ORG. 1 -Política de Seguridad

Historia de cambios

Version	Date	Comment
Current Version (v. 2)	**Jul 24, 2023 20:11**	**AV-Idrus**
v. 1	Jul 24, 2023 19:48	AV-Idrus

Tabla de Contenidos

Objetivo general

Establecer las directrices y principios que regirán el modo en que IDRUS gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) aplicando los requisitos normativos y de sus partes interesadas, dentro del marco regulatorio legal y vigente como el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad,

siendo su aplicación en el ámbito de la actividad de la organización para con los clientes que operan con el sector público y la exigencia en cuanto al establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

Misión y visión

Desde IDRUS, se establecen las siguientes estipulaciones a tener en cuenta:

Considerar la satisfacción de nuestros clientes como el objetivo fundamental de todas nuestras actividades, tanto de los pacientes, que son los usuarios finales de nuestro servicio, como de los demás clientes (servicios sanitarios públicos, compañías, mutuas, etc.).

Conseguir la tranquilidad y confianza de nuestros pacientes, y que se sientan lo más cómodos posible durante la realización de la prueba de resonancia magnética nuclear.

Emplear las mejores tecnologías disponibles en el mercado, desde la infraestructura de la propia resonancia hasta las herramientas informáticas para la transmisión de las imágenes, con el fin de conseguir un servicio de máxima calidad, cifrado y seguro.

Contar con un equipo humano competente y comprometido, que actúa siempre con ética, y que es el principal motor de nuestro servicio.

El cumplir los REQUISITOS APLICABLES, tanto los legales, prestando especial atención a la protección de datos personales, como otros que la organización suscribe, relativos a plazos, fiabilidad y calidad de la imagen, fundamentales para el mantenimiento de un buen nivel de calidad asistencial.

Marco Regulatorio

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, obliga a IDRUS a proteger los servicios que presta a sus partes interesadas en los que emplea medios electrónicos y que están documentados en el sistema de seguridad de la información.

IDRUS trata datos personales que deberán mantenerse inventariados por tratamiento, con el objeto de facilitar el control, la gestión y la protección de los mismos, aplicando medidas para cumplir con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos, equivalente a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

El ENS de IDRUS se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias correspondientes y llevando un registro y control de estas para el empleo adecuado de éstas en el desarrollo de las actividades.

Por lo tanto, el marco legal antes indicado estará en consonancia con el ENS de IDRUS, ya que uno de los grupos de controles de seguridad de este, es el cumplimiento de la legislación aplicable.

Funciones y/o responsabilidades de Seguridad de la información

El Comité de Seguridad de la Información formado por personal técnico de la organización, así como por el Administrador del Sistema y Responsable de la Seguridad de la Información centralizará los mecanismos de coordinación y resolución de conflictos que puedan surgir durante el desarrollo de la actividad y que se tratarán en las reuniones de dicho comité. Entre las funciones, responsabilidad y deberes principales a destacar por responsabilidad exigida, se encuentran las siguientes:

Responsable de Información del Sistema

- Será el encargado de aprobar la política y responsable de la autorización de sus modificaciones, así como de toda la información documentada del ENS de la entidad.
- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Asegurarse de que los controles de seguridad establecidos son cumplidos estrictamente.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.

- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurarse de que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.

Responsable de Seguridad de la Información

- Notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan, así como de determinar la categoría de seguridad del sistema y coordinar las acciones de implantación, mantenimiento y mejora del ENS de la organización.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad y según la información proporcionada por los Responsables de Servicio.
- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará al Responsable de Información y al Responsable de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por el Responsable de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

Responsable del Servicio

El Responsable del Servicio se encargará de gestionar los requisitos de seguridad de las actividades de su área para la prestación de los servicios. En concreto:

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Tiene la responsabilidad última del uso de la información que se haga en los servicios competentes y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios competentes.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del ENS, junto con el Responsable de Seguridad.
- El Responsable del servicio deberá informar al responsable de seguridad del nivel de seguridad aplicable a su servicio, para que este pueda definir y aplicar las medidas de seguridad acorde a las necesidades del servicio.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

Responsable del Sistema

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta los riesgos expuestos en la evaluación correspondiente.
- Tiene la responsabilidad del uso que se haga de la información y, por tanto, de su protección.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

Delegado de Protección de Datos

Será el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679) / Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, por lo que trabajará en coordinación con el Responsable de Seguridad de la Información y con el Responsable de Sistemas (Responsable del Sistema).

Resto del personal

Todo el personal de la entidad, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del ENS de http://Red.es en sus actividades laborales que afecta a su desempeño en seguridad de la información.

Procedimiento para la designación y renovación de responsabilidades.

Con una periodicidad bienal, se revisarán en comité de seguridad de la información las responsabilidades definidas en el ENS de cara a confirmar la continuidad de las personas que, a fecha de la celebración de dicha comisión, ostentan las responsabilidades correspondientes. Por lo tanto, será dicha comisión la que decida, al menos en la temporalidad definida, la continuidad o sustitución de dichas personas, si bien, podrán producirse modificaciones a lo largo de las reuniones periódicas que son llevadas a cabo.

Estructura y composición del Comité de Seguridad

La Dirección de IDRUS se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del ENS de la entidad, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad de la Información que tendrá los deberes y responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de la entidad.
- Asegurar que los recursos necesarios para el ENS estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
- Asegurar que el ENS consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

El detalle de las funciones específicas del Comité de Seguridad de la Información, se describirán en la Normativa de Organización de la Seguridad de la Información.

Directrices para la estructuración de la documentación de seguridad del sistema, gestión y acceso

El ENS de IDRUS se iniciará a partir del Análisis de Riesgos de Seguridad de los Sistemas de Información (incluyendo los derivados del tratamiento de datos personales), que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios y oportunidades de mejora para el tratamiento del riesgo y llevarlo a un nivel aceptable, tomando en cuenta el Contexto de la Organización.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá ser revisada y aprobada por el Comité de Seguridad de la Información, según el procedimiento de control de la documentación descrito en el Manual de Gestión.

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los requisitos mínimos definidos en dicho precepto, para incluirse en la documentación del sistema.

Además de aplicar los requisitos del propio Real Decreto 311/2012 como tal, se deberán utilizar las Guías CCN-STIC de Seguridad que son las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de seguridad de las organizaciones, especialmente la Serie CCN-STIC-800 que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de este modo, al cumplimiento de los requisitos del sistema de gestión de IDRUS.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del sistema de seguridad de la información en todo su alcance, de manera que se puedan establecer acciones correctivas que permitan mejorar la eficacia del mismo.

Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad.

Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

Directrices de tratamiento

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo las inversiones que considere necesarias para buen desarrollo del sistema de seguridad de la información.

Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por la persona responsable de esa información y servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

Necesidad de realizar o actualizar las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad programada en el sistema de gestión, además este se realizará:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.