POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

IBERORAD 1895, SL (en adelante, la Entidad) depende de sus sistemas de información y comunicaciones 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 o de los servicios prestados.

Esta Política de Seguridad de la Información define el marco de gestión para garantizar la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de la información y de los servicios, en cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), y constituye el documento de máximo nivel del cuerpo normativo de seguridad de la Entidad.

2. Alcance

Esta Política es de aplicación a todos los sistemas de información, servicios y activos de la Entidad; a todos los miembros de la organización, con independencia de su puesto o relación contractual; y a todos los prestadores de servicios, proveedores y terceros que accedan o traten información o sistemas de la Entidad. En particular, aplica al sistema de información que da soporte a los servicios de telerradiología y diagnóstico por imagen (plataforma Nubelan), categorizado como de categoría MEDIA conforme al documento 01-02 «Categorización y valoración de los sistemas».

3. Misión y objetivos de seguridad

La misión de la Entidad es la prestación de servicios de telerradiología y diagnóstico por imagen a centros médicos y profesionales sanitarios: recepción de los estudios radiológicos realizados por los centros, interpretación por radiólogos especialistas y emisión de los informes de diagnóstico correspondientes a través de la plataforma Nubelan, garantizando la calidad asistencial, la protección de los datos de salud de los pacientes y la confianza de los centros clientes.

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

- Asegurar que los sistemas de información están protegidos frente a las amenazas que puedan comprometer la continuidad de los servicios de diagnóstico prestados a los centros clientes.
- Proteger la confidencialidad de la información, especialmente de los datos de carácter personal y de salud, garantizando que solo sea accesible por personas autorizadas y con necesidad de conocer.
- Garantizar la integridad, autenticidad y trazabilidad de la información clínica y administrativa, de modo que pueda confiarse en los estudios e informes y atribuirse cada actuación a su autor.
- Cumplir la legislación y la normativa aplicables, en particular el Esquema Nacional de Seguridad y la normativa de protección de datos personales y sanitaria.
- Promover la mejora continua del sistema de gestión de la seguridad mediante la gestión de riesgos, la formación del personal y la revisión periódica de las medidas implantadas.

4. Marco normativo

Las actividades de seguridad de la información de la Entidad se rigen por la legislación y normativa siguientes:

Norma	Objeto
Real Decreto 311/2022, de 3 de mayo	Esquema Nacional de Seguridad: principios básicos, requisitos mínimos y medidas de seguridad (Anexo II) aplicables al sistema de información.
Instrucciones Técnicas de Seguridad del ENS	ITS de Informe del Estado de la Seguridad (Resolución de 7/10/2016), ITS de Conformidad con el ENS (Resolución de 13/10/2016), ITS de Auditoría de la Seguridad (Resolución de 27/3/2018) e ITS de Notificación de Incidentes de Seguridad (Resolución de 13/4/2018).
Guías CCN-STIC	Guías de seguridad del Centro Criptológico Nacional aplicables al sistema, conforme al documento «Inventario de ITS y guías CCN-STIC aplicables» (ENS-INV-CCN).
Reglamento (UE) 2016/679 (RGPD)	Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
Ley Orgánica 3/2018 (LOPDGDD)	Protección de datos personales y garantía de los derechos digitales.
Ley 41/2002, de 14 de noviembre	Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, aplicable al tratamiento de estudios e informes de diagnóstico.
Ley 34/2002 (LSSI-CE)	Servicios de la sociedad de la información y comercio electrónico, aplicable al portal web de acceso a resultados.
Reglamento (UE) 910/2014 (eIDAS)	Identificación electrónica y servicios de confianza para las transacciones electrónicas (certificados y firma electrónica).
Normativa laboral y mercantil aplicable	Obligaciones generales de la Entidad como empleador y sociedad mercantil con incidencia en la gestión de la información.

El Responsable de Seguridad mantiene actualizado el registro de la legislación y normativa aplicables, revisándolo al menos con carácter anual y cuando se publiquen novedades normativas que afecten al sistema.

5. Principios de seguridad

La seguridad de la Entidad se rige por los principios básicos establecidos en el Capítulo II del Real Decreto 311/2022:

- Seguridad integral: la seguridad se entiende como un proceso integral constituido por los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema.
- Gestión de la seguridad basada en los riesgos: el análisis y la gestión de riesgos es parte esencial del proceso de seguridad y permite mantener un entorno controlado, minimizando los riesgos a niveles aceptables.
- Prevención, detección, respuesta y conservación: la seguridad contempla la prevención de incidentes, su detección temprana, la respuesta eficaz y la conservación de las evidencias.
- Existencia de líneas de defensa: el sistema dispone de una estrategia de protección constituida por múltiples capas de seguridad independientes.
- Vigilancia continua y reevaluación periódica: las medidas de seguridad se reevalúan y actualizan periódicamente para adecuarlas a la evolución de los riesgos y de las tecnologías.

- Diferenciación de responsabilidades: la responsabilidad de la seguridad del sistema está diferenciada de la responsabilidad de su operación.

6. Organización de la seguridad

6.1. Estructura organizativa

La estructura de seguridad de la Entidad está formada por la Dirección, el Comité de Seguridad de la Información, el Responsable de la Información, el Responsable del Servicio, el Responsable de Seguridad, el Responsable del Sistema y el Delegado de Protección de Datos. Los titulares vigentes de cada rol constan en las actas y resoluciones de nombramiento custodiadas en el repositorio documental del sistema de gestión.

6.2. Funciones y responsabilidades de los roles

Dirección. Es la responsable última de la seguridad de la información de la Entidad. Aprueba esta Política y sus revisiones, dota a la organización de los recursos necesarios, nombra a los titulares de los roles de seguridad, preside el Comité de Seguridad de la Información y acepta formalmente el riesgo residual del sistema a propuesta del Responsable de Seguridad.

Comité de Seguridad de la Información. Órgano colegiado de coordinación de la seguridad, presidido por la Dirección e integrado por el Responsable de Seguridad, el Responsable del Sistema y el Responsable de la Información y del Servicio, con la participación del Delegado de Protección de Datos cuando los asuntos afecten a datos personales. Coordina e impulsa el sistema de gestión, aprueba la normativa de seguridad de desarrollo de esta Política, realiza el seguimiento periódico del estado de la seguridad y de los planes de mejora, propone a la Dirección la revisión de esta Política y resuelve los conflictos de criterio entre los responsables.

Responsable de la Información. Persona con potestad para determinar los requisitos de seguridad de la información tratada, valorándola en las dimensiones de confidencialidad, integridad, trazabilidad y autenticidad conforme al Anexo I del ENS, y para aprobar y suscribir formalmente dicha valoración. Acepta los niveles de riesgo que afectan a la información.

Responsable del Servicio. Persona con potestad para determinar los requisitos de los servicios prestados, incluida su disponibilidad y niveles de servicio, y para aprobar y suscribir formalmente su valoración. Acepta los niveles de riesgo que afectan a los servicios. En la Entidad, las funciones de Responsable de la Información y de Responsable del Servicio recaen en la misma persona, acumulación prevista por la guía CCN-STIC 801.

Responsable de Seguridad. Determina las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios; supervisa la implantación de las medidas del Anexo II y su eficacia; determina la categoría del sistema conforme al Anexo I y la aprueba formalmente; elabora y aprueba la Declaración de Aplicabilidad; aprueba los procedimientos operativos de seguridad; promueve la formación y concienciación; gestiona las auditorías de seguridad y los planes de acción derivados; gestiona la notificación de incidentes a las autoridades cuando proceda; y reporta del estado de la seguridad al Comité y a la Dirección. Es una figura distinta e independiente del Responsable del Sistema.

Responsable del Sistema. Desarrolla, opera y mantiene el sistema de información durante todo su ciclo de vida; define su topología y la gestión de su configuración; implanta las medidas de seguridad en el plano técnico y operativo; gestiona las incidencias de explotación; y puede acordar la suspensión del tratamiento de una información o de la prestación de un servicio si tiene conocimiento de deficiencias graves de seguridad, informando al Responsable de Seguridad y a los responsables afectados.

Delegado de Protección de Datos (DPD). Informa y asesora a la Entidad sobre las obligaciones de la normativa de protección de datos, supervisa su cumplimiento, atiende a los interesados y coopera con la autoridad de control. Coordina su actuación con el Responsable de Seguridad, garantizándose en todo caso la ausencia de conflicto de intereses en el desempeño de sus funciones.

6.3. Responsabilidades de aprobación

Las responsabilidades de aprobación dentro del sistema de gestión quedan asignadas del modo siguiente:

Elemento	**Aprobación**
Política de Seguridad de la Información (este documento) y sus revisiones	Dirección
Normativa de seguridad (segundo nivel documental)	Comité de Seguridad de la Información
Procedimientos operativos de seguridad (tercer nivel documental)	Responsable de Seguridad
Valoración de la información y de los servicios	Responsable de la Información y del Servicio
Categoría de seguridad del sistema	Responsable de Seguridad
Declaración de Aplicabilidad	Responsable de Seguridad
Análisis de riesgos y aceptación del riesgo residual	Dirección, a propuesta del Responsable de Seguridad
Nombramientos de los roles de seguridad	Dirección

6.4. Procedimiento de designación y renovación

Los nombramientos de los roles de seguridad y de los miembros del Comité se realizan mediante resolución formal de la Dirección, con aceptación expresa de las funciones por la persona designada. Los nombramientos se revisan cada dos años o cuando el puesto quede vacante, y se garantiza la sustitución temporal en caso de ausencia para asegurar la continuidad de las funciones. Las designaciones y ceses quedan registrados en las actas correspondientes.

6.5. Resolución de conflictos

En caso de conflicto de criterio entre los diferentes responsables, este será resuelto por el Comité de Seguridad de la Información, prevaleciendo, mientras se resuelve, la decisión más restrictiva desde el punto de vista de la seguridad.

7. Gestión de riesgos

El análisis y la gestión de riesgos es parte esencial del proceso de seguridad. Se rige por las directrices siguientes: el análisis de riesgos se realiza conforme a la metodología documentada del sistema de

gestión, al menos una vez al año; se repite cuando se producen cambios significativos en la información tratada, en los servicios prestados o en la tecnología, y tras un incidente grave de seguridad; sus conclusiones orientan la selección de las medidas de seguridad y los planes de mejora; el riesgo residual resultante se eleva a la Dirección para su aceptación formal; y se consideran específicamente los riesgos derivados del tratamiento de datos personales, en coordinación con el Delegado de Protección de Datos.

8. Protección de datos personales

La Entidad trata datos de carácter personal, incluidos datos relativos a la salud (categoría especial del artículo 9 del RGPD). Aplicará las medidas técnicas y organizativas necesarias para cumplir el RGPD y la LOPDGDD, mantendrá actualizado el registro de actividades de tratamiento, realizará el análisis de riesgos de privacidad y, cuando proceda, la evaluación de impacto en la protección de datos (EIPD), y gestionará las violaciones de seguridad de datos personales conforme al protocolo establecido, con la participación del Delegado de Protección de Datos.

9. Estructura documental

El cuerpo normativo de seguridad de la Entidad se estructura en tres niveles: la normativa de seguridad, documentos de obligado cumplimiento que regulan el uso correcto de los sistemas (aprobada por el Comité de Seguridad de la Información); los procedimientos de seguridad, que describen las tareas operativas (aprobados por el Responsable de Seguridad); y las guías técnicas, recomendaciones y buenas prácticas de configuración y uso seguro. Esta Política prevalece sobre el resto de la documentación. Toda la documentación está disponible para 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 dirigida a todo el personal, y el personal con responsabilidades técnicas recibirá formación específica en seguridad de las tecnologías de la información. Es obligación de todo el personal conocer y cumplir esta Política y la normativa que la desarrolla, y se dejará constancia de las acciones formativas realizadas.

11. Terceras partes y proveedores

Cuando la Entidad contrate servicios tecnológicos o ceda información a terceros, estos serán partícipes de esta Política y de la normativa que les afecte, y se les exigirá el cumplimiento de los requisitos del ENS de forma proporcional al riesgo del servicio prestado. Los contratos incluirán cláusulas de confidencialidad, requisitos de seguridad y acuerdos de nivel de servicio, y cada proveedor designará un punto de contacto de seguridad para la coordinación operativa y la gestión de incidentes. Si un proveedor no puede satisfacer los requisitos exigidos, el Responsable de Seguridad emitirá un informe de riesgos que requerirá la aprobación de la Dirección con carácter previo a la contratación.

12. Gestión de incidentes

La Entidad dispone de un procedimiento formal para la detección, registro, notificación y resolución de los incidentes de seguridad, incluida la notificación a los organismos competentes cuando resulte exigible conforme a la ITS de Notificación de Incidentes de Seguridad y a la normativa de protección de datos. Todo el personal está obligado a comunicar sin dilación cualquier anomalía o sospecha de incidente a través de los canales establecidos.

13. Revisión de la Política

Esta Política se revisará con carácter ordinario una vez al año. La revisión será preparada por el Responsable de Seguridad, analizada por el Comité de Seguridad de la Información y, cuando comporte modificaciones, aprobada por la Dirección. Adicionalmente, se realizará una revisión extraordinaria cuando concurran cambios normativos, organizativos o tecnológicos significativos, cambios relevantes en los servicios prestados o en los riesgos identificados, incidentes graves de seguridad o conclusiones de auditoría que así lo aconsejen.

Cada revisión quedará registrada en el histórico de versiones de este documento, con indicación de la versión, la fecha, los cambios realizados y su aprobación. La versión vigente es la última aprobada por la Dirección, que deroga las anteriores y se difunde conforme al capítulo 14.

14. Entrada en vigor y difusión

La presente Política entra en vigor el día siguiente al de su aprobación y firma por la Dirección, derogando cualquier versión anterior. Se difundirá a todo el personal de la Entidad y a los terceros afectados a través de los canales internos establecidos, dejando constancia de cada acción de difusión en el registro del Anexo I. Las nuevas incorporaciones recibirán la Política como parte de su proceso de acogida.

Firmado por ***3573** JAVIER MOTA (R:
****8551*) el día 12/06/2026 con un certificado
emitido por AC Representación