

Política de Seguridad de la Información ISO27001

IBERORAD 1895, SL

A continuación se presenta la Política de Seguridad de la Información, el documento de más alto nivel que establece el compromiso, la dirección y los principios fundamentales que rigen la seguridad en IBERORAD. Este documento formaliza el respaldo de la Alta Dirección al SGSI, define el marco de actuación para proteger los activos de información de la compañía y de sus clientes, y sirve como referencia obligatoria para todo el personal y las partes interesadas, en cumplimiento con los requisitos de la norma ISO 27001 y las normativas aplicables.

Redactado / Revisado por:	Toni Sánchez 22 dic 2025
Aprobado por:	Julio Moreno 22 dic 2025
Estat	Aprobado

Historial de cambios

Versión	Cambios	Fecha	Autor
1.0	Versión inicial del documento	16-01-2026	

Índice

1. Declaración de Compromiso de la Dirección.....	4
2. Propósito y Objetivos Estratégicos.....	4
3. Alcance.....	4
4. Marco Normativo y de Cumplimiento.....	5
5. Principios Fundamentales de Seguridad.....	5
6. Organización y Responsabilidades de Seguridad.....	6
7. Estructura Documental del SGSI.....	6
8. Comunicación, Revisión y Disponibilidad.....	6

1. Declaración de Compromiso de la Dirección

La Dirección de **IBERORAD**, consciente de la importancia crítica que la información representa para el desarrollo de nuestras operaciones, la consecución de nuestros objetivos de negocio y, especialmente, para mantener la confianza de nuestros clientes, reconoce la seguridad de la información como un pilar estratégico y un principio fundamental de nuestra actividad.

Los datos de nuestros clientes, junto con nuestra propiedad intelectual, información corporativa y nuestros procesos internos, constituyen activos de máximo valor que deben ser protegidos de forma adecuada frente a amenazas internas y externas.

Por todo ello, la Dirección de **IBERORAD** se compromete a liderar, promover y mantener un **Sistema de Gestión de Seguridad de la Información (SGSI)** eficaz y en mejora continua, basado en los requisitos de la norma **UNE-ISO/IEC 27001:2022** y la legislación vigente aplicable.

Esta política es de obligado cumplimiento para todo el personal de **IBERORAD** y será comunicada, entendida y aplicada en todos los niveles de la organización.

2. Propósito y Objetivos Estratégicos

El propósito de esta política es establecer el marco de referencia general para proteger los activos de información de **IBERORAD** y los que nos confían nuestros clientes, garantizando la **confidencialidad, integridad y disponibilidad** de la información, así como la continuidad de las operaciones de negocio.

Esta política proporciona el marco para el establecimiento de objetivos anuales de seguridad de la información, los cuales serán medibles y coherentes con la dirección estratégica de la compañía, orientados a:

- Minimizar el riesgo de incidentes de seguridad.
- Asegurar la resiliencia de nuestros servicios.
- Garantizar el cumplimiento legal y contractual.

3. Alcance

Esta política es de aplicación a todos los empleados, directivos, personal subcontratado y terceros que tengan acceso a los activos de información y sistemas incluidos en el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

El SGSI cubre los sistemas de información que dan soporte a:

Sistemas de información que dan soporte a la prestación de servicios de telerradiología a través de la plataforma web nubelan.net, sus aplicaciones asociadas, los procesos relacionados con la recepción, procesamiento, almacenamiento, diagnóstico y entrega de informes y estudios radiológicos.

4. Marco Normativo y de Cumplimiento

IBERORAD se compromete a cumplir con todos los requisitos aplicables a su actividad, incluyendo:

- La legislación y regulación vigente, con especial atención al **Reglamento (UE) 2016/679 General de Protección de Datos (RGPD)** y la **Ley Orgánica 3/2018 (LOPDGDD)**.
- *El Real Decreto 311/2022 (Esquema Nacional de Seguridad) cuando IBERORAD trabaja con la administración pública.*
- Los requisitos derivados de la norma internacional **UNE-ISO/IEC 27001:2022**.
- Las obligaciones contractuales en materia de seguridad y privacidad suscritas con clientes, proveedores y socios.

5. Principios Fundamentales de Seguridad

La gestión de la seguridad de la información en **IBERORAD** se regirá por los siguientes principios:

1. **Gestión de Riesgos:** Las decisiones y la selección de controles de seguridad se basarán en un proceso continuo de identificación, análisis, evaluación y tratamiento de los riesgos.
2. **Seguridad como Proceso Integral:** La seguridad se gestionará como un proceso continuo e integrado en todos los ciclos de vida de los servicios y sistemas de la organización.
3. **Prevención, Detección y Respuesta:** Se implementarán medidas para prevenir los incidentes de seguridad, mecanismos para detectarlos cuando ocurran y planes para responder de forma eficaz y minimizar su impacto.
4. **Defensa en Profundidad:** Se establecerán múltiples capas de seguridad (organizativas, físicas y lógicas) para proteger los activos de información.
5. **Seguridad Física y del Entorno:** Se implementarán las medidas necesarias para proteger las instalaciones físicas y las infraestructuras de soporte frente a amenazas ambientales (incendios, inundaciones, desastres naturales) y accesos físicos no autorizados.
6. **Medio ambiente:** Se adoptarán las medidas necesarias considerando la protección del medio ambiente y evaluando de manera rigurosa el impacto que dichas medidas puedan generar sobre este.

7. **Vigilancia Continua:** Se supervisará de forma constante el estado de la seguridad de los sistemas para detectar amenazas y vulnerabilidades.
8. **Mejora Continua:** Se revisará y mejorará de forma periódica la eficacia del SGSI para incrementar el nivel de seguridad y la madurez de la organización.

6. Organización y Responsabilidades de Seguridad

La seguridad de la información es una responsabilidad compartida, articulada a través de la siguiente estructura:

- **Alta Dirección:** Es la máxima responsable del SGSI, asegurando el liderazgo, el compromiso y la provisión de los recursos necesarios.
- **Comité de Seguridad de la Información:** Órgano de gobierno responsable de la toma de decisiones estratégicas, supervisión del SGSI y aprobación de normativas.
- **Responsable de Seguridad de la Información (RSI / CISO):** Responsable de la implantación, operación, supervisión y mantenimiento del SGSI, actuando como punto de contacto principal.
- **Todo el Personal:** Todos los empleados y colaboradores tienen la responsabilidad de conocer y cumplir esta política y la normativa de seguridad aplicable en el desempeño de sus funciones.

El incumplimiento de esta política y su normativa de desarrollo podrá dar lugar a las medidas disciplinarias pertinentes, de acuerdo con la legislación vigente.

7. Estructura Documental del SGSI

Esta Política de Seguridad de la Información es el documento de máximo nivel del SGSI. Se desarrolla y se materializa a través de una jerarquía de documentos que incluye:

1. **Políticas Específicas:** (Ej. Control de Accesos, Uso Aceptable de Activos, Copias de Seguridad).
2. **Procedimientos Operativos:** Pasos detallados para ejecutar tareas de seguridad.
3. **Registros:** Evidencias de cumplimiento.

8. Comunicación, Revisión y Disponibilidad

Esta política será comunicada a todo el personal y a las partes interesadas relevantes para asegurar su comprensión y aplicación. Será revisada como mínimo **anualmente**, o siempre que se produzcan cambios significativos en la organización o en el entorno (legislativo, tecnológico, de negocio), para garantizar su continua idoneidad y eficacia.

Como documento de carácter público (o disponible bajo solicitud), esta Política de Seguridad de la Información reafirma nuestro compromiso con la transparencia y la confianza.

Fdo.: JAVIER MOTA MARTÍNEZ

Director General **IBERORAD**
