

[redacted]

Commented [AES19]: Eliminar todo este punto si el control [redacted]

Commented [AES20]: Para obtener más información sobre este tema, lea estos artículos:

[redacted]

Commented [AES21]: O hacer referencia a la Política sobre [redacted]

Commented [AES22]: Se puede especificar la frecuencia; por [redacted]

Commented [AES23]: Se pueden especificar los controles; por [redacted]

Commented [AES24]: Para obtener más información sobre este tema, lea este artículo:

[redacted]

Commented [AES25]: Si el control A.8.10 está marcado como [redacted]

Commented [AES26]: Por ejemplo, enumere las herramientas [redacted]

3.9. Eliminación y destrucción de equipos y medios

Todos los datos y software con licencia almacenado en medios móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, etc., y también en papel) y en todos los equipos que tienen medios de almacenamiento (por ej., ordenadores, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el medio, antes de ser eliminados o reutilizados.

La persona responsable de borrar los datos o destruir el medio debe informar al propietario del activo en cuestión acerca del borrado o eliminación de datos, y el propietario del activo debe actualizar el inventario de activos.

3.9.1. Equipos

El [cargo] es el responsable de verificar y borrar datos de los equipos, salvo que la Política de clasificación de la información establezca otra cosa. Los datos deben ser borrados (indicar la tecnología utilizada para el borrado de datos en los medios de los equipos), para lo, teniendo en cuenta la sensibilidad de los datos, el proceso no es suficientemente seguro, entonces los medios de almacenamiento deben ser destruidos.

3.9.2. Medios de almacenamiento móviles

El [cargo] es el responsable de borrar datos de los medios de almacenamiento móviles, salvo que la Política de clasificación de la información establezca otra cosa. Los datos deben ser borrados (indicar la tecnología utilizada para el borrado de datos en los medios), para lo, teniendo en cuenta la sensibilidad de los datos, el proceso de borrado no es suficientemente seguro, entonces los medios de almacenamiento deben ser destruidos.

3.9.3. Medios en papel

Los empleados de la organización que manejan documentos individuales son responsables de destruir los medios en papel, salvo que la Política de clasificación de la información establezca otra cosa. Los documentos en papel se destruyen en trituradoras de papel.

3.9.4. Borrado y destrucción de registros; comisión para la destrucción de datos

Se deben llevar registros de todo el borrado o destrucción de datos clasificados como "Restringido" y "Confidencial". Los registros deben incluir la siguiente información: datos sobre los medios, fecha de borrado o destrucción, método de borrado o destrucción, persona que realizó el proceso.

Toda la información clasificada como "Confidencial" debe ser borrada o destruida ante la presencia de una comisión integrada por personas autorizadas a acceder a dicha información.

3.10. Transferencia de información

3.10.1. Canales de comunicación electrónica

La información de la organización puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde Internet, transferencia de

Commented [AES27]: Eliminar todo este punto si los controles

Commented [AES28]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES29]: Eliminar este punto si la Política de

Commented [AES30]: Es posible aclarar que esto significa

Commented [AES31]: Es posible aclarar que esto significa que

Commented [AES32]: Eliminar este punto si el control A.5.9

Commented [AES33]: Eliminar esta sección si el control A.7.14

Commented [AES34]: Eliminar si no existe esta Política.

Commented [AES35]: Por ej., enumerar herramientas

Commented [AES36]: Esto puede ser, por ejemplo, un disco

Commented [AES37]: Eliminar si no existe esta Política.

Commented [AES38]: Eliminar esta sección si el control A.8.10

Commented [AES39]: Eliminar si no existe esta Política.

Commented [AES40]: O especificar alguna otra tecnología.

Commented [AES41]: Adaptar a los niveles de confidencialidad

Commented [AES42]: Eliminar este punto si la Política de

datos por medio de [indicar los nombres de los sistemas de comunicación especializados], teléfonos, equipos de fax, mensajes de texto por teléfonos móviles, medios móviles y foros o redes sociales.

[Cargo] determina qué canales de comunicación se pueden utilizar para cada tipo de información y las posibles restricciones sobre los permisos para usar dichos canales, es decir, define qué actividades serán prohibidas.

Además de los controles establecidos por la Política de clasificación de la información, el [Cargo] determina controles adicionales para cada tipo de datos y canales de comunicación según los resultados de la evaluación de riesgos.

3.10.2. Relaciones con entidades externas

Entre las entidades externas se incluyen a diversos proveedores de servicios, empresas de mantenimiento de software y hardware, empresas que manejan transacciones o procesamiento de datos, clientes, etc.

El [cargo] debe preparar y firmar un acuerdo con la parte externa antes de intercambiar información y/o software a través de medios electrónicos, físicos o verbales. El contrato puede estar en papel o en formato electrónico (por ejemplo, aceptando los términos y condiciones generales) y debe contener cláusulas que coincidan con la evaluación de riesgos, incluyendo, al menos, las siguientes:

- Método de identificación de la otra parte.
- Autorizaciones para acceder a la información.
- Asegurando la inviolabilidad.
- Estándares técnicos para la transferencia de datos.
- Respuesta a incidentes.
- Etiquetado y manejo de información sensible.
- Derechos de autor.

Los acuerdos con terceros externos deben ser confeccionados de acuerdo con la [Política de seguridad para proveedores].

3.11. Manejo del código fuente

Los códigos fuente del programa se almacenan [describa la implementación técnica], y el acceso a él se define en la [Política de control de acceso].

3.12. Uso de programas de utilidad

El [cargo] es responsable de aprobar las solicitudes para el uso de programas de utilidad privilegiados.

3.13. Supervisión del sistema

En base a los resultados de la evaluación de riesgos, el [cargo] decide qué registros se guardarán en qué sistemas, para qué sistemas y por cuánto tiempo. Se deben guardar los registros para todos los sistemas críticos y aquellos de acuerdo con sistemas sensibles.

Commented [AES43]: Se puede especificar el medio en cuestión.

Commented [AES44]: Agregar o eliminar canales de

Commented [AES45]: Se pueden especificar los foros y redes

Commented [AES46]: Este texto puede ser reemplazado

Commented [AES47]: Eliminar si no existe esta Política.

Commented [AES48]: Elimine este elemento si el control A.8.4

Commented [AES49]: Por ejemplo, usando GitHub, Bitbucket,

Commented [AES50]: Eliminar esta sección si el control A.8.18

Commented [AES51]: Un programa de utilidad privilegiado es

Commented [AES52]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES53]: Entre los registros se pueden incluir

Commented [AES54]: Eliminar este texto si el control A.8.15

El [cargo] es el responsable de supervisar diariamente los registros de los fallos informados en forma automática, como también de registrar los fallos informados por los usuarios, de analizar por qué se produjeron los errores, de identificar nuevas amenazas potenciales, así como un potencial de fuga de datos, y de aplicar las acciones correctivas correspondientes. [Se pueden indicar autorizaciones específicas para acciones en caso de error, como también cómo se guardan los registros sobre los errores.]

El [cargo] es el responsable de revisar periódicamente los registros para verificar las actividades de los usuarios, administradores y operadores de sistemas, de identificar nuevas amenazas potenciales, así como el potencial de fuga de datos. La supervisión se realiza de acuerdo a intervalos determinados por el [cargo], que es quien establece y asigna los registros para supervisar y determina cómo se registrará la supervisión. Se debe informar al [cargo] acerca de los resultados de la revisión.

El [cargo] es responsable de monitorear todas las vulnerabilidades de las aplicaciones y otros sistemas, y el [cargo] debe seleccionar las acciones a tomar en caso de que se identifiquen nuevas vulnerabilidades.

El [cargo] es responsable de monitorear las configuraciones aplicadas en los dispositivos y sistemas con respecto a la configuración documentada aprobada, y el [cargo] debe seleccionar las acciones que se tomarán en caso de que las configuraciones reales difieran de las aprobadas.

El [cargo] es responsable de verificar los informes de las pruebas de penetración realizadas y las evaluaciones de vulnerabilidad y de tomar las medidas correctivas apropiadas.

3.14. Monitoreo de amenazas externas

El [cargo] es responsable de monitorear a los proveedores, fabricantes y grupos de referencia de seguridad para identificar amenazas externas que puedan afectar las aplicaciones y los sistemas, y el [cargo] debe seleccionar las acciones que se tomarán en caso de que se identifiquen nuevas amenazas.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
[Nombre del registro de cambio] - en formato electrónico	[Nombre de carpeta de Intranet]	[cargo]	Una vez creado, el registro ya no puede ser modificado.	3 años
[Directorios sobre los canales de comunicación]	[Nombre de carpeta de	[cargo]	Una vez creado, el registro ya no puede ser	3 años

Commented [AES55]: Eliminar este texto si el control A.5.7 está

Commented [AES56]: Eliminar este texto si el control A.8.12

Commented [AES57]: Eliminar este texto si el control A.8.15

Commented [AES58]: Se puede especificar que aquí se incluye,

Commented [AES59]: Eliminar este texto si el control A.5.7 está

Commented [AES60]: Eliminar este texto si el control A.8.12

Commented [AES61]: Si fuera necesario, esto se puede

Commented [AES62]: Eliminar este texto si el control A.8.15

Commented [AES63]: Eliminar este texto si el control A.8.8 está

Commented [AES64]: Eliminar este texto si el control A.8.8 está

Commented [AES65]: Eliminar este texto si el control A.8.8 está

Commented [AES66]: Eliminar esta sección si el control A.5.7

Commented [AES67]: Modifique estos registros para que

[redacted]	[redacted]		[redacted]	
[Registros del proceso para copias de seguridad] - formato electrónico	Sistema que ejecuta el procedimiento de copias de seguridad	[cargo]	Los registros son de sólo lectura, no pueden ser eliminados ni editados.	Los registros son almacenados por el plazo de 1 año.
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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.

Commented [AES68]: Esto es sólo una recomendación; ajustar

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el funcionamiento seguro de los sistemas de TIC.
- Cantidad de incidentes debido a responsabilidades ambiguas para el funcionamiento de los sistemas de TIC.

[cargo]
[nombre]

[firma]

Commented [AES69]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.