POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad de la Información

Código	POL-0001-SGI POLITICA DE SEGURIDAD DE LA INFORMACIÓN
Versión	01
Fecha de la versión	09/06/2026
Clasificación	Público

Índice

1. INFORMACIÓN DE LA EMPRESA

Ewala IT Services SL (en adelante, Ewala) ofrece servicios de ciberseguridad gestionada y servicios de Gobierno, Riesgo y Cumplimiento (GRC) en los ámbitos IT y OT a través de su departamento de MSSP, además de desarrollar productos propios de ciberseguridad y/o en colaboración con terceros a través de su departamento de I+D+i.

La Dirección se compromete con los máximos estándares de seguridad de la información en sus procesos de negocio y con el cumplimiento normativo.

2. OBJETO

La presente Política de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información gestionada por Ewala, protegiendo los recursos de información frente a amenazas internas y externas, deliberadas o accidentales, y garantizando el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables.

Particularmente, el desarrollo y la implantación de esta política de seguridad pretende alcanzar los siguientes objetivos:

- Garantizar el cumplimiento de la legislación, reglamentación y compromisos contractuales aplicables.
- Mantener el riesgo bajo niveles aceptables definidos por la Dirección.
- Generar una cultura organizacional que reconozca y valore la seguridad de la información.
- Proporcionar una guía para los estándares, procedimientos y medidas que sustenten el SGSI.

Los objetivos específicos y medibles de seguridad de la información de Ewala se establecen para cada ejercicio en los registros internos del SGSI, junto con sus responsables, recursos, plazos y criterios de evaluación, conforme al proceso de mejora continua de la organización. Los objetivos se revisan en cada Revisión por la Dirección y se actualizan cuando los cambios del contexto, los resultados de la evaluación de riesgos o los requisitos aplicables así lo requieran.

3. ALCANCE

Esta política aplica a todos los procesos, sistemas, personas e información comprendidos en el alcance del Sistema de Gestión de Seguridad de la Información de Ewala, definido en el documento de Alcance del SGSI.

El detalle operativo de los requisitos establecidos en la presente Política se desarrolla en la información documentada del SGSI (normas, procedimientos, instrucciones y registros), mantenida bajo control documental y control de versiones, conforme al Registro de Control de la Documentación del SGSI vigente.

4. DEFINICIONES

- **Activo de información:** cualquier elemento que tenga valor para la organización, incluyendo información, software, hardware, servicios, personas y elementos intangibles como la reputación.
- **Amenaza:** causa potencial de un incidente no deseado que puede resultar en daño a un sistema u organización.
- **Confidencialidad**: la información debe ser accesible solo a aquellas personas autorizadas a tal fin.
- **Disponibilidad:** la información y sus recursos relacionados deben estar disponibles cada vez que se los requiera.
- **Incidente de seguridad:** evento o serie de eventos de seguridad de la información no deseados que tengan una probabilidad significativa de comprometer las operaciones o amenazar la seguridad de la información.
- **Integridad:** la información y sus métodos de procesamiento deben ser completos y exactos.
- **Riesgo:** efecto de la incertidumbre sobre los objetivos de seguridad de la información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Trazabilidad:** capacidad de rastrear el histórico de acceso o modificación de un activo de información.
- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO NORMATIVO Y LEGAL

Ewala se compromete al cumplimiento de la legislación, normativa y reglamentación aplicable a su actividad, incluyendo, con carácter enunciativo, pero no limitativo:

- Reglamento General de Protección de Datos (RGPD — Reglamento UE 2016/679).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
- Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996).
- Normativa sectorial aplicable en materia de ciberseguridad industrial.
- Requisitos contractuales con clientes y proveedores.
- Norma ISO/IEC 27001:2022 como marco de referencia del SGSI.

La Dirección revisará periódicamente las obligaciones legales y regulatorias aplicables, con el apoyo y asesoramiento necesarios.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información en Ewala se fundamenta en los siguientes principios:

- **Proporcionalidad:** las medidas de seguridad serán proporcionales al valor de los activos que protegen y al nivel de riesgo identificado.
- **Responsabilidad compartida:** la seguridad de la información es responsabilidad de todos los miembros de la organización, no solo del equipo técnico.
- **Defensa en profundidad:** se aplicarán múltiples capas de protección para que el fallo de una medida no comprometa la seguridad global.
- **Mínimo privilegio:** los usuarios dispondrán únicamente de los accesos y permisos estrictamente necesarios para el desempeño de sus funciones.
- **Necesidad de conocer:** el acceso a la información se otorgará exclusivamente a quienes la necesiten para realizar su trabajo.

- **Mejora continua:** el SGSI se revisará y perfeccionará de forma sistemática para adaptarse a nuevas amenazas, cambios organizativos y lecciones aprendidas.
- **Cumplimiento:** todas las actividades de la organización se realizarán conforme a la legislación vigente y a los compromisos contractuales adquiridos.

7. ROLES, RESPONSABLES Y RESPONSABILIDADES

Ewala establece y mantiene un marco de gobernanza del Sistema de Gestión de Seguridad de la Información (SGSI) que define roles, responsabilidades, autoridades y canales de escalado, con el fin de asegurar la protección de la información y el cumplimiento de la presente Política.

La Dirección garantiza la asignación de recursos y la definición de criterios de aceptación del riesgo, así como la aprobación del tratamiento del riesgo y, cuando proceda, la aceptación formal del riesgo residual y de las excepciones debidamente justificadas.

Asimismo, existen funciones designadas para coordinar la seguridad de la información y la gestión del SGSI, junto con propietarios de activos responsables de su correcta clasificación y de promover la aplicación de controles adecuados.

Todo el personal y los terceros con acceso a la información o a los sistemas de Ewala están obligados a conocer y cumplir esta Política, aplicar los controles que les sean de aplicación y notificar de forma inmediata cualquier incidente o sospecha.

8. GESTIÓN DE RIESGOS

Ewala adopta un enfoque basado en riesgos para la gestión de la seguridad de la información. La organización mantiene una metodología documentada que contempla la identificación de activos, amenazas y vulnerabilidades, la valoración del impacto y la probabilidad, y la comparación del riesgo resultante con los criterios de aceptación aprobados por la Dirección.

Para cada riesgo que supere el nivel aceptable se seleccionará una opción de tratamiento: reducir, transferir, evitar o aceptar de forma informada. Las decisiones de tratamiento se documentan conforme a los procedimientos establecidos.

La evaluación de riesgos se realizará al menos una vez al año y siempre que se produzcan cambios significativos.

9. CLASIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Ewala clasifica su información en diferentes niveles. Cada activo de información tendrá un propietario asignado responsable de su clasificación y de garantizar que se aplican los controles de protección correspondientes a su nivel. La destrucción de información se realizará mediante métodos seguros acordes al nivel de clasificación del activo.

El inventario de activos se revisará al menos una vez al año.

10. CONTROL DE ACCESO LÓGICO

El acceso a los sistemas de información de Ewala se rige por los principios de mínimo privilegio y necesidad de conocer. Cada usuario dispondrá de una cuenta personal e intransferible. Las cuentas genéricas o compartidas están prohibidas salvo para servicios técnicos específicos debidamente justificados y aprobados.

Se exigirá autenticación multifactor (MFA) para el acceso a sistemas críticos, acceso remoto y servicios corporativos en la nube, además del uso obligado de un gestor de contraseñas corporativo para la gestión y almacenamiento de contraseñas que afecten al ámbito laboral. Las cuentas con privilegios de administración estarán sujetas a controles reforzados.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

Ewala mantiene controles de seguridad física en sus instalaciones para prevenir el acceso no autorizado, los daños y las interferencias sobre la información y los sistemas. Estos controles incluyen medidas de acceso físico, vigilancia, protección ambiental, gestión de visitantes, puesto de trabajo despejado y gestión segura de equipos.

12. ENTORNO TECNOLÓGICO

Ewala define una configuración base estandarizada para los equipos de usuario, que incluye sistema operativo actualizado y las herramientas necesarias para el desempeño de las funciones asignadas.

13. SEGURIDAD DE LAS COMUNICACIONES Y LA RED

Ewala aplicará controles de segmentación de red, filtrado de tráfico, protección perimetral y seguridad de los servicios de red para proteger la información en tránsito y prevenir accesos no autorizados.

14. SEGURIDAD EN LA NUBE Y CON TERCEROS

Ewala utiliza servicios proporcionados por terceros para diversas funciones corporativas y operativas. La contratación exigirá evaluación de riesgos, inclusión de cláusulas de seguridad y confidencialidad, requisitos de control de acceso, y evidencias de cumplimiento acordes al servicio. Asimismo, durante la vigencia de la relación, Ewala realizará un seguimiento periódico del desempeño y del cumplimiento de los requisitos de seguridad acordados, y gestionará las incidencias o desviaciones detectadas conforme a los procedimientos internos aplicables.

15. CRIPTOGRAFÍA

Ewala empleará técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad de la información cuando así lo requiera su nivel de clasificación o el análisis de riesgos. Como mínimo, se aplicará cifrado en los dispositivos de usuario, en la transmisión de información confidencial y en las comunicaciones remotas.

16. COPIAS DE SEGURIDAD

Ewala realizará copias de seguridad de la información y los sistemas críticos con la frecuencia y retención adecuadas para garantizar la recuperación ante pérdida de datos o incidentes. Las copias se almacenarán en ubicaciones seguras, separadas

de los sistemas de producción, y se verificará periódicamente su integridad y capacidad de restauración.

17. GESTIÓN DE VULNERABILIDADES

Ewala mantendrá un proceso sistemático para la identificación, evaluación y remediación de vulnerabilidades técnicas en sus sistemas e infraestructura. Se realizarán análisis periódicos de vulnerabilidades y se aplicarán parches y actualizaciones de seguridad dentro de los plazos definidos según la criticidad.

18. MONITORIZACIÓN Y REGISTRO

Ewala registrará los eventos relevantes de seguridad en sus sistemas de información para permitir la detección de actividades no autorizadas, la investigación de incidentes y el cumplimiento de requisitos legales y normativos. Los registros se protegerán frente a manipulación y acceso no autorizado y se conservarán durante el periodo definido.

19. GESTIÓN DE CAMBIOS

Todo cambio en los sistemas de información, la infraestructura o las aplicaciones de Ewala seguirá un proceso controlado que incluya la solicitud, evaluación del impacto en seguridad, aprobación, implementación, verificación y documentación del cambio. Los cambios de emergencia seguirán un procedimiento abreviado con regularización posterior.

20. GESTIÓN DE INCIDENTES DE SEGURIDAD

Ewala mantendrá un proceso de gestión de incidentes de seguridad que permita detectar, notificar, evaluar, responder, documentar y aprender de los incidentes. Todo el personal tiene la obligación de informar inmediatamente de cualquier evento o sospecha de incidente de seguridad a través de los canales establecidos. Los incidentes que afecten a datos personales se gestionarán además conforme a los requisitos de notificación del RGPD.

21. CONTINUIDAD DEL NEGOCIO

Ewala establecerá y mantendrá planes de continuidad del negocio y recuperación ante desastres que garanticen la disponibilidad de los servicios críticos en caso de interrupción. Se definirán los tiempos de recuperación objetivo (RTO) y los puntos de recuperación objetivo (RPO) para cada servicio o sistema crítico, y se realizarán pruebas periódicas para verificar la eficacia de los planes.

22. USO ACEPTABLE DE LOS RECURSOS

Los usuarios de Ewala utilizarán los recursos de la organización exclusivamente para el intercambio de información o el cumplimiento de sus funciones laborales. Queda expresamente prohibido:

- El uso de los recursos para actividades ilegales o contrarias a la normativa interna.
- La instalación o distribución de software no autorizado.
- La introducción deliberada de software malicioso.
- La revelación de credenciales a terceros.
- El acceso a información, sistemas o cuentas sin autorización.
- La realización de actividades que comprometan la seguridad o disponibilidad de los sistemas.
- La extracción de información clasificada sin aprobación del responsable correspondiente.
- El uso de soportes extraíbles no autorizados.

Los empleados pueden quedar exceptuados temporalmente de alguna de estas restricciones cuando sea necesario para el ejercicio legítimo de sus funciones (por ejemplo, administradores de sistemas en el desempeño de sus tareas), siempre con autorización previa.

Los dispositivos móviles que accedan a recursos de la empresa deberán bloquearse cuando cese la actividad. El software utilizado cumplirá en todo momento los términos de su licencia.

23. TRABAJO REMOTO Y MOVILIDAD

Cuando se efectúe trabajo remoto, el empleado cumplirá las siguientes directrices:

- Solo se permitirá el uso del equipo de trabajo proporcionado por la organización.
- El acceso a los sistemas de la organización se realizará a través de los canales cifrados autorizados.
- Solo se permitirá la conexión a redes que cumplan los requisitos mínimos de seguridad definidos por la organización.
- Se mantendrá el espacio de trabajo despejado de información fuera del horario laboral.
- Se aplicarán las mismas normas de clasificación, protección y uso aceptable que en las instalaciones de Ewala.

24. FORMACIÓN Y CONCIENCIACIÓN

Ewala mantendrá un programa de formación y concienciación en seguridad de la información dirigido a todo el personal. El programa incluirá sesiones de inducción para nuevas incorporaciones, formación periódica y acciones de concienciación específicas basadas en las necesidades detectadas y los riesgos identificados.

Todo el personal deberá completar las actividades de formación que le sean asignadas.

25. REVISIÓN, MEDICIÓN Y MEJORA CONTINUA

El SGSI se someterá a revisión global con periodicidad anual, coincidente con la Revisión por la Dirección, así como a revisiones extraordinarias ante fallos importantes de seguridad. Se realizarán auditorías internas al menos una vez al año para verificar la conformidad con los requisitos de ISO 27001, esta política y los procedimientos asociados.

Ewala definirá indicadores de seguridad de la información que permitan medir la eficacia de los controles y el desempeño del SGSI. La mejora continua se sustentará en el seguimiento de no conformidades, acciones correctivas, lecciones aprendidas y resultados de auditorías.

26. PROCESO DE EXCEPCIONES

Cualquier desviación respecto a lo establecido en esta política o en los procedimientos del SGSI requerirá una excepción formal, que incluirá la justificación, un análisis del riesgo residual, la aprobación del responsable competente y una vigencia máxima definida.

27. RÉGIMEN DISCIPLINARIO

El incumplimiento de esta política o de los procedimientos de seguridad asociados podrá dar lugar a la adopción de medidas disciplinarias conforme a la legislación laboral vigente y al convenio colectivo aplicable. Las medidas serán proporcionales a la gravedad del incumplimiento y a la intencionalidad del mismo.

En el caso de contratistas o terceros, el incumplimiento podrá dar lugar a la terminación de la relación contractual conforme a las cláusulas de seguridad incluidas en sus contratos.

28. DOCUMENTACIÓN RELACIONADA

Los documentos, procedimientos, instrucciones técnicas y registros que desarrollan la presente Política se gestionan bajo control documental en el **Registro de Control de la Documentación del SGSI**, disponible para el personal autorizado a través del repositorio documental corporativo.

Dado el carácter público de esta Política, no se incluye en este documento la enumeración completa de la documentación interna del SGSI. La versión vigente de cada documento aplicable se identifica en dicho registro.

29. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

Esta política se revisará al menos anualmente, coincidiendo con la Revisión por la Dirección del SGSI, así como ante cambios significativos o incidentes graves que lo justifiquen. Las revisiones serán aprobadas por la Dirección y el histórico de versiones se registra en la sección correspondiente de este documento.

30. ÁMBITO DE APLICACIÓN Y DIFUSIÓN

La presente Política entrará en vigor una vez aprobada por la Dirección de Ewala y será comunicada a todo el personal a través de los canales corporativos establecidos.

Esta política vincula a empleados, contratistas, consultores, trabajadores temporales y otros colaboradores de Ewala, incluido todo el personal afiliado a terceros con acceso a los recursos de la organización, a quienes se informará de la obligación de conocer y cumplir la presente política.

31. CONTROL DEL DOCUMENTO

CONTROL DE VERSIONES		
Versión	**Fecha**	**Cambios realizados**
00	10/02/2026	Primera edición del documento y aprobación
01	09/06/2026	Incorporación en §2 (OBJETO) de la referencia al proceso de mejora continua y a los registros internos del SGSI para el establecimiento, revisión y actualización de los objetivos específicos de seguridad de la información, en cumplimiento de la cláusula 5.2 de ISO/IEC 27001:2022. Actualización del alcance del SGSI (no modificación sustancial)

APROBACIÓN		
Rol	Firma	Fecha
Dirección/CEO		09/06/2026