[logo de la organización]

[nombre de la organización]

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

POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Commented [AES2]: Para aprender a seleccionar cláusulas de seguridad, lea estos artículos:

- 6-step process for handling supplier security according to ISO 27001 https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/
- Which security clauses to use for supplier agreements? https://advisera.com/27001academy/blog/2017/06/19/which-security-clauses-to-use-for-supplier-agreements/

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 de este documento es definir las reglas básicas para las relaciones con proveedores y socios, incluidos los proveedores de servicios en la nube.

Este documento se aplica a todos los proveedores y socios que puedan tener influencia sobre la confidencialidad, integridad y disponibilidad de información sensible de [nombre de la organización].

Los usuarios de este documento son la alta dirección y las personas responsables de proveedores y socios en [nombre de la organización].

Commented [AES4]: Esta Política de alto nivel está escrita de acuerdo con ISO 27001, Anexo A, control A.5.19, que define los requisitos para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización, y no describe las prácticas detalladas que se deben seguir.

Si su organización desea definir las prácticas detalladas que deben seguir los proveedores, consulte como ejemplo el documento Política de seguridad de TI. Puede encontrar una plantilla para este documento en la carpeta del Paquete de Documentos sobre ISO 27001 "09_Anexo_A_Controles_de_seguridad".

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

Commented [AES6]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.7, A.5.11, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.6.1, A.6.2, A.6.3 y A.8.30
- Metodología de evaluación y tratamiento de riesgos
- Informe sobre la evaluación y tratamiento de riesgos
- Política de control de acceso
- Declaración de confidencialidad

Commented [AES7]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "06_Evaluacion_y_tratamiento_de_riesgos".

Commented [AES8]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "06_Evaluacion_y_tratamiento_de_riesgos".

3. Relación con proveedores y socios

3.1. Identificación de riesgos

Commented [AES9]: Borrar esta sección si el control A.5.19 se

Los riesgos de seguridad relacionados con proveedores y socios, incluidos los proveedores de servicios en la nube, se identifican durante el proceso de evaluación de riesgos, según se define en la Metodología de evaluación y tratamiento de riesgos.

3.2. Selección

Commented [AES10]: Borrar esta sección si el control A.6.1 se

El [cargo] decide si es necesario realizar verificaciones de antecedentes de determinados proveedores y socios y, en caso que sea necesario, determinará los métodos que deben aplicarse.

Commented [AES11]: Por ejemplo, experiencia de otros

3.3. Contratos

Commented [AES12]: Borrar esta sección si el control A.5.20 se

El [cargo] es responsable de decidir qué cláusulas de seguridad se incluirán en el contrato con un proveedor o socio. Esta decisión debe estar basada en los resultados de la evaluación y tratamiento de riesgos.

- Mantener la confidencialidad de la información.
- Devolución de los bienes después de la terminación del contrato.
- Cómo se comunica la información sobre amenazas entre el proveedor y el comprador.
- Garantizar una entrega confiable de los productos y servicios, lo cual es particularmente importante con los proveedores de servicios en la nube.

En el documento Cláusulas de seguridad para proveedores y socios se incluye una lista de cláusulas sugeridas.

El [cargo] decidirá si los empleados del proveedor o socio deberán firmar las Declaraciones de confidencialidad cuando trabajen para [nombre de la organización].

El [cargo] decide quién será el propietario de cada contrato; es decir, quién será responsable de un determinado proveedor o socio.

3.4. Formación y concienciación

El propietario del contrato decide qué empleados del proveedor o socio necesita formación y concienciación sobre seguridad.

El [cargo] es responsable de suministrar toda la formación y de realizar la concienciación a esos empleados.

3.5. Supervisión y revisión

El propietario del contrato debe supervisar y controlar periódicamente el nivel de los servicios y cumplimiento de las cláusulas de seguridad de parte de los proveedores o socios y los informes y registros generados por ellos, como también deben realizarles una auditoría de un proveedor o socio al menos una vez al año.

Todos los incidentes de seguridad relacionados con el trabajo del proveedor o socio deben ser elevados inmediatamente al [cargo].

3.6. Cambios o finalización de servicios del proveedor

El propietario del contrato propone cambios o la finalización del contrato y el [cargo] toma la decisión final. Si es necesario, el [cargo] realizará una nueva evaluación de riesgos antes de aceptar los cambios.

3.7. Eliminación de derecho de acceso y devolución de activos

Cuando se modifica o finaliza un contrato, se deben eliminar los derechos de acceso para los empleados del proveedor o socio de acuerdo a la Política de control de acceso.

Además, cuando se cambia o finaliza un contrato, el propietario del contrato debe asegurarse de que todo el equipamiento, software o información en formato electrónico o papel sea devuelto.

Commented [AES13]: Incluya el nombre de su organización.

Commented [AES14]: Borrar esta sección si el control A.6.3 se

Commented [AES15]: Puede sugerir esta formación al

Commented [AES16]: Borrar esta sección si el control A.5.22 se

Commented [AES17]: Si fuera necesario, se pueden

Commented [AES18]: Las auditorías presenciales deben ser

Commented [AES19]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES20]: Adaptar según sea necesario; por ej., en

Commented [AES21]: Generalmente es el gerente de

Commented [AES22]: Borrar esta sección si el control A.5.22 se

Commented [AES23]: Borrar esta sección si el control A.5.18 se

Commented [AES24]: Borrar esta sección si el control A.5.11 se

4. Gestión de registros guardados en base a este documento

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Contratos con proveedores y socios	[gabinete, caja fuerte o similar]	[cargo]	Solamente el [cargo] tiene acceso al [gabinete, caja fuerte].	5 años luego de la finalización del contrato.
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [AES25]: Modifique estos registros para que [illegible]

Commented [AES26]: Adaptar este período en función de sus [illegible]

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[illegible]

Commented [AES27]: Esto es sólo una recomendación; ajustar [illegible]

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

- Cantidad e importancia de incidentes que surgen por actividades de proveedores y socios.
- [illegible]

[cargo]
[nombre]

[firma]

Commented [AES28]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.