POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN PROVEEDORES

Elaborado por: Carlos Torres	**Revisado por:** Jesus Medina	**Aprobado por:** Rafael Carvajal
Senior Developer / Cybersecurity	Vice President of Finance	CEO

1. Introducción

Esta política establece las directrices y principios que regulan la gestión de la seguridad de la información en colaboración con nuestros proveedores.

Reconocemos que la seguridad de nuestros datos no solo depende de nuestras prácticas internas, sino también de la forma en que nuestros proveedores manejan y protegen la información.

El objetivo de esta política es garantizar que todos los proveedores cumplan con los estándares adecuados de seguridad, protegiendo así la confidencialidad, integridad y disponibilidad de la información que compartimos. La implementación efectiva de estas medidas es vital para mitigar riesgos, proteger nuestros activos de información y mantener la confianza de nuestros clientes y socios comerciales.

2. Objetivo

El objetivo de la Política Global de Seguridad de la Información para Proveedores tiene como fin establecer un marco claro y coherente que garantice la protección de la información sensible y crítica durante la interacción con estos.

Esta política busca:

1. **Proteger la Información**: Asegurar la confidencialidad, integridad y disponibilidad de la información compartida con los proveedores, minimizando los riesgos de brechas de seguridad.

2. **Establecer Normativas Comunes**: Definir estándares y requisitos de seguridad que todos los proveedores deben cumplir, promoviendo un enfoque uniforme hacia la gestión de la seguridad de la información.

3. **Mitigar Riesgos**: Identificar, evaluar y gestionar los riesgos asociados con el acceso y uso de la información por parte de los proveedores, estableciendo controles adecuados para prevenir incidentes de seguridad.

4. **Fomentar la Colaboración**: Promover una cultura de seguridad compartida entre la organización y sus proveedores, promoviendo la capacitación y el intercambio de mejores prácticas en materia de seguridad.

5. **Cumplir con la Normativa**: Asegurar el cumplimiento de las leyes, regulaciones y estándares aplicables en materia de protección de datos y seguridad de la información.

3. Alcance

Este documento establece el alcance de la Política Global de Seguridad de la Información para Proveedores, definiendo los lineamientos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información gestionada por proveedores externos.

Incluye, pero no se limita a:

- Datos personales identificables.
- Información financiera.
- Propiedad intelectual.
- Datos comerciales confidenciales.
- Cualquier otra información clasificada como sensible por la organización.
- Cumplimiento de:

    - Declaración de Derechos Digitales de Florida» (FLDBOR), la cual establece disposiciones generales para la protección de datos personales, Se centra en la protección de los consumidores y establece derechos como:
        - Derecho a confirmar si una empresa está procesando sus datos personales.
        - Derecho a corregir datos inexactos.
        - Derecho a eliminar sus datos personales.
        - Derecho a la portabilidad de los datos.

    - Ley de Protección de la Información de Florida (FIPA): rige la notificación de violaciones de datos para entidades gubernamentales y sus socio y terceros contratados por ellas
        - Si ocurre una filtración de datos, la entidad debe notificar a las personas afectadas dentro de los 30 días posteriores a su descubrimiento.

4. Principios de Seguridad de la Información

Confidencialidad

La información sensible gestionada por proveedores debe ser accesible únicamente a personas autorizadas. Los proveedores deben implementar controles de acceso robustos y asegurarse de que la transmisión y

almacenamiento de datos cumplan con los requisitos de confidencialidad establecidos, en consonancia con la Declaración de Derechos Digitales de Florida» (FLDBOR) y Ley de Protección de la Información de Florida (FIPA)

Integridad

La integridad de la información debe ser garantizada para mantener su exactitud y completitud. Los proveedores deben establecer medidas que detecten y prevengan alteraciones no autorizadas, asegurando que los datos de los consumidores se gestionen de manera fiable y precisa.

Disponibilidad

La información debe estar disponible cuando sea necesario para las operaciones comerciales legítimas. Los proveedores deben contar con planes de continuidad del negocio y recuperación ante desastres para asegurar la disponibilidad continua de la información y los sistemas críticos

Responsabilidad

Los proveedores son responsables de la gestión adecuada de la seguridad de la información y deben designar a un responsable de seguridad que supervise el cumplimiento de estos principios. Este responsable deberá asegurarse de que se realicen auditorías y evaluaciones de riesgo regularmente.

Capacitación y Concientización

Los proveedores deben implementar programas de capacitación en materia de seguridad de la información para todos sus empleados y colaboradores. Esto incluye formación sobre Declaración de Derechos Digitales de Florida» (FLDBOR) y Ley de Protección de la Información de Florida (FIPA).

Gestión de Incidentes

Los proveedores deben establecer procesos claros para la identificación, notificación y gestión de incidentes de seguridad. Esto incluye la obligación de reportar cualquier incidente que pueda comprometer la confidencialidad, integridad o disponibilidad de la información y, en particular, aquellos que afecten los derechos de los consumidores.

5. Requisitos de Seguridad de la Información para Proveedores

Los proveedores deben:

Evaluación de Riesgos

- **Realizar Evaluaciones**: Los proveedores deben llevar a cabo evaluaciones de riesgo periódicas para identificar y mitigar riesgos potenciales asociados con el manejo de información sensible.
- **Informes Periódicos**: Presentar informes sobre la evaluación de riesgos y las medidas correctivas adoptadas.

Control de Acceso

- **Autenticación**: Implementar mecanismos de autenticación robustos que incluyan el uso de contraseñas seguras y autenticación multifactor cuando sea posible.
- **Permisos Basados en Roles**: Asegurar que el acceso a la información se limite a los empleados que necesiten acceder a esos datos para cumplir con sus funciones laborales.

Protección de Datos

- **Cifrado**: Utilizar cifrado para la transmisión y almacenamiento de datos sensibles, cumpliendo con los estándares de la industria.
- **Clasificación de Datos**: Clasificar la información según su sensibilidad y aplicar controles acordes en función de esta clasificación.

Acuerdos de Confidencialidad

- **Firmar Acuerdos**: Todos los proveedores deben firmar acuerdos de confidencialidad que detallen sus responsabilidades en la protección de la información de la organización y de sus consumidores.

6. Evaluación y Auditoría

CIMA 360 se reserva el derecho de realizar auditorías y evaluaciones de seguridad de la información en cualquier momento para verificar el cumplimiento por parte de los proveedores. Los proveedores deben cooperar plenamente en estas auditorías y proporcionar acceso a la información y recursos necesarios.

7. Cumplimiento y Sanciones

El incumplimiento de esta política puede resultar en la rescisión del contrato, acciones legales u otras sanciones según lo estipulado en los acuerdos contractuales y las leyes aplicables.

8. Revisión y Actualización

Esta política será revisada periódicamente para asegurar su relevancia y eficacia frente a los cambios en el entorno operativo y las amenazas emergentes.

9. Aprobación

Esta política de seguridad de la información para proveedores ha sido aprobada por la alta dirección y entrará en vigor a partir de la fecha de su publicación.

10. Comunicación

Esta política es comunicada a todos los proveedores actuales y se incluye como parte integral de los nuevos contratos y acuerdos con proveedores externos.

11. Control de cambios

Versión	Fecha de aprobación (DD/MM/AAAA)	Descripción del cambio
0	01/07/2025	Aprobación, estandarización y publicación de la política Global de Seguridad de la Información Proveedores
1	06/01/2026	Revisión, cambio razón social