POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN PROVEEDORES

Elaborado por:	**Revisado por:**	**Aprobado por:**
Cargo: Gerente riesgo y control interno Coordinador TI	**Cargo:** Coordinador Control Interno y Calidad	**Cargo:** Gerencia general

ÍNDICE

1. INTRODUCCIÓN

En un entorno de negocios interconectado y global, ATM BPO confía en una red de proveedores, contratistas, consultores y aliados estratégicos (en adelante, "Proveedores") para garantizar la excelencia operativa, la innovación y la continuidad de sus servicios. Al habilitar relaciones, los Proveedores adquieren, procesan, almacenan o transmiten activos de información crítica de la compañía o de sus clientes, o acceden a su infraestructura tecnológica, lo que extiende el perímetro de riesgo de la compañía hacia terceros.

Consciente de que la seguridad de la información es un compromiso compartido, ATM BPO adopta la presente Política Global de Seguridad de la Información para Proveedores. Este documento establece el marco normativo y los estándares mínimos obligatorios que todo tercero debe cumplir durante el ciclo de vida de la relación comercial (selección, contratación, ejecución y finalización), asegurando la confidencialidad, integridad y disponibilidad de los activos digitales, mitigando los riesgos en la cadena de suministro y garantizando el estricto cumplimiento de los requisitos legales, regulatorios y del Sistema de Gestión de Seguridad de la Información (SGSI).

2. OBJETIVO

Establecer los requisitos, lineamientos y controles mínimos de seguridad de la información que deben cumplir de forma obligatoria todos los proveedores, contratistas y terceros que interactúan con los activos de información, Ley de protección de datos personales o infraestructura tecnológica de ATM BPO. Lo anterior tiene como fin mitigar de manera proactiva los riesgos inherentes a la cadena de suministro, garantizar que los terceros mantengan niveles de protección equivalentes a los de la compañía, asegurar el cumplimiento de las obligaciones legales y contractuales, y definir las acciones de supervisión y auditoría durante todo el ciclo de vida de la relación comercial.

3. ALCANCE

De manera específica, los lineamientos de este documento se aplican a cualquier tercero que cumpla con al menos una de las siguientes condiciones:

- Tenga acceso físico o lógico a las instalaciones, redes, sistemas o infraestructura tecnológica de la compañía.
- Almacene, procese, transmita o gestione información de propiedad de la compañía, de sus colaboradores o de sus clientes (incluyendo datos personales, secretos comerciales y propiedad intelectual).

- Desarrolle, administre o soporte aplicaciones, plataformas o herramientas informáticas para uso interno o para los servicios que ATM BPO ofrece al mercado.
- Suministre hardware, software o servicios críticos que impacten directamente la continuidad del negocio o la entrega de servicios de Call Center / BPO de la compañía.

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

    - Ley 1581 de 2012, la cual establece disposiciones generales para la protección de datos personales, garantizando el derecho constitucional a conocer, actualizar y rectificar la información en bases de datos.

    - La Ley 2300 de 2023, también conocida como "Ley dejen de fregar", protege el derecho a la intimidad de los consumidores. Esta ley establece los canales, horarios y frecuencia con los que las empresas pueden contactar a los consumidores.

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 Ley 2300 de 2023 y la protección del derecho a la intimidad de los consumidores, Ley 1581 de 2012 Protección de datos.

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 la Ley 2300 de 2023 y cómo influye en la interacción con los consumidores, promoviendo una cultura de protección de datos y Ley 1581 de 2012 Protección de datos.

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.

1. 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.

2. Evaluación y Auditoría

ATM BPO 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.

3. 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.

4. 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.

5. 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.

6. 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.

5. CONTROL DE CAMBIOS

Versión	Fecha de aprobación (DD/MM/AAAA)	Descripción del cambio
0	27/06/2024	Aprobación de la política Global de Seguridad de la Información Proveedores.
1	20/03/2025	Se revisa, se actualiza el objetivo y el alcance
2	07/06/2026	Se revisa, se alinea el objetivo y alcance a la norma ISO 27001:2022, para su aprobación y publicación en la pagina web : www.atbpo.com/normatividad