POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Versión 1.0
7. Apoyo

Código:	POL-07/008/V1.0_Política de seguridad para proveedores
Versión:	1.0
Fecha de emisión:	2025
Creador por:	Depto. Seguridad de la Información
Responsable:	Coordinación del SGSI
Revisión	Anual o ante cambios regulatorios
Nivel de Confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28-may-25	1.0	Coordinación del SGSI	Creación de documento

Tabla de contenido

1. Objetivo, alcance y usuarios 3

2. Documentos de referencia 3

3. Relación con clientes y socios 3

3.1. Identificación de riesgos 3

3.2. Selección 3

3.3. Contratos 3

3.4. Capacitación y concienciación 4

3.5. Supervisión y revisión 4

3.6. Cambios o finalización de servicios del proveedor 4

3.7. Eliminación de derecho de acceso y devolución de activos 4

4. Gestión de registros guardados en base a este documento 5

5. Validez y gestión de documentos 5

6. Apéndices 5

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas para la relación con proveedores y socios.

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

Los usuarios de este documento son la alta dirección y las personas responsables de proveedores y socios en EthicsGlobal.

2. Documentos de referencia

• Norma ISO/IEC 27001, capítulos A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
• Metodología de evaluación y tratamiento de riesgos
• Informe de evaluación y tratamiento de riesgos
• Política de control de acceso
• Declaración de confidencialidad

3. Relación con clientes y socios

3.1. Identificación de riesgos

Los riesgos de seguridad relacionados con proveedores y socios se identifican durante el proceso de evaluación de riesgos, según se define en la Metodología de evaluación y tratamiento de riesgos.
Durante la evaluación de riesgos, se debe tener especial cuidado para identificar riesgos relacionados con tecnología de la información y comunicación, como también riesgos relacionados con la cadena de suministro de productos.

El Coordinador del SGSI decide si también es necesario evaluar los riesgos relacionados con proveedores y socios específicos.

3.2. Selección

El Coordinador del SGSI 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.

3.3. Contratos

El Coordinador del SGSI es responsable de decidir qué cláusulas de seguridad se incluirán en el contrato con el proveedor o socio. Esta decisión debe estar basada en los resultados de la evaluación y tratamiento de riesgos; sin embargo, las cláusulas que establecen la confidencialidad y la devolución de activos una vez finalizado el acuerdo son obligatorias. Además, los contratos deben

garantizar la entrega confiable de productos y servicios, que es sumamente importante con proveedor de servicios de la nube.

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

El Coordinador del SGSI decidirá si los empleados del proveedor o socio deberán firmar las declaraciones de confidencialidad cuando trabajen para EthicsGlobal.

El Coordinador del SGSI decide quién será el propietario de cada contrato; es decir, quién será responsable de un determinado proveedor o socio.

3.4. Capacitación y concienciación

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

El Coordinador del SGSI es responsable de suministrar toda la capacitación y de realizar la concienciación a esos empleados.

3.5. Supervisión y revisión

El propietario del contrato debe revisar 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.

Todos los incidentes de seguridad relacionados con el trabajo del proveedor o socio deben ser elevados inmediatamente al Coordinador del SGSI.

3.6. Cambios o finalización de servicios del proveedor

El propietario del contrato propone cambios o la finalización del contrato y el Coordinador del SGSI toma la decisión final. Si es necesario, el Coordinador del SGSI 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.

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 del contrato
Contratos con proveedores y socios	Gabinetes de gerencia administrativa	Gerente de administración	Solamente el gerente de administración tiene acceso a los gabinetes	5 años luego de la finalización del contrato.

5. Validez y gestión de documentos

Esta política será revisada anualmente por el Comité de Seguridad de la Información o, cuando ocurra un cambio significativo en los roles organizacionales.

El propietario de este documento es el Coordinador del SGSI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

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.
- Cantidad de contratos en los que no está definido el propietario del contrato.

6. Apéndices

- Cláusulas de seguridad para proveedores y socios

Representante de la Dirección General
Liuva Anahí Figueroa Gracián

_____