atls

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

INFORMACIÓN IMPORTANTE SOBRE ESTE DOCUMENTO	
Identificación del documento	Política de seguridad de la información
Versión	1.0
Responsable principal de su vigilancia	Responsable de Seguridad
Autor	CIO
Órgano de aprobación	Comité de Dirección
Fecha de aprobación	15 de diciembre de 2021

1. Introducción

El Comité de Dirección ha aprobado en su sesión de 15 de diciembre de 2021 la presente Política de seguridad de la información, que establece los principios y directrices con los que ATLS (en adelante la "Compañía") protegerá su información en conformidad con la normativa aplicable, sus valores éticos y cualquier otra normativa interna que resulte aplicable.

La presente Política estará disponible en la intranet para todos los empleados y estará disponible en la web corporativa para todos los grupos de interés de la Compañía. Asimismo, la Política será objeto de las adecuadas acciones de comunicación, formación y sensibilización para su oportuna comprensión y puesta en práctica.

2. Alcance

La presente Política se aplicará a ATLS y vinculará a todos sus empleados, independientemente de la posición y función desempeñada.

ATLS velará por la protección de la información, independientemente de la forma en la que esta se comunique, comparta o almacene. Esta protección se aplica tanto a la información existente dentro de la Compañía como a la información compartida con terceros.

Se entiende por Seguridad de la información a la conservación y protección de:

- Información titularidad de la Compañía, con independencia de que se encuentre en sistemas propios o de terceros.
- Información titularidad de terceros que se encuentre en sistemas de la Compañía.

De conformidad con la Política, ATLS podrá desarrollar procedimientos e instrucciones para implementar y dar cumplimiento a las obligaciones asumidas, así como para adaptarla a las diversas legislaciones locales aplicables al Grupo.

Asimismo, la aplicación de esta Política es complementaria a otras normas internas de obligado cumplimiento, como la Política de cumplimiento en materia de protección de datos personales y privacidad, y aquellas otras que regulen cuestiones relacionadas con la información de la Compañía.

3. Objetivos de seguridad de la información

La presente Política establece el marco de referencia mediante el que ATLS define los principios y reglas básicas de protección de la información gestionada por la Compañía y tiene los siguientes objetivos:

- Comprender y tratar los **riesgos** operacionales y estratégicos en materia de seguridad de la información para que permanezcan en niveles aceptables para la Compañía.
- Asegurar el grado de **confidencialidad** necesario a cada clase de información y prevenir la fuga de información.
- Mantener la **integridad** de la información, evitando que sufra alteraciones respecto al momento en que haya sido generada por los propietarios o responsables de la misma.
- Garantizar la **disponibilidad** de la información, en todos los soportes y siempre que sea necesaria, asegurando la continuidad del negocio y el cumplimiento de las obligaciones que sean exigibles a la Compañía.

4. Principios de seguridad de la información

La presente Política responde a las recomendaciones de las mejores prácticas de seguridad de la información, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la seguridad de la información, puedan afectar a la Compañía.

Adicionalmente, ATLS establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- **Uso de los sistemas de información.** El uso de los sistemas de información estará limitado exclusivamente a la realización de tareas relacionadas con el puesto de trabajo. Estos medios y sistemas no están destinados al uso personal ni podrán ser utilizados para ninguna finalidad ilícita.
- **Seguridad de la información en los sistemas desarrollados.** Los entornos de desarrollo y producción se mantendrán en sistemas independientes. El desarrollo y mantenimiento de los sistemas de información deben considerar la implementación de las especificaciones de seguridad.
- **Segregación de funciones.** Se deberán evitar los riesgos derivados de la ausencia de segregación de funciones y la dependencia unipersonal de funciones críticas para el negocio.
- **Retención de la información**. Se establecerán períodos de retención de la información por categorías, cuando resulte conveniente a las necesidades operativas o de cumplimiento regulatorio.
- **Recursos necesarios.** Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento.
- **Riesgos.** La Compañía afronta la toma de riesgos y tolera aquellos que, en base a la información disponible, son comprensibles, controlados y tratados cuando es necesario.
- **Continuidad.** Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la información crítica para la Compañía en caso de desastre, minimizando el tiempo de indisponibilidad a niveles aceptables.
- **Cumplimiento.** Los sistemas de información y comunicaciones de la Compañía deberán estar permanentemente conformes a las exigencias de la legislación vigente, así como a la normativa interna de desarrollo que resulte de aplicación.
- **Cumplimiento legal.** Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.

5. Responsabilidades

La responsabilidad de la protección de la información y de los sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles organizativos y funcionales de ATLS, cada uno en la medida que le corresponda, como se detalla a continuación:

- Todos los empleados de la Compañía deberán conocer y cumplir la Política, estando obligados a mantener la confidencialidad de la información manejada en su entorno laboral y debiendo comunicar, con carácter de urgencia, las posibles incidencias o problemas de seguridad que se detecten.
- El uso de los sistemas o servicios digitales por parte de los empleados, incluyendo expresamente el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines lícitos y exclusivamente relacionados con las tareas del puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.
- Los contratos con terceros que impliquen el acceso de estos últimos a la información, entre los que se encuentran los de prestación de servicios o contratos de externalización, deberán garantizar que los proveedores, el personal subcontratado o cualquier empresa externa que utilice o acceda a la información conoce y cumple la Política en lo que les sea de aplicación, estando obligados a mantener el secreto profesional y la confidencialidad de la información manejada en su relación con la Compañía.
- El responsable de Seguridad de la información es responsable de implementar esta Política y monitorizar su cumplimiento, así como el de todos los requerimientos derivados de las leyes, normas y buenas prácticas en materia de seguridad de la información que sean de aplicación. Por ello, es responsable de:
    - Implementar una estrategia de seguridad de la información que vele por el cumplimiento de los principios básicos de esta Política.
    - Establecer y revisar los controles correspondientes para asegurar el cumplimiento de esta Política y su normativa de desarrollo.
    - Prevenir, detectar y responder ante cualquier incidente en materia de seguridad de la información y actuar de acuerdo con lo establecido en el Plan de Respuesta ante Incidentes.
    - Impulsar actividades de formación y concienciación en materia de los procesos de seguridad de la información.
    - Establecer un enfoque de mejora continua.
    - Velar por el cumplimiento de la legislación vigente en el ámbito de las competencias que le atribuye la presente Política.
    - Revisar, actualizar y comunicar cualquier cambio que derive en variaciones de esta Política.

6. Control y auditoría

ATLS se reserva expresamente el derecho de adoptar, con proporcionalidad, las medidas de vigilancia y control necesarias para comprobar la correcta utilización de los sistemas que pone a disposición de sus empleados, incluyendo el contenido de las comunicaciones y dispositivos, respetando la legislación vigente y garantizando la dignidad del empleado. La comunicación y aceptación de esta Política surtirá los efectos de notificación previa al trabajador.

La Compañía se someterá a revisiones y controles periódicos, así como a auditorías internas y externas para evaluar el cumplimiento general de esta Política.

7. Revisión de la Política

La aprobación de esta Política implica que su implantación contará con el apoyo del Comité de Dirección para lograr todos los objetivos establecidos en ella, así como para cumplir con todos sus requisitos.

La presente Política de seguridad de la información será revisada y actualizada cuando proceda, a fin de adaptarla a los cambios que puedan surgir, ya sean estos de tipo operativo, legal, regulatorio o contractual, asegurando así que la Política permanece adaptada en todo momento a la realidad de la Compañía.