Empowering the cloud

Política de Sistema de Gestión

Security & Compliance

V 8.0 Noviembre 2025

1. Objeto y finalidad

La presente Política del Sistema de Gestión y de Seguridad de la Información tiene por objeto integrar las políticas relativas a los Sistemas de Gestión de la Seguridad de la Información, de Calidad y de gestión de Servicios IT y establecer las directrices y principios generales que rigen cómo EVOLUTIO gestiona y protege la información que trata y los servicios que presta, en alineamiento explícito con el Esquema Nacional de Seguridad (ENS) regulado por el Real Decreto 311/2022, de 3 de mayo.

Esta política emana desde la Dirección hacia el resto de la organización para garantizar y promover la excelencia de la seguridad y la calidad de los servicios que se ofrecen en EVOLUTIO de forma plena e integral.

Esta política da cumplimiento a la medida [org.1] sobre Política de seguridad del marco organizativo definido en el Anexo II del Real Decreto 311/2022 relativo a ENS.

Su finalidad es:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tramitada por EVOLUTIO que se cubren en todos los procesos de negocio.
- Permitir la gestión de los servicios acordados y ofrecer estándares de Calidad con los clientes de forma eficaz y eficiente, dentro de un ciclo de vida que permita la mejora continua de los procesos implantados, asegurando que los acuerdos establecidos se cumplen con plenas garantías.
- Establecer un marco formal de referencia para el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI) y demás sistemas de gestión certificados (ISO 27001, ISO 20000, ISO 9001, ENS), garantizando su coherencia.

2. Directrices y principios de seguridad de la información

La Dirección está comprometida con el éxito a largo plazo del Sistema, y para ello proporciona los recursos humanos, tecnológicos y económicos necesarios para su funcionamiento eficiente y eficaz, es por ello por lo que se establecen las siguientes directrices para alcanzarlo:

a) Compromiso con el desarrollo y funcionamiento eficaz del Sistema de Gestión, lo que permitirá poner en práctica las estrategias fijadas por la Dirección en materia de seguridad y calidad en la entrega de los servicios.

b) Asegurar que todos los servicios son gestionados de tal forma que garanticen el cumplimiento de los plazos, la rápida respuesta y una alta calidad.

c) Asegurar los principios de confidencialidad, integridad y disponibilidad de la información gestionada por la compañía.

d) Gestionar los riesgos que puedan impactar a la organización estableciendo los mecanismos necesarios para su control y mejora.

e) Se aplicarán todos los controles apropiados para dotar de seguridad nuestras instalaciones de tratamiento de la información.

f) EVOLUTIO cuenta con un comité de representantes de los departamentos de la compañía involucrados en la gestión del sistema, cuya misión es la de fomentar la cultura de seguridad y calidad en la organización, así como, detectar y discutir posibles carencias e irregularidades y proponer acciones correctivas cuya viabilidad es evaluada en el comité, así como, formular acciones de mejora e impulsarlas en sus correspondientes departamentos para su consecución.

g) Garantizar el cumplimiento de todas las obligaciones legales y otros requisitos normativos aplicables.

h) Garantizar la satisfacción de nuestros clientes estableciendo un equilibrio entre la calidad aportada y las necesidades reales de los clientes.

i) Gestionar la prestación de los servicios de forma eficaz y eficiente, dentro de un ciclo de vida que permita la mejora continua de los procesos implantados.

j) Disponer de mecanismos de Continuidad que garanticen la prestación de los servicios y la Seguridad de la Información ante eventos disruptivos.

k) Gestionar de forma adecuada todos los incidentes que puedan afectar a la Calidad y Seguridad de la Información de EVOLUTIO.

l) Existencia de contratos y acuerdos de nivel operativo con Proveedores y Terceros (tanto internos como externos) para establecer los niveles de servicio requeridos que brinden los mismos altos niveles de servicio que nos esforzamos por brindar a nuestros Clientes.

m) Tratar la Seguridad como proceso integral: La seguridad se gestiona de forma global, abarcando personas, procesos, tecnología, instalaciones y proveedores.

n) Proporcionar formación al personal relacionado con la información y los sistemas sobre sus deberes y obligaciones en materia de seguridad, de tal modo que dicho personal sea capaz de aplicar los principios de seguridad en el desempeño de su cometido, incluyendo el compromiso de confidencialidad y el cumplimiento de los deberes de seguridad en el ejercicio de sus funciones.

o) Realizar una gestión de la seguridad basada en riesgos: Todas las decisiones en materia de seguridad se apoyan en análisis de riesgos sistemáticos, considerando el impacto sobre los servicios y los datos.

p) Prevención, detección, respuesta y conservación: Se establecerán las medidas necesarias para prevenir incidentes, detectarlos de forma temprana, responder adecuadamente y conservar evidencias cuando sea necesario.

q) Existencia de líneas de defensa: Se aplican controles en múltiples capas (organizativos, físicos, lógicos, técnicos y procedimentales) para incrementar la resiliencia.

r) Diferenciación de responsabilidades: Se separan, cuando es viable, las funciones de operación, control y supervisión para reducir el riesgo de errores o fraudes.

s) Proteger la confidencialidad de la información de clientes, usuarios y de la propia organización.

t) Salvaguardar la integridad de la información y los sistemas.

u) Garantizar la autenticidad de los usuarios, sistemas y servicios, autorizando y tomando las medidas de control de los accesos a los sistemas de información de tal modo que solo puedan acceder las personas usuarios, procesos, dispositivos u otros sistemas debidamente autorizados, Proporcionando únicamente los permisos mínimos necesarios por perfil para que la organización alcance sus objetivos.

v) Protección de las instalaciones, implantar controles de acceso físico basados en gestión de identidades y controles de protección frente a amenazas físicas y ambientales

w) Asegurar la trazabilidad de las acciones relevantes, manteniendo registros de actividad suficientes para la investigación de incidentes y el cumplimiento normativo.

x) Mejorar de forma continua el sistema de gestión y los controles de seguridad, asegurando la integridad y actualización del sistema de información, aplicando mecanismos formales para la instalación de cualquier elemento físico, así como los parches de seguridad y actualizaciones garantizando su procedencia legítima y debida diligencia.

y) Uso responsable de inteligencia artificial. El diseño, adopción y uso de sistemas de IA se regirán por seguridad desde el diseño y por defecto, proporcionalidad de controles, transparencia y trazabilidad, garantizando el cumplimiento normativo aplicable.

z) Gestionar los riesgos asociados al tratamiento de datos personales se lleva a cabo de acuerdo con los principios establecidos por el Reglamento General de Protección de Datos (RGPD) y las directrices del Esquema Nacional de Seguridad (ENS). Asegurando lo siguiente:

    1. Identificación y evaluación de riesgos: Se identifican los riesgos asociados al tratamiento de datos personales, evaluando su impacto en la confidencialidad, integridad y disponibilidad de la información. Se llevará a cabo una Evaluación de Impacto sobre la Protección de Datos (DPIA)

    2. Medidas de mitigación: Se implementan controles adecuados, como el cifrado de datos, el control de accesos y la auditoría continua, para mitigar los riesgos identificados.

    3. Gestión de incidentes: Se establece un procedimiento específico para gestionar incidentes de seguridad relacionados con los datos personales, que incluye la notificación de violaciones de seguridad a la Autoridad de Protección de Datos y a los afectados cuando sea necesario, conforme al RGPD.

    4. Revisión continua: El análisis de riesgos se revisa regularmente o cuando se producen cambios significativos y se ajusta según los cambios en los servicios o el tratamiento de los datos personales.

Madrid a 19 de Noviembre de 2025

Jacinto Cavestany

Director General EVOLUTIO