[logo de la organización]

[nombre de la organización]

Commented [27A1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

PROCEDIMIENTOS DE SEGURIDAD PARA EL DEPARTAMENTO DE TI

Commented [27A2]: 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 [27A3]: 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.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
DD-MM-AAAA	0.1	27001Academy	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS 3

2. DOCUMENTOS DE REFERENCIA 3

3. PROCEDIMIENTOS DE SEGURIDAD PARA EL DEPARTAMENTO DE TI 3

3.1. GESTIÓN DE CAMBIOS 3
3.2. COPIAS DE SEGURIDAD 4
3.2.1. Procedimiento para copias de seguridad 4
3.2.2. Prueba de las copias de seguridad 4
3.3. GESTIÓN DE SEGURIDAD DE RED 4
3.4. SERVICIOS DE RED 5
3.5. ELIMINACIÓN Y DESTRUCCIÓN DE EQUIPOS Y SOPORTES 5
3.5.1. Equipos 5
3.5.2. Soportes móviles de almacenaje 5
3.5.3. Soportes en papel 5
3.5.4. Borrado y destrucción de registros; comisión para la destrucción de datos 5
3.6. POLÍTICAS Y PROCEDIMIENTOS PARA 6
3.6.1. Canales de comunicación electrónica 6
3.6.2. Relaciones con entidades externas 6
3.7. SUPERVISIÓN DEL SISTEMA 6

4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO 7

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 8

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

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, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
- Política de seguridad de la información
- [Estrategia de continuidad de negocio]
- [Política sobre dispositivos móviles y tele-trabajo]
- [Política de clasificación de la información]
- [Inventario de activos]
- [Política de seguridad para proveedores]

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. [redacted]
2. [redacted]
3. Los cambios deben ser implementados por [cargo].
4. El [cargo] es el responsable de verificar que los cambios se han implementado de acuerdo al [redacted]
5. El [cargo] es el responsable de probar y verificar la estabilidad del sistema, el sistema no debe ser puesto en producción antes de haber realizado pruebas exhaustivas.
6. La implementación de los cambios debe ser reportada a las siguientes personas: [detalles todos los cargos necesarios]

Los registros sobre los cambios son llevados en [indicar el nombre del formulario o informar un método diferente para registrar los cambios].

Commented [27A4]: Eliminar todo este punto si el control A.12.1.2 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A5]: Eliminar este punto si la Política de gestión de cambio forma parte de un documento aparte.

Commented [27A6]: Para obtener más información sobre este tema, lea este artículo:

How to manage changes in an ISMS according to ISO 27001 A.12.1.2 https://advisera.com/27001academy/blog/2015/09/14/how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/

Commented [27A7]: Se puede especificar qué es y qué no se [redacted]

Commented [27A8]: Otra forma de formular los pasos, puede [redacted]

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

3.2. Copias de seguridad

3.2.1. Procedimiento para copias de seguridad

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

El [cargo] es el responsable de crear copias de seguridad de información, software e imágenes del sistema. Es hacer necesario, detallar qué tecnología se utiliza para crear las copias de seguridad, indicar las responsabilidades sobre las actividades individuales, los [illegible] para almacenar las copias, la protección física que tienen, encriptado, claves, etc.]

Se crean automáticamente registros del proceso de creación de copias de seguridad en los sistemas [illegible].

3.2.2. 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 [describir el servidor en el cual se realiza la recuperación de datos] y la verificación de que todos los datos han sido recuperados satisfactoriamente.

El [cargo] es el responsable de probar las copias de seguridad. Los registros de las pruebas realizadas sobre las copias de seguridad se llevan [indicar el formato del registro (en papel o electrónico), si hay un formulario determinado, etc.].

3.3. 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 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.
- Proteger los datos sensibles que se transmiten por la red pública [describir la tecnología que se utiliza para la protección y especificar las responsabilidades y las personas responsables].
- Proteger los datos sensibles que se transmiten por redes inalámbricas [describir la tecnología que se utiliza para la protección y especificar las responsabilidades y las personas responsables].
- Proteger a los equipos que se conectan a la red desde ubicaciones remotas [describir la tecnología que se utiliza para la protección y especificar las responsabilidades y las personas responsables].
- Separar el tráfico que ingresa por dispositivos móviles, establecer políticas exclusivas de cortafuegos, rutas estáticas, redes virtuales de área local, etc.
- Garantizar la disponibilidad de los servicios en red [describir los controles que asegurarán la disponibilidad].
- El [cargo] debe periódicamente verificar y probar los controles implementados.

Commented [27A9]: Eliminar todo este punto si el control A.12.3.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A10]: Eliminar este punto si la Política para [illegible]

Commented [27A11]: Para obtener más información sobre este tema, lea este artículo:

Backup policy – How to determine backup frequency
https://advisera.com/27001academy/blog/2013/05/07/backup-policy-how-to-determine-backup-frequency/

Commented [27A12]: En caso que no exista este documento, [illegible]

Commented [27A13]: Las copias de seguridad deben ser [illegible]

Commented [27A14]: Adaptar la frecuencia de acuerdo con el riesgo evaluado.

Commented [27A15]: Eliminar todo este punto si el control A.13.1.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A16]: Para obtener más información sobre este tema, lea este artículos:

- How to manage network security according to ISO 27001 A.13.1
https://advisera.com/27001academy/blog/2016/06/27/how-to-manage-network-security-according-to-iso-27001-a-13-1/

- Requirements to implement network segregation according to ISO 27001 control A.13.1.3
https://advisera.com/27001academy/blog/2015/11/02/requirements-to-implement-network-segregation-according-to-iso-27001-control-a-13-1-3/

- Network segregation in cloud environments according to ISO 27017
https://advisera.com/27001academy/blog/2016/09/26/network-segregation-in-cloud-environments-according-to-iso-27017/

- Using Intrusion Detection Systems and Honeypots to comply with ISO 27001 A.13.1.1 network controls
https://advisera.com/27001academy/blog/2016/07/04/using-intrusion-detection-systems-and-honeypots-to-comply-with-iso-27001-a-13-1-1-network-controls/

- How to use firewalls in ISO 27001 and ISO 27002 implementation
https://advisera.com/27001academy/blog/2015/05/25/how-to-use-firewalls-in-iso-27001-and-iso-27002-implementation/

Commented [27A17]: O hacer referencia a la Política sobre dispositivos móviles y tele-trabajo.

Commented [27A18]: Se puede especificar la frecuencia; por ej., diariamente o en algunos días del mes, etc.

Commented [27A19]: Se pueden especificar los controles; por ej., cortafuegos, sistemas de detección de intrusiones, etc.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

3.4. Servicios de red

El [cargo] debe definir las características de seguridad y el nivel de servicio deseado para todos los

según se define en la [Política de seguridad para proveedores].

3.5. Eliminación y destrucción de equipos y soportes

almacenaje (por ej., ordenadores, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el soporte, antes de ser eliminados o reutilizados.

3.5.1. Equipos

cuenta la sensibilidad de los datos, el proceso no es suficientemente seguro, entonces los soportes de almacenaje deben ser destruidos.

3.5.2. Soportes móviles de almacenaje

El [cargo] es el responsable de borrar datos de los soportes móviles de almacenaje, salvo que la

de almacenaje deben ser destruidos.

3.5.3. Soportes en papel

Los empleados de la organización que manejan documentos individuales son responsables de

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

de borrado o destrucción, método de borrado o destrucción, persona que realizó el proceso.

Commented [27A20]: Para obtener más información sobre este tema, lea este artículo:

How to manage the security of network services according to ISO 27001 A.13.1.2
https://advisera.com/27001academy/blog/2017/02/13/how-to-manage-the-security-of-network-services-according-to-iso-27001-a-13-1-2/

Commented [27A21]: Eliminar todo este punto si los controles A.8.3.2 y A.11.2.7 están marcado como no aplicables en la Declaración de aplicabilidad.

Commented [27A22]: Eliminar este punto si la Política de eliminación y destrucción forma parte de un documento aparte.

Commented [27A23]: Para obtener más información sobre este tema, lea este artículo:

Secure equipment and media disposal according to ISO 27001
https://advisera.com/27001academy/blog/2015/12/07/secure-equipmentand-media-disposal-according-to-iso-27001/

Commented [27A24]: Es posible aclarar que esto significa

Commented [27A25]:

Commented [27A26]: Eliminar este punto si el control A.8.1.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A27]: Eliminar si no existe esta Política.

Commented [27A28]: Por ej., enumerar herramientas

Commented [27A29]: Esto puede ser, por ejemplo, un disco duro de un servidor.

Commented [27A30]: Eliminar si no existe esta Política.

Commented [27A31]: Eliminar si no existe esta Política.

Commented [27A32]: O especificar alguna otra tecnología.

Commented [27A33]: Adaptar a los niveles de confidencialidad que se utilizan en la organización.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

Toda la información clasificada como "Confidencial" debe ser borrada o destruida ante la presencia de una persona [illegible] a dicha información.

3.6. Políticas y procedimientos para

3.6.1. 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 datos por medio de [illegible] los sistemas de comunicación especializados), teléfonos, equipos de fax, mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

El [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 están 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.

3.6.2. 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.

Antes de intercambiar información y/o software con cualquier entidad externa, se debe firmar un contrato, el cual es responsabilidad del [cargo]. 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].

3.7. 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 administradores y operadores de sistema sobre sistemas sensibles.

Commented [27A34]: Eliminar este punto si la Política de transferencia de información forma parte de un documento aparte.

Commented [27A35]: Eliminar todo este punto si el control A.13.2.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A36]: Se puede especificar el soporte en cuestión.

Commented [27A37]: Se pueden especificar los foros y redes sociales en cuestión.

Commented [27A38]: Agregar o eliminar canales de

Commented [27A39]: Este texto puede ser reemplazado

Commented [27A40]: Eliminar si no existe esta Política.

Commented [27A41]: Eliminar todo este punto si el control A.13.2.2 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A42]: Para obtener más información sobre este tema, lea este artículo:

Logging and monitoring according to ISO 27001 A.12.4
https://advisera.com/27001academy/blog/2015/11/23/logging-and-monitoring-according-to-iso-27001-a-12-4/

Commented [27A43]: Entre los registros se pueden incluir

Commented [27A44]: Eliminar este texto si el control A.12.4.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Commented [27A45]: Eliminar este texto si el control A.12.4.3 está marcado como no aplicable en la Declaración de aplicabilidad.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

El [cargo] es el responsable de supervisar diariamente los registros de los fallos informados en forma [illegible] registros sobre los errores.]

[illegible] la revisión.

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
[Decisiones sobre los canales de comunicación utilizados para tipos específicos de información, restricciones, actividades prohibidas] - formato electrónico	[Nombre de carpeta de Intranet]	[cargo]	Una vez creado, el registro ya no puede ser modificado.	3 años
[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.
[Registros de las pruebas realizadas sobre las copias de seguridad] - en papel o formato electrónico	[nombre de la carpeta de archivo o gabinete]	[cargo]	Solamente el [cargo] tiene el derecho para acceder a estos registros	Los registros son almacenados por el plazo de 1 año.

Commented [27A46]: Eliminar este texto si los controles A.12.4.1 y A.12.4.3 están marcados como no aplicables en la Declaración de aplicabilidad.

Commented [27A47]: Se puede especificar que aquí se [illegible]

Commented [27A48]: Si fuera necesario, esto se puede [illegible]

Commented [27A49]: Eliminar este texto si los controles A.12.4.1 y A.12.4.3 están marcados como no aplicables en la Declaración de aplicabilidad.

Commented [27A50]: Modifique estos registros para que coincidan con lo que ya tiene en su empresa. Si no tiene registros similares, puede crear nuevos en el formato que más le convenga.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

[Características de seguridad y nivel de servicio deseado para servicios en red] - formato electrónico o papel	Ordenador del [cargo], [nombre de la carpeta de archivo o gabinete]	[cargo]	Solamente el [cargo] tiene el derecho para acceder a estos registros	5 años luego del vencimiento del acuerdo o del servicio prestado
[Borrado o destrucción de registros] - en papel	[nombre de la carpeta de archivo o gabinete]	[cargo]	El gabinete tiene cerradura, las llaves están en custodia de [cargos]	Los registros son almacenados por el plazo de 5 años.
[Evidencia de revisión de registros] - en formato electrónico y papel	Ordenador del [cargo], [nombre de la carpeta de archivo o gabinete]	[cargo]	Solamente el [cargo] tiene el derecho para acceder a estos registros	Los registros son almacenados por el plazo de 5 años.

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 [27A51]: Esto es sólo una recomendación; ajustar la frecuencia según sea necesario.

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

- [illegible]
- [illegible]

[cargo]
[nombre]

_____
[firma]

Commented [27A52]: Sólo es necesario si el Procedimiento para control de documentos y registros establece que los documentos en papel deben ser firmados.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.