Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

Política de seguridad de la información en las relaciones con los proveedores.

1. Introducción.

En un entorno empresarial cada vez más digitalizado y globalizado, la seguridad de la información y la ciberseguridad se han convertido en pilares fundamentales para proteger los activos, datos y la reputación de las organizaciones. Como empresa partner premier de AWS con una amplia presencia en Latinoamérica, tenemos la responsabilidad de asegurar que tanto nuestra infraestructura como la de nuestros proveedores estén alineadas con los más altos estándares de seguridad.

Reconocemos que los proveedores desempeñan un papel crucial en nuestra cadena de suministro y, por ende, en la protección de la información sensible. Por ello, es imperativo establecer políticas claras que garanticen un enfoque integral hacia la ciberseguridad, no solo para mitigar riesgos, sino también para fomentar una cultura de seguridad compartida entre todas las partes involucradas.

Estas políticas están diseñadas para proporcionar un marco que asegure el cumplimiento de las normativas vigentes y el manejo responsable de la información, estableciendo expectativas claras para todos los proveedores que colaboran con nuestra organización. A través de la implementación de estas políticas, buscamos fortalecer nuestra postura de seguridad y asegurar la confianza de nuestros clientes en la protección de sus datos.

La presente política se aplica de forma coordinada e integrada con la Política de Cancelación y Retención de Datos Personales, el Procedimiento de evaluación de proveedores y los Contratos de Encargo del Tratamiento (DPA), con el fin de garantizar un marco documental homogéneo, coherente y alineado con el RGPD para la gestión de terceros.

2. Objetivo.

Establecer un marco de seguridad que garantice la protección de la información y los sistemas de Escala 24x7 y de sus clientes, asegurando que todos los proveedores cumplan con estándares adecuados de ciberseguridad.

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.

Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

3. Alcance.

Estas políticas son aplicables a todos los proveedores y terceros que suministran, desarrollan, integran, gestionan, almacenan o procesan información y/o componentes tecnológicos para Escala 24x7, así como los que acceden, transmiten, procesan o gestionan en cualquier momento información física o electrónica que es propiedad de Escala 24x7.

A efectos de la presente política se establece una diferenciación expresa entre aquellos proveedores que únicamente prestan servicios tecnológicos sin acceso a datos personales, y aquellos proveedores que actúan como Encargados del Tratamiento por tener acceso y gestionar datos personales por cuenta de Escala 24x7. A estos últimos se les aplicarán los requisitos adicionales y específicos previstos en la normativa de privacidad aplicable. .

4. Propiedad de la Información.

La información que Escala 24x7 revele, dé a conocer, entregue o confíe al proveedor durante la ejecución o con ocasión de los servicios contratados, es propiedad de Escala 24x7 y debe ser tratada y protegida por el proveedor en los términos previstos en el contrato correspondiente, el Acuerdo de Confidencialidad suscrito entre las Partes y el presente documento.

5. Cumplimiento Normativo y/o Estándares de seguridad.

Los proveedores deben contar con estándares de seguridad, con mejores prácticas de seguridad de la información y ciberseguridad, cumplir con las leyes y regulaciones locales e internacionales relacionadas con la protección de datos y la seguridad de la información, en la medida de lo posible disponer de certificaciones como:

- Leyes de protección de datos personales (ej. GDPR).
- Normas ISO 27001/27002.
- Regulaciones de la industria (ej. PCI DSS, HIPAA).
- Informes de controles tipo SOC1, SOC2, SOC3.

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.

Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

6. Control de Acceso.

- Cumplir con las políticas de control de acceso, políticas de password, garantizar autenticación segura con un segundo factor de autenticación (MFA).
- Implementar controles de acceso estrictos basados en el principio de menor privilegio, accesos basados en roles o funciones, segregación de funciones.
- El proveedor debe respetar los controles para mitigar los riesgos del acceso remoto orientados a mitigar la exposición potencial derivada del uso no autorizado.
- Todos los accesos deben ser autenticados y autorizados adecuadamente.
- Monitoreo y revisión periódica de los accesos.

7. Seguridad de la Información

- Realizar evaluaciones de riesgo anuales para identificar y mitigar vulnerabilidades.
- Implementar cifrado de datos en tránsito y en reposo.
- Establecer políticas de gestión de incidentes de seguridad.
- Contar con procedimiento de Controles de Cambio.

8. Concienciación y Capacitación

- Proveer capacitación regular a todos los empleados sobre prácticas de seguridad cibernética.
- Sensibilizar sobre las amenazas comunes (phishing, malware, etc.) y cómo mitigarlas.

9. Gestión de Proveedores

- Evaluar la ciberseguridad y el nivel de protección de datos de los proveedores. Esta evaluación debe verificar específicamente:
    - Existencia de políticas de privacidad documentadas.
    - Cumplimiento del RGPD u otra normativa aplicable.
    - Ubicación geográfica donde se realizará el tratamiento de los datos.
    - Identificación de subencargados utilizados por el proveedor.
    - Certificaciones o evidencias relacionadas con la protección de datos.
- Incluir cláusulas de ciberseguridad en todos los contratos con proveedores.
- Monitorear el desempeño de los proveedores en relación con la seguridad de la información.

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.

Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

- Formalizar un Contrato de Encargo del Tratamiento (Data Processing Agreement - DPA) en todos los casos donde el proveedor trate datos personales por cuenta de Escala 24x7.
- Garantizar que los subproveedores o subencargados utilizados por los proveedores principales ofrezcan garantías de seguridad y privacidad equivalentes a las exigidas por Escala 24x7. Su utilización deberá respetar estrictamente las condiciones de autorización y notificación establecidas en los Contratos de Encargo del Tratamiento (DPA) aplicables.

10. Seguridad Física.

- Proteger las instalaciones donde se manejan datos sensibles, asegurando el acceso controlado.
- Implementar medidas de seguridad física como cámaras, guardias y controles de acceso.

11. Gestión de activos de información y tecnológicos.

El proveedor debe disponer, mantener y gestionar los activos tecnológicos y de información durante todo su ciclo de vida y en el uso, tránsito y reposo.
Se debe mantener un inventario, clasificación y etiquetado de los activos tecnológicos y de información según el nivel de criticidad, y realizar revisiones periódicas para garantizar que el inventario está actualizado.

12. Prevención de fuga de información y/o pérdida de datos.

El proveedor debe asegurar que los activos de información y/o datos de Escala 24x7 bajo su custodia estén protegidos a través de una combinación de técnicas de cifrado, medios seguros para el acceso a los datos, protección de la integridad y técnicas y controles de prevención de la fuga de información. Se debe limitar el acceso a los activos de información/datos de Escala 24x7.

13. Detección de denegación de servicio.

El proveedor debe disponer de capacidades de detección y protección frente a los ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS). Se asegurará de que los canales externos o conectados a internet que se empleen para prestar servicios a Escala 24x7 cuenten con una adecuada protección contra este tipo de ataques, a fin de garantizar la disponibilidad.

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.

Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

14. Protección de Datos.

- Desarrollar y mantener políticas de privacidad y protección de datos.
- Establecer procedimientos para la gestión de datos sensibles y su eliminación segura.
- Asegurar que cualquier transferencia internacional de datos personales realizada por un proveedor únicamente se ejecute cuando exista una base jurídica. Esto implica verificar previamente la existencia de una decisión de adecuación, la firma de Cláusulas Contractuales Tipo u otras garantías legalmente previstas y aprobadas, para lo cual se deberá obtener visto bueno del equipo de Compliance y del equipo Legal.
- Garantizar que, una vez finalizada la prestación del servicio o la relación contractual, el proveedor proceda a devolver o eliminar de forma segura y definitiva toda la información y los datos personales tratados por cuenta de Escala 24x7, salvo en aquellos casos en los que exista una obligación legal que exija su conservación.

15. Respaldo y Recuperación.

- Implementar procedimientos de respaldo regular de datos críticos.
- Desarrollar un plan de continuidad del negocio y recuperación ante desastres.

16. Auditoría y Monitoreo.

- El proveedor debe recopilar, gestionar y analizar los registros de auditoría de eventos que puedan ayudar a supervisar, detectar, comprender y recuperarse de un ataque, donde los sistemas, componentes tecnológicos y procesos clave de su compañía usados para prestar servicios a Escala 24x7.
- Realizar auditorías de seguridad periódicas para evaluar el cumplimiento de estas políticas.
- Monitorear continuamente los sistemas para detectar actividades sospechosas.
- Contar con un histórico de eventos de seguridad que permita comprender, analizar y mejorar las estrategias de seguridad.
- Conservar evidencias documentales que acrediten el cumplimiento de los requisitos establecidos en esta política (principio de responsabilidad proactiva). Esto incluye mantener un registro accesible de auditorías, certificaciones de terceros, revisiones de seguridad, evaluaciones de proveedores y toda la documentación contractual relacionada (como los DPA).

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.

Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

17. Seguridad en las aplicaciones.

Si el proveedor desarrolla aplicaciones para uso de Escala 24x7, o que se utilicen para respaldar el servicio prestado a Escala 24x7, deberá disponer de un marco de desarrollo seguro para prevenir afectaciones relacionadas con la seguridad e identificar y corregir las vulnerabilidades en el código durante el proceso de desarrollo.
Para el desarrollo de aplicaciones se debe hacer uso de estándares y entornos de desarrollo seguros, apropiados al lenguaje de programación, alineados con las recomendaciones de estándares como el OWASP Top Ten, o equivalente.

18. Gestión de Vulnerabilidades

El proveedor debe disponer de políticas, procesos y controles implementados para la supervisión efectiva, la detección y la remediación de vulnerabilidades de sus aplicaciones o las aplicaciones administradas que sean propiedad de Escala 24x7, infraestructura, y componentes tecnológicos.

19. Gestión de incidentes de ciberseguridad

El proveedor debe disponer y operar un marco para la gestión de eventos e incidentes de ciberseguridad y seguridad de la información que valide, remita, contenga y repare efectivamente los incidentes de seguridad del entorno del proveedor y que contenga fases de detección, investigación y reacción ante la ocurrencia de estos.
Así mismo se deben disponer de planes escritos y probados de respuesta a los incidentes, adaptados a diferentes categorías de incidentes conocidos.

20. Reporte de Incidentes.

- Establecer un proceso claro para la notificación de incidentes de seguridad.
- Los proveedores deben notificar a la empresa a la mayor brevedad y a todo evento dentro de las 24 horas de detectar un incidente. Para dar cumplimiento a los estándares mundiales en materia de privacidad y protección de datos personales, dicha notificación deberá incluir, como mínimo, la siguiente información:
    - La naturaleza del incidente de seguridad.
    - Las categorías de datos personales afectadas.
    - El volumen aproximado de interesados (personas) afectados.
    - Las posibles consecuencias derivadas de la brecha.
    - Las medidas correctoras adoptadas o previstas por el proveedor para mitigar los daños

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.

Docusign Envelope ID: 0AA10ECC-993F-891A-83C6-F7214730F1B6

21. Revisión de Políticas

- Estas políticas deben ser revisadas y actualizadas cuando se produzcan cambios significativos en la operación o el entorno legal.

La implementación de estas políticas es fundamental para proteger la información y los activos de Escala 24x7 y sus clientes. Todos los proveedores deben comprometerse a cumplir con estas directrices para garantizar un entorno seguro y resiliente.

Versión 2

Fecha de actualización: Julio 2026

DocuSigned by:
Harold Barber
2C6B784F39ED4EB...

2026 Escala 24x7™ . All rights reserved. Escala 24x7 Confidential Information.