[logo de la organización]

[nombre de la organización]

POLÍTICA DE SEGURIDAD DE TI

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

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

Commented [AES2]: Para ver más sobre la estructura de este documento, lea el siguiente artículo:

How to structure the documents for ISO 27001 Annex A controls https://advisera.com/27001academy/blog/2014/11/03/how-to-structure-the-documents-for-iso-27001-annex-a-controls/

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 definir reglas claras para el uso aceptable de los sistemas y de otros activos de información en [nombre de la organización].

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización].

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19 y A.8.23
- Política de seguridad de la información
- [Política de clasificación de la información]
- [Procedimiento para gestión de incidentes]
- [Inventario de activos]
- [Procedimientos operativos para el departamento de TI]
- [Política de transferencia de información]

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la organización, o que se encuentran bajo responsabilidad de la organización. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, medios de almacenamiento de datos, etc.

3.2. Uso aceptable

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de negocios con el objetivo de ejecutar tareas vinculadas con la organización.

3.3. Responsabilidad sobre los activos

Commented [AES4]: Incluya el nombre de su organización.

Commented [AES5]: Incluya el nombre de su organización.

Commented [AES6]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

Commented [AES7]: Puede encontrar plantillas para estos documentos en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

Commented [AES8]: En base a los resultados de la evaluación de riesgos de [redacted]

Commented [AES9]: Eliminar todo este punto si el control A.5.9 [redacted]

Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

3.4. Eliminación de información

[redacted]

3.5. Actividades prohibidas

Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad. También está prohibido:

- Descargar archivos de imágenes o vídeos que no tienen objetivos de negocios, enviar cadenas de correos electrónicos, jugar juegos, etc.
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del [cargo]; el uso en conformidad con la Política de clasificación de la información está permitido.

3.6. Uso de activos fuera de las instalaciones

Los equipos, la información o software, independientemente de su formato o medio de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo del [cargo].

[redacted]

3.7. Devolución de activos a la finalización de un contrato

Al finalizar un contrato de empleo, o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información al [cargo].

3.8. Procedimiento para copias de seguridad

[redacted]

3.9. Protección antivirus/malware

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

Commented [AES11]: Eliminar si el control A.8.19 está marcado [redacted]

Commented [AES12]: Eliminar si no existe esta Política.

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

Commented [AES14]: Se puede especificar si este permiso [redacted]

Commented [AES15]: Eliminar todo este punto si el control [redacted]

Commented [AES16]: Eliminar todo este punto si el control [redacted]

Commented [AES17]: Para obtener más información sobre este tema, lea este artículo:

[redacted]

Commented [AES18]: Adaptar la frecuencia según los [redacted]

Commented [AES19]: Asegurarse que esto no interfiera con los [redacted]

Commented [AES20]: Eliminar todo este punto si el control [redacted]

En cada ordenador debe estar instalado [nombre del malware] con actualización automática activada.

3.10. Facultados para el uso de sistemas de información

Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

[illegible]

Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

3.11. Responsabilidades sobre la cuenta de usuario

[illegible]

El propietario de la cuenta de usuario es su usuario, que es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

3.12. Responsabilidades sobre la clave

Los usuarios deben aplicar las siguientes buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo la dirección y los administradores del sistema.
- [illegible]
- Se deben escoger claves seguras de la siguiente forma:
  - utilizando al menos 16 caracteres;
  - utilizando al menos un carácter numérico;
  - [illegible]

Commented [AES21]: Eliminar si el control A.5.17 está marcado [illegible]

Commented [AES22]: Eliminar todo este punto si la Política de [illegible]

Commented [AES23]: Eliminar todo este punto si el control [illegible]

- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- [illegible]
- [illegible]

3.13. Política de escritorio y pantalla limpios

Toda la información clasificada como "Uso interno", "Restringido" o "Confidencial" de acuerdo a lo establecido en la Política de clasificación de la información, es considerada sensible para este punto.

3.13.1. Política de escritorio limpio

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los dispositivos móviles (terminales), y los medios de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

[illegible]

3.13.2. Política de pantalla limpia

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

[illegible]

3.13.3. Protección de instalaciones y equipos compartidos

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

[illegible]

Commented [AES24]: Eliminar todo este punto si la Política de [illegible]

Commented [AES25]: Para obtener más información sobre este tema, lea este artículo:

[illegible]

Commented [AES26]: Eliminar todo este punto si el control [illegible]

Commented [AES27]: Cambie esta referencia a [illegible]

Commented [AES28]: Elimine este elemento si los controles [illegible]

Commented [AES29]: Eliminar todo este punto si el control [illegible]

Commented [AES30]: Adaptar al sistema que se utiliza en la organización.

Commented [AES31]: Eliminar este punto si el control A.8.1 [illegible]

Commented [AES32]: Por ejemplo, cerrando la instalación, etc.

Commented [AES33]: Por ejemplo, cerrando la instalación, etc.

El uso no autorizado de impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado [indicar los equipos y su ubicación] se evita [indicar cómo].

Antes de abandonar las instalaciones por un periodo más prolongado o de forma permanente, se debe realizar una inspección detallada de las habitaciones, las oficinas y el mobiliario que se encuentra en ellas para asegurarse de que no se dejen atrás los bienes de [nombre de la organización].

3.14. Uso de Internet

Sólo se puede acceder a Internet a través de la red local de la organización, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está prohibido.

El [cargo] puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la organización, con el fin de reducir el riesgo de acceso a sitios web con contenido malicioso o ilegal, o que puedan ser utilizados para la fuga de datos. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita al [cargo] solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.

El usuario debe considerar como no confiable la información recibida a través de sitios web no verificados. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

3.15. Correo electrónico y otros métodos de intercambio de mensajes

Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde Internet, la transferencia de datos por medio de [indicar los nombres de los sistemas de comunicación especializados], teléfonos, equipos de fax, el envío de mensajes de texto por teléfonos móviles, medios móviles y foros o redes sociales.

De acuerdo con [Procedimientos de seguridad para el departamento de TI / Política de transferencia de información], como también con la [Política de clasificación de la información], el [cargo] determina el canal de comunicación que se puede utilizar para cada tipo de dato, como también las posibles restricciones sobre quién tiene permiso para utilizar los canales, es decir, define qué actividades están prohibidas.

Los usuarios solamente pueden enviar mensajes que contengan información veraz. Está prohibido enviar materiales perturbadores, desagradables, sexualmente explícitos, groseros, difamatorios o cualquier otro contenido inaceptable o ilegal. Los usuarios no deben enviar mensajes basura a personas con las cuales no se ha establecido relación de negocios o a personas que no solicitaron ese tipo de información.

Si un usuario recibe un correo electrónico basura, debe informarlo al [cargo].

Commented [AES34]: Por ejemplo, mediante bloqueo de la

Commented [AES35]: Por ejemplo, más de dos semanas.

Commented [AES36]: Incluya el nombre de su organización.

Commented [AES37]: Eliminar todo este punto si el control

Commented [AES38]: Se puede especificar el medio en cuestión.

Commented [AES39]: Se pueden especificar los foros y redes

[illegible]

El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la organización utilizando el método especificado por el [cargo].

[illegible]

3.16. Derechos de autor

Los usuarios no deben realizar copias no autorizadas del software que pertenece a la organización, excepto en los casos permitidos por ley, por el propietario o por el [cargo].

[illegible]

3.17. Computación móvil

3.17.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos, sin importar dónde se utilice dicho equipo.

[illegible]

3.17.2. Reglas básicas

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos (incluidos automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- [illegible]
- [illegible]
- [illegible]

Commented [AES40]: Eliminar si no existe esta Política.

Commented [AES41]: Eliminar todo este punto si el control [illegible]

Commented [AES42]: Eliminar este punto si la Política sobre [illegible]

Commented [AES43]: Eliminar todo este punto si el control [illegible]

Commented [AES44]: Eliminar este párrafo si el control A.7.10 [illegible]

Commented [AES45]: Eliminar si el control A.7.9 está marcado [illegible]

Commented [AES46]: Por ejemplo, acceso semanal al servidor [illegible]

Commented [AES47]: Por ejemplo, obligando a instalar la [illegible]

- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad de datos [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina el proceso].
- La conexión a redes de comunicación se realiza [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina este proceso].
- La información que se encuentra en ordenadores portátiles debe estar encriptada [indicar si es obligatorio para todo el disco duro o sólo para archivos sensibles, etc.].
- La protección de datos sensibles debe ser implementada de acuerdo con la [Política de clasificación de la información].
- La persona que utilice equipos informáticos móviles fuera de las instalaciones debe observar las instrucciones del fabricante con respecto a la protección del equipo (por ejemplo, de las condiciones climáticas, exposición a interferencias electromagnéticas, vibraciones físicas, etc.)
- Cuando las personas usan sus propios dispositivos, las reglas adicionales que se deben aplicar se definen en la [Política BYOD].

El [cargo] es el responsable de la formación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

3.18. Tele-trabajo y trabajo desde casa

3.18.1. Introducción

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización, incluido el trabajo desde casa. El tele-trabajo no incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El tele-trabajo debe ser autorizado por [cargo] mediante [especificar el método de autorización].

3.18.2. Normas adicionales para el tele-trabajo

Todas las personas que realicen tele-trabajo deben seguir las reglas de computación móvil definidas en la sección 3.17 de este documento, y las reglas definidas a continuación:

- El lugar físico donde se realiza el tele-trabajo debe estar protegido por [especificar cómo se implementa técnicamente, o hacer referencia a un documento que defina el proceso]
- Como mínimo, las personas que realicen tele-trabajo deben tener [concretar aquí la configuración mínima requerida para el tele-trabajo].
- La prevención del acceso no autorizado por parte de personas que viven o trabajan en el lugar donde se realiza la actividad de tele-trabajo debe implementarse de conformidad con la [Política de control de acceso] y la [Política de escritorio y pantalla limpios].
- La protección de los derechos de propiedad intelectual de la organización, por ejemplo para software o otros materiales que puedan estar protegidos por derechos de propiedad intelectual, debe implementarse de acuerdo con la [Política de clasificación de la información].
- La devolución de datos y equipos en caso de terminación del empleo debe implementarse de acuerdo con la sección 3.7 de esta Política

Commented [AES48]: Por ejemplo, accediendo a la red de la

Commented [AES49]: Por ejemplo, al establecer un canal de

Commented [AES50]: Especifique el tipo de información

Commented [AES51]: Por ejemplo, mediante encriptado de

Commented [AES52]: Si su organización no cuenta con una

Commented [AES53]: Si su organización no tiene una Política

Commented [AES54]: Se eliminará en caso de que no se

Commented [AES55]: Puede utilizar la siguiente formación de

Commented [AES56]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES57]: Eliminar todo este punto si la Política

Commented [AES58]: Eliminar todo este punto si el control

Commented [AES59]: La autorización puede ser concedida de

Commented [AES60]: Ejemplos de elementos a utilizar son:

Commented [AES61]: Por ejemplo, fuente de alimentación

Commented [AES62]: En caso de que la Política de escritorio y

Commented [AES63]: Si su organización no cuenta con una

- Las actividades prohibidas específicas para los empleados que realizan tele-trabajo son: [enumere aquí las actividades específicamente prohibidas para los empleados que realizan tele-trabajo]
- [redacted]

Commented [AES64]: Puede eliminar este texto si no hay [redacted]

Commented [AES65]: Por ejemplo, participar en reuniones con [redacted]

Commented [AES66]: Puede eliminar este texto si no hay [redacted]

Commented [AES67]: Por ejemplo, cambiar configuraciones en [redacted]

3.19. Supervisión del uso de sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación, de la organización, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad de [nombre de la organización].

[redacted]

[redacted]

3.20. Incidentes

Cada empleado, proveedor o tercero que esté en contacto con datos y/o sistemas de [nombre de la organización] debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente, de acuerdo a lo establecido en el Procedimiento para gestión de incidentes.

4. Gestión de registros guardados en base a este documento

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[Autorizaciones para instalación de software, uso de aplicaciones Java y controles Active X, uso de herramientas criptográficas, descarga de códigos de programas desde medios externos, instalación de	[carpeta de Intranet]	[cargo]	Los registros no pueden ser editados, solamente el [cargo] puede guardar estos registros.	Los registros son almacenados por el plazo de 3 años.

Commented [AES68]: Modifique estos registros para que [redacted]

Commented [AES69]: Modificar según sea necesario.

dispositivos periféricos] - formato electrónico				
[Autorizaciones para retirar activos fuera de las instalaciones] - formato electrónico	[carpeta de Intranet]	[cargo]	Los registros no pueden ser editados, solamente el [cargo] puede guardar estos registros.	Los registros son almacenados por el plazo de 3 años.
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Commented [AES70]: Modificar según sea necesario.

Commented [AES71]: Modificar según sea necesario.

Commented [AES72]: Modificar según sea necesario.

Commented [AES73]: Modificar según sea necesario.

Commented [AES74]: Modificar según sea necesario.

Solamente el [cargo] puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

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 [AES75]: 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 uso inadecuado o no autorizado de los activos de información.
- Cantidad de incidentes relacionados con inadecuados programas de formación o de concienciación de empleados sobre el uso aceptable de los activos de información.

[cargo]
[nombre]

[firma]

Commented [AES76]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.