# Política de Seguridad de la Información ENS

IBERORAD 1895, SL

Este documento constituye la Política de Seguridad de la Información de IBERORAD, redactada en conformidad con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS). Establece los principios básicos y los requisitos mínimos para la protección adecuada de la información tratada y los servicios prestados por la organización.

| | |
|---|---|
| Redactado / Revisado por: | Toni Sánchez 2 ene 2026 |
| Aprobado por: | Julio Moreno 2 ene 2026 |
| Estat | Aprobado |

# Historial de cambios

| Versión | Cambios | Fecha | Autor |
|---|---|---|---|
| 1.0 | Versión inicial del documento | 01-01-2026 | |
| | | | |
| | | | |

# Índice

## 1. INTRODUCCIÓN

IBERORAD 1895, SL (en adelante, la Entidad) depende de sus sistemas de información y comunicaciones (TIC) para alcanzar sus objetivos de negocio. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada.

Esta Política define el marco de gestión para garantizar la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de la información y los servicios, en estricto cumplimiento con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

## 2. ALCANCE

Esta Política es de aplicación a:

- Todos los sistemas de información, servicios y activos de la Entidad.
- Todos los miembros de la organización.
- Todos los prestadores de servicios, proveedores y terceros que accedan o traten información de la Entidad.

## 3. MISIÓN Y OBJETIVOS DE SEGURIDAD

La misión de la Entidad es la prestación de servicios de [Describir brevemente la actividad principal, ej: diagnóstico por imagen, servicios médicos, etc.], garantizando la excelencia y la confianza de sus clientes y pacientes.

Para apoyar esta misión, la Entidad establece los siguientes objetivos de seguridad:

- Asegurar que los sistemas TIC están protegidos contra amenazas para garantizar la continuidad de los servicios prestados.
- Proteger la confidencialidad de los datos, especialmente aquellos de carácter personal o clínico, asegurando que solo sean accesibles por personas autorizadas.
- Garantizar la integridad y trazabilidad de la información médica y administrativa.
- Cumplir con la legislación vigente, incluyendo el ENS y la normativa de protección de datos.

## 4. MARCO NORMATIVO

Las actividades de seguridad se regirán por la legislación aplicable, destacando principalmente:

- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.

- Reglamento (UE) 2016/679 (RGPD) relativo a la protección de datos personales.
- Ley Orgánica 3/2018 (LOPDGDD) de Protección de Datos Personales.
- [Añadir normativa sectorial si aplica, ej: Ley 41/2002 de autonomía del paciente].

## 5. PRINCIPIOS DE SEGURIDAD

La seguridad en la Entidad se rige por los principios básicos establecidos en el Capítulo II del ENS:

1. **Seguridad integral:** Entendida como un proceso que cubre elementos humanos, técnicos y organizativos.
2. **Gestión basada en riesgos:** Las medidas de seguridad se seleccionan basándose en un análisis de riesgos profesional.
3. **Prevención, detección, respuesta y conservación:** Actuar para prevenir incidentes, detectarlos rápido si ocurren, restaurar el servicio y conservar evidencias.
4. **Líneas de defensa:** Implementar capas de seguridad independientes (defensa en profundidad).
5. **Vigilancia continua:** Evaluar y actualizar las medidas de seguridad de forma constante.
6. **Diferenciación de responsabilidades:** Separar las funciones de supervisión de la seguridad de las de operación del sistema.

## 6. ORGANIZACIÓN DE LA SEGURIDAD

### 6.1. Roles y Responsabilidades

Conforme al Artículo 12 del RD 311/2022, se definen los siguientes roles:

- **Comité de Seguridad de la Información:** Órgano colegiado encargado de coordinar la seguridad, aprobar normativas y resolver conflictos. Estará presidido por la Dirección e integrado por los Responsables de Seguridad, Sistema e Información.
- **Responsable de la Información:** Persona con potestad para determinar los requisitos de seguridad de la información (niveles de confidencialidad, integridad, etc.).
- **Responsable del Servicio:** Persona con potestad para determinar los requisitos de los servicios prestados (disponibilidad y nivel de servicio).
- **Responsable de la Seguridad:** Determina las decisiones para satisfacer los requisitos de seguridad y supervisa el cumplimiento de la normativa. Reporta a la Dirección y es distinto del Responsable del Sistema.
- **Responsable del Sistema:** Encargado de la operación, mantenimiento y administración técnica del sistema de información.

### 6.2. Procedimiento de Designación

- Los nombramientos del Responsable de Seguridad y del Comité se realizan mediante resolución formal de la Dirección.
- Los nombramientos se revisarán cada dos años o cuando el puesto quede vacante.
- Se garantizará la sustitución de estos roles en caso de ausencia o enfermedad para asegurar la continuidad.

#### 6.3. Resolución de Conflictos

En caso de conflicto de criterio entre los diferentes responsables (ej. entre Seguridad y Sistemas), el Comité de Seguridad de la Información será el órgano encargado de dirimir la discrepancia y tomar la decisión final.

## 7. GESTIÓN DE RIESGOS

El análisis y gestión de riesgos es parte esencial del proceso de seguridad.

- Se realizará un análisis de riesgos formal al menos **una vez al año**.
- Se repetirá el análisis siempre que haya cambios significativos en la información, los servicios o tras un incidente grave.
- Se tendrán en cuenta los riesgos específicos derivados del tratamiento de datos personales, coordinándose con el Delegado de Protección de Datos (DPD).

## 8. DATOS PERSONALES

La Entidad aplicará las medidas técnicas y organizativas necesarias para cumplir con el RGPD. Cualquier tratamiento de datos personales estará sujeto al correspondiente análisis de riesgos de privacidad y, cuando proceda, a una Evaluación de Impacto (EIPD).

## 9. ESTRUCTURA DOCUMENTAL

Para desarrollar esta Política, la Entidad generará un cuerpo normativo clasificado en:

- **Normativa de Seguridad:** Documentos de obligado cumplimiento que regulan aspectos concretos (ej. Normativa de Uso Aceptable, Normativa de Control de Accesos).
- **Procedimientos:** Instrucciones paso a paso para la ejecución de tareas operativas de seguridad.
- **Guías Técnicas:** Recomendaciones y buenas prácticas para la configuración o uso de sistemas.

Esta documentación estará disponible y accesible para todo el personal que necesite conocerla para el desempeño de sus funciones.

## 10. FORMACIÓN Y CONCIENCIACIÓN

La seguridad incumbe a todos los miembros de la Entidad.

- Se realizará al menos una acción de concienciación anual para todo el personal.
- El personal con responsabilidades técnicas (administradores de sistemas) recibirá formación específica en seguridad TIC.
- Es obligación de todo el personal conocer y cumplir esta Política y sus normas de desarrollo.

## 11. TERCERAS PARTES Y PROVEEDORES

Cuando la Entidad contrate servicios tecnológicos o ceda información a terceros:

- Se les hará partícipes de esta Política y se les exigirá el cumplimiento del ENS de forma proporcional al riesgo del servicio.
- Los contratos incluirán cláusulas de confidencialidad y requisitos de seguridad (Acuerdos de Nivel de Servicio - SLA).
- El proveedor deberá designar un Punto de Contacto (POC) de seguridad para la coordinación operativa y gestión de incidentes.
- Si un proveedor no puede cumplir con los requisitos exigidos, el Responsable de Seguridad deberá emitir un informe de riesgos que requerirá aprobación de la Dirección antes de la contratación.

## 12. GESTIÓN DE INCIDENTES

La Entidad dispondrá de un procedimiento formal para la detección, notificación, y resolución de incidentes de seguridad. Todo empleado está obligado a reportar cualquier anomalía o sospecha de incidente de seguridad a través de los canales establecidos, sin dilación indebida.

## 13. ENTRADA EN VIGOR

La presente Política de Seguridad entra en vigor a partir del día siguiente de su fecha de aprobación y firma, derogando cualquier política anterior en la materia.

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