Política de Seguridad de la Información

IBERORAD 1895, SL

La Política de Seguridad de la Información de IBERORAD 1895, SL es el documento fundamental que establece el marco estratégico y las directrices generales para proteger todos los activos de información de la empresa. Este documento define los principios, roles y responsabilidades necesarios para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información empresarial. La política se desarrolla en cumplimiento del Esquema Nacional de Seguridad (ENS) e ISO/IEC 27001:2022, estableciendo las bases del Sistema de Gestión de Seguridad de la Información. Es de obligado cumplimiento para todo el personal de la organización y terceros que acceden a los sistemas, constituyendo el pilar sobre el que se construye toda la arquitectura de ciberseguridad corporativa.

Redactado / Revisado por:	Toni Sanchez 30 mar 2026
Aprobado por:	Julio Moreno 30 mar 2026
Estat	Aprobado

Historial de cambios

Versión	Cambios	Fecha	Autor
1.0	Versión inicial del documento	07-10-2025	
2.0	Versión firmada	30-03-2026	

Índice

1. Introducción y Declaración de la Dirección

La Dirección de IBERORAD 1895, SL, consciente de la importancia crítica de la información como activo fundamental para la consecución de sus objetivos de negocio, establece la presente Política de Seguridad de la Información como pilar de su Sistema de Gestión de Seguridad de la Información (SGSI).

Esta política manifiesta el compromiso firme de la Dirección con la protección de sus activos de información frente a todo tipo de amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada y los servicios prestados.

El cumplimiento de esta política es obligatorio para todo el personal de la organización, así como para cualquier tercero que acceda, procese o gestione información propiedad de IBERORAD 1895, SL o bajo su custodia.

2. Objeto y Alcance

Objeto:
El objeto de esta política es establecer el marco de actuación común para proteger los activos de información, definir las directrices generales del SGSI y promover una cultura de seguridad en toda la organización. Se busca garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables, así como alinear la seguridad con los objetivos estratégicos de la empresa.

Alcance:
El SGSI y esta política aplican a todos los sistemas de información, procesos, infraestructuras tecnológicas, datos y servicios que soportan la actividad de IBERORAD 1895, SL, incluyendo:

- Todos los empleados, directivos y personal temporal.
- Contratistas, proveedores y colaboradores externos con acceso a los sistemas de información.
- Todos los activos de información, tanto en formato físico como digital.
- Las infraestructuras tecnológicas, incluyendo hardware, software, redes de comunicaciones y servicios en la nube.

3. Marco Normativo y de Referencia

Esta política se desarrolla en conformidad con la legislación vigente y los estándares reconocidos en materia de seguridad de la información, ciberseguridad y protección de datos, incluyendo el Esquema Nacional de Seguridad y la norma internacional ISO/IEC 27001.

4. Principios Fundamentales de la Seguridad

La seguridad de la información en IBERORAD 1895, SL se rige por los siguientes principios rectores:

- Seguridad como proceso integral: La seguridad se aborda como un proceso continuo y dinámico que requiere una gestión constante.
- Gestión de riesgos: La identificación, evaluación y tratamiento de los riesgos es la base para la selección de las medidas de seguridad, buscando un equilibrio entre la protección y la funcionalidad.
- Prevención, detección, respuesta y conservación: Se implementarán controles para prevenir incidentes, mecanismos para detectarlos cuando ocurran, planes para responder eficazmente y procedimientos para conservar las evidencias.
- Vigilancia continua: El estado de la seguridad de los sistemas se supervisará de forma permanente para detectar vulnerabilidades y actividades anómalas.
- Líneas de defensa: Se establecerá una estrategia de defensa en profundidad, combinando medidas organizativas, físicas y tecnológicas para crear múltiples barreras de protección.
- Reevaluación periódica: El análisis de riesgos y las medidas de seguridad implementadas se revisarán y actualizarán periódicamente o tras cambios significativos en el entorno.

5. Organización de la Seguridad

Para garantizar una gestión eficaz de la seguridad, se define la siguiente estructura de roles y responsabilidades:

- Comité de Seguridad de la Información: Órgano colegiado, presidido por un miembro de la Dirección, responsable de impulsar y supervisar el SGSI, aprobar las políticas y los recursos necesarios.
- Responsable de la Información: Tiene la potestad de establecer los requisitos de la información tratada en cuanto a su nivel de confidencialidad, integridad y disponibilidad.
- Responsable del Servicio: Tiene la potestad de establecer los requisitos de seguridad de los servicios prestados.
- Responsable de la Seguridad (RSI): Es el principal responsable de la correcta implementación, operación y mantenimiento del SGSI, así como de la supervisión del cumplimiento de las políticas y procedimientos. Actúa como punto de contacto para la coordinación de incidentes.
- Responsable del Sistema: Es responsable de la operación diaria del sistema de información, aplicando las medidas de seguridad definidas.

6. Directrices Generales de Seguridad

6.1. Gestión de Activos y Riesgos

- Se mantendrá un inventario de activos de información actualizado, clasificándolos según su criticidad y requisitos de seguridad.
- Se realizará un análisis de riesgos periódico sobre los activos y servicios para identificar las amenazas y vulnerabilidades, evaluando su impacto y probabilidad.
- Las medidas de seguridad se seleccionarán y aplicarán en función de los resultados del análisis de riesgos.

6.2. Control de Acceso

- El acceso a la información y a los sistemas estará restringido y se basará en los principios de "necesidad de conocer" y "mínimo privilegio".
- Todo acceso estará prohibido por defecto, salvo autorización expresa.
- Se utilizarán identificadores de usuario únicos e intransferibles para cada persona, prohibiéndose el uso de cuentas genéricas.
- Se implementarán mecanismos de autenticación robustos, que podrán incluir múltiples factores de autenticación para accesos a sistemas críticos o desde redes no controladas.
- Se gestionará el ciclo de vida completo de los derechos de acceso (alta, modificación y baja), asegurando la revocación inmediata de los permisos cuando finalice la relación del usuario con la organización.
- El acceso remoto será autorizado, cifrado y auditado.

6.3. Seguridad Física y del Entorno

- Los equipos e infraestructuras críticas se ubicarán en áreas seguras, con controles de acceso físico adecuados para prevenir accesos no autorizados, daños o interferencias.
- Se establecerán medidas de protección contra amenazas ambientales (incendios, inundaciones) y fallos de suministro eléctrico.

6.4. Seguridad en las Operaciones

- Se aplicarán procedimientos de configuración segura (bastionado) en todos los sistemas antes de su puesta en producción, eliminando funcionalidades, cuentas y contraseñas por defecto.
- La gestión de cambios se realizará de forma controlada para minimizar el impacto en la seguridad y la disponibilidad de los servicios.
- Se implementarán mecanismos de protección contra código malicioso (malware) en todos los sistemas susceptibles.

- Se generarán y conservarán registros de actividad (logs) que permitan la auditoría, la detección de incidentes y el análisis forense. El acceso a estos registros estará protegido.
- Se utilizarán algoritmos criptográficos autorizados y se gestionará de forma segura el ciclo de vida de las claves criptográficas.

6.5. Seguridad de las Comunicaciones

- Se protegerá la información durante su transmisión a través de redes públicas o inalámbricas mediante el uso de cifrado.
- Las redes se segmentarán para limitar el impacto de posibles incidentes de seguridad.
- Toda interconexión con sistemas de otras entidades deberá ser autorizada formalmente.

6.6. Relaciones con Proveedores y Terceros

- Los requisitos de seguridad de la información se incluirán en los contratos y acuerdos de nivel de servicio (SLA) con proveedores.
- Se exigirá a los proveedores que manejen información sensible o presten servicios críticos el cumplimiento de esta política y de las normativas aplicables.
- Se supervisará el cumplimiento de los acuerdos de seguridad por parte de los terceros.

6.7. Gestión de Incidentes de Seguridad

- Se establecerá un proceso formal para la notificación, análisis, contención, erradicación y recuperación de los incidentes de seguridad.
- Todos los empleados tienen la obligación de notificar cualquier sospecha de incidente de seguridad a través de los canales establecidos.
- Los incidentes se registrarán, investigarán y se utilizarán para la mejora continua del SGSI (lecciones aprendidas).
- Se realizarán las notificaciones pertinentes a las autoridades competentes según los plazos y formas legalmente establecidos.

6.8. Continuidad del Negocio

- Se realizarán análisis de impacto en el negocio (BIA) para identificar los procesos críticos y sus requisitos de disponibilidad.
- Se desarrollarán e implementarán planes de continuidad y de recuperación ante desastres para garantizar la restauración de los servicios esenciales en tiempos aceptables tras una interrupción.
- Estos planes se probarán periódicamente para asegurar su eficacia.

6.9. Cumplimiento Normativo y Auditoría

- Se identificarán y cumplirán todos los requisitos legales, regulatorios y contractuales aplicables en materia de seguridad de la información y protección de datos.
- Se llevarán a cabo auditorías internas y externas de forma periódica para verificar la eficacia y el cumplimiento del SGSI.

7. Formación y Concienciación

IBERORAD 1895, SL se compromete a proporcionar formación y concienciación continua en materia de seguridad de la información a todo el personal. El objetivo es que todos los miembros de la organización comprendan sus responsabilidades y estén capacitados para proteger los activos de información en su trabajo diario.

8. Revisión y Mejora Continua

Esta política será revisada anualmente por el Comité de Seguridad, o antes si se producen cambios significativos en el entorno tecnológico, de negocio o normativo. El SGSI se gestionará bajo un ciclo de mejora continua para garantizar su adecuación, idoneidad y eficacia a lo largo del tiempo.

Firmado por ***1931** JULIO MORENO (R: ****8551*) el día 07/04/2026 con un certificado emitido por AC Representación