

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

ÍNDICE

- 1. INTRODUCCIÓN**
- 2. ALCANCE**
- 3. MISIÓN**
- 4. MARCO NORMATIVO**
- 5. ROLES: FUNCIONES Y RESPONSABILIDADES**
 - 5.1. RESPONSABLE DE INFORMACIÓN
 - 5.2. RESPONSABLE DEL SERVICIO
 - 5.2. RESPONSABLE DE SEGURIDAD
 - 5.4. RESPONSABLE DEL SISTEMA
- 6. GESTIÓN DE VULNERABILIDADES**
- 7. DATOS DE CARACTER PERSONAL**
- 8. OBLIGACIONES DEL PERSONAL**
- 9. TERCERAS PARTES**
- 10. HISTORIAL DE REVISIONES**

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

1. INTRODUCCIÓN

La Dirección de **AGENOR MANTENIMIENTOS, S.A., Mantenimiento, S.A.**, entiende que el sistema de información que da soporte a la prestación de sus actividades es un activo fundamental.

Este sistema da soporte a los servicios específicos (definidos claramente según las actividades que **AGENOR Mantenimientos, S.A.**, realiza):

Dado el impacto que tiene este sistema en el desarrollo y prestación de servicios, la Organización mantiene un firme compromiso con la protección de sus activos más significativos. Este compromiso forma parte de una estrategia orientada a la continuidad del negocio, la gestión de riesgos y el fortalecimiento de una cultura sólida de seguridad de la información.

Desde su constitución, el objetivo ha sido prestar un servicio de alta calidad a sus clientes, cumpliendo con los requisitos establecidos para garantizar la máxima satisfacción con nuestros servicios, a la vez que se asegura la confidencialidad y seguridad de la información.

La satisfacción de nuestros clientes y la confidencialidad de la información son la piedra angular de nuestra política. Entendemos la satisfacción como el cumplimiento eficiente de los compromisos contractuales, así como el esfuerzo por cumplir con las expectativas no contractuales derivadas de las necesidades descubiertas en la ejecución del servicio y las que nos comunican nuestros clientes.

Como punto fundamental de esta política, **AGENOR MANTENIMIENTOS, S.A.**, ha establecido la implantación, operación y mantenimiento de un Marco de Seguridad Integral, alineado con los requisitos del Esquema Nacional de Seguridad (ENS), conforme al Real Decreto 311/2022, y la Directiva NIS2, garantizando la gestión de riesgos, la resiliencia y la continuidad del servicio.

Este marco de seguridad se fundamenta en los siguientes principios clave:

- **Enfoque basado en riesgos:** Gestionar de manera sistemática y proactiva las amenazas y vulnerabilidades, asegurando una defensa en profundidad que minimice los riesgos y fortalezca la protección de la información frente a amenazas cibernéticas.
- **Cumplimiento normativo:** Garantizar la conformidad con el ENS y la NIS2, así como con los requisitos legales y reglamentarios aplicables a la seguridad de la información.
- **Mejora continua de la ciberseguridad:** Promover la resiliencia organizativa mediante la supervisión, auditoría y actualización constante de los controles de seguridad.
- **Fortalecimiento de la seguridad en la cadena de suministro:** Exigir a terceros el cumplimiento de estándares equivalentes en materia de seguridad de la información y ciberseguridad.

Como parte de este compromiso, todo el personal, incluidos terceros y proveedores críticos, recibirá formación y concienciación en seguridad de la información de acuerdo con las exigencias del ENS y la Directiva NIS2, estableciendo mecanismos de reporte obligatorio ante incidentes de seguridad.

Los pilares fundamentales de esta política se resumen en las siguientes directrices, que servirán de base para el establecimiento de los objetivos anuales de **AGENOR MANTENIMIENTOS, S.A.**:

1. **Lograr que la seguridad de la información y el respeto a los datos personales sean una constante:**
Preservar la confidencialidad de la información, evitando su divulgación y el acceso por personas no autorizadas.
Mantener la integridad de la información, asegurando su exactitud y evitando su deterioro.
Garantizar la disponibilidad de la información en todos los soportes y cuando sea necesaria.
2. **Cumplimiento de los requisitos legales y reglamentarios:**
Cumplir con todos los requisitos legales y reglamentarios aplicables, así como con los compromisos adquiridos, evaluando continuamente dicho cumplimiento en todas las áreas de actividad.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

3. **Continuidad del negocio:**
Implementar y mantener un plan de continuidad que permita recuperarse de un desastre en el menor tiempo posible.
4. **Formación y concienciación continua:**
Velar por la continua y permanente actualización de nuestros recursos, tanto tecnológicos como humanos. Fomentar políticas de formación continua que permitan a nuestros empleados avanzar al ritmo del sector y promover la conciencia sobre la seguridad de la información.
5. **Responsabilidad del personal:**
Todos los empleados recibirán formación periódica en seguridad de la información conforme a las directrices del ENS y la NIS2, siendo responsables del cumplimiento de sus obligaciones en materia de seguridad y notificando cualquier incidente de seguridad detectado.
6. **Mejora continua del sistema de gestión:**
Asegurar la mejora continua del sistema de seguridad de la información, manteniéndolo eficaz y eficiente, para garantizar el compromiso con los clientes y optimizar la organización interna, en particular en lo que respecta al tratamiento de la información de los clientes.
7. **Gestión de incidencias y riesgos:**
Gestionar adecuadamente todas las incidencias de seguridad, evaluando de manera rigurosa los riesgos de la organización, y analizando los posibles riesgos de los procesos y activos de información para prevenir desviaciones y minimizar posibles no conformidades.
8. **Comunicación y cumplimiento de la política:**
Comunicar a todo el personal y a los terceros que trabajen en nombre de AGENOR MANTENIMIENTOS, S.A., la obligación de cumplir con esta política, incluyendo contratistas y visitantes a nuestras instalaciones.
9. **Satisfacción del cliente y cumplimiento de requisitos:**
Asegurar la satisfacción de los clientes basándonos en un trato correcto y en un esfuerzo continuo para ofrecer un servicio que cumpla con sus requisitos y con nuestros compromisos de actualización y mejora.
10. **Protección de la información, personas y recursos:** Establecer procesos operacionales que salvaguarden la información, los datos, las aplicaciones, y los recursos humanos y materiales de la organización, garantizando la seguridad integral.
11. **Revisión de objetivos y participación del personal:**
Establecer y revisar regularmente los objetivos de seguridad de la información, alineados con los compromisos asumidos en esta política, fomentando la participación activa de todo el personal en la consecución de los objetivos.

La Dirección General valora especialmente la disponibilidad, confidencialidad e integridad de la información, tanto propia como de nuestros clientes, como criterios principales para la estimación de riesgos y la toma de decisiones.

2. ALCANCE

La organización establece esta Política de Seguridad de la Información para los sistemas de información y servicios esenciales que estén dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS) y la Directiva NIS2, asegurando la protección de activos críticos y la resiliencia operativa.

Servicios Específicos:

El alcance de esta política se extiende a:

“Los sistemas de información que dan soporte a la actividad desarrollada en el mantenimiento integral de los equipos electromédicos, instalaciones generales y oficina técnica de apoyo a los centros sanitarios”

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

Ámbito de Aplicación de la Política:

La Política de Seguridad de la Información abarca todos los procesos, activos y servicios mencionados, alineándose con los principios y requisitos del ENS y NIS2. Esto incluye:

1. Sistemas de Información y Procesos Relacionados:

- Todos los sistemas de información que soportan los servicios mencionados estarán sujetos a las medidas de seguridad exigidas en el ENS, garantizando la **confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad** de la información, conforme a los requisitos establecidos en el RD 311/2022 y Reglamento UE 2690/2024.

2. Actividades de Soporte:

- Además de los servicios directamente vinculados con los sistemas de información, la política cubre **actividades de apoyo esenciales**, tales como la gestión de incidentes, el mantenimiento, la actualización, la protección de activos tecnológicos, y la supervisión de proveedores críticos.

3. Identificación de Activos y Procesos Críticos:

- Se identificarán y gestionarán los **activos de información críticos** asociados a cada servicio, aplicando un proceso de **evaluación y tratamiento de riesgos**, conforme a las categorías de seguridad establecidas en el Anexo I del ENS.

4. Cumplimiento de Requisitos Legales y Normativos:

- El alcance de esta política garantiza el cumplimiento de los **requisitos legales, reglamentarios y contractuales** aplicables en materia de seguridad de la información, conforme a la legislación española y europea, en alineación con el ENS y la NIS2.

5. Gestión y Mejora Continua de la Seguridad:

- La organización se compromete a la **mejora continua de los controles y procedimientos de seguridad**, mediante la **revisión periódica de riesgos**, la **gestión de incidentes** y el establecimiento de **planes de contingencia** para garantizar la continuidad de las operaciones.

6. Declaración de Aplicabilidad ENS:

- Se establecerá y mantendrá una **Declaración de Aplicabilidad** alineada con el ENS definiendo las **medidas de seguridad aplicables** a los sistemas de información cubiertos por esta política.

Extensión de la Política:

El alcance de esta política se aplica a todos los **sistemas de información, procesos y actividades de la Organización** que den soporte a los servicios mencionados, sin limitación alguna. También se extiende a todos los **empleados y partes interesadas**, quienes deberán cumplir con los principios de seguridad de la información, los procedimientos operacionales y los requisitos legales y normativos aplicables.

3. MISIÓN

La misión de **AGENOR MANTENIMIENTOS, S.A.**, es un proyecto basado en las personas que trabajando en equipo lograr una Organización fuerte en la que proporcionemos a nuestros clientes, respuestas eficaces y eficientes en la gestión de los servicios que ofrecemos, ayudándoles a consolidar sus actividades.

La Organización para cumplir con esta misión, se compromete a:

- **Garantizar la seguridad de la información:** Adoptar un enfoque integral en la gestión de la seguridad de la información, basado en los principios y requisitos establecidos en el Esquema Nacional de Seguridad (ENS) (RD 311/2022) y la Directiva NIS2, con el objetivo de proteger la información de los clientes y los datos internos de la organización frente a amenazas y vulnerabilidades.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

- **Asegurar la gestión y protección de activos críticos:** Aplicar medidas de seguridad adecuadas para la protección de los activos críticos de información, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, en cumplimiento con el ENS y la NIS2.

- **Fomentar la mejora continua:** Implementar procesos de evaluación y revisión continua de la seguridad de la información, alineados con el ENS y la NIS2, para garantizar la adaptación a nuevas amenazas, regulaciones y necesidades del negocio.

- **Concienciar y capacitar al personal:** Desarrollar programas de formación y concienciación en seguridad de la información para todo el personal, fomentando una cultura de ciberseguridad y asegurando el cumplimiento de las directrices del ENS y la NIS2.

- **Cumplir con los requisitos legales y regulatorios:** Garantizar que todas las actividades y servicios, cumplen con las obligaciones legales, regulatorias y contractuales en materia de seguridad de la información, en alineación con el Esquema Nacional de Seguridad (ENS) y la Directiva NIS2.

- **Proteger la continuidad del negocio:** Implementar planes de continuidad de negocio y recuperación ante desastres, asegurando la resiliencia de los sistemas de información y servicios esenciales frente a incidentes de ciberseguridad, en cumplimiento con el ENS y la NIS2.

En resumen, la Organización, se dedica a ofrecer soluciones seguras e innovadoras a sus clientes, garantizando la protección de la información mediante un enfoque integral alineado con los estándares del Esquema Nacional de Seguridad (ENS) y la Directiva NIS2.

Esto nos permite ser un socio confiable, capaz de optimizar los procesos de nuestros clientes mientras garantizamos su seguridad frente a los riesgos inherentes al tratamiento de la información.

4. MARCO NORMATIVO

AGENOR MANTENIMIENTOS, S.A., se compromete a cumplir con toda la normativa aplicable a su actividad, incluyendo legislación general y específica en materia de seguridad de la información, ciberseguridad y protección de datos. A continuación, se destacan las principales normativas que rigen la seguridad de la información en la organización:

Normativa Nacional

- **Real Decreto 311/2022, de 3 de mayo:** Regula el Esquema Nacional de Seguridad (ENS), estableciendo principios y requisitos de ciberseguridad para el sector público y las entidades del sector privado que estén sujetas a esta regulación.
- **Ley 40/2015, de 1 de octubre:** Regula el Régimen Jurídico del Sector Público, abordando aspectos clave sobre la administración digital y la seguridad de la información.
- **Ley 39/2015, de 1 de octubre:** Establece el Procedimiento Administrativo Común de las Administraciones Públicas, promoviendo la digitalización y la accesibilidad en los procesos administrativos.
- **Real Decreto-ley 12/2018, de 7 de septiembre:** Regula la seguridad de redes y sistemas de información, estableciendo medidas para la protección de infraestructuras críticas y servicios esenciales.
- **Real Decreto 43/2021, de 26 de enero:** Desarrolla el Real Decreto-ley 12/2018, especificando medidas de ciberseguridad y las obligaciones de notificación de incidentes para operadores de servicios esenciales y proveedores de servicios digitales.
- **Ley Orgánica 3/2018, de 5 de diciembre:** Relativa a la Protección de Datos Personales y la garantía de los derechos digitales, complementa y desarrolla el Reglamento General de Protección de Datos (RGPD).

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

- **Ley 9/2014, de 9 de mayo:** Ley General de Telecomunicaciones, regula el acceso y prestación de servicios de comunicaciones electrónicas y establece derechos y obligaciones en materia de seguridad y privacidad.
- **Ley 34/2002, de 11 de julio (LSSI-CE):** Regula los servicios de la sociedad de la información y el comercio electrónico, incluyendo obligaciones en materia de seguridad y protección de datos.
- **Guías CCN-STIC (Serie 800):** Documentos técnicos del Centro Criptológico Nacional (CCN) que establecen recomendaciones para la implementación del ENS y buenas prácticas en seguridad de la información.

Normativa Europea

- **Directiva (UE) 2022/2555 (NIS2):** Refuerza los requisitos de seguridad para operadores de servicios esenciales y empresas de sectores estratégicos, estableciendo obligaciones en materia de gestión de riesgos, notificación de incidentes y supervisión de ciberseguridad.
- **Reglamento (UE) 2016/679 (RGPD):** Relativo a la protección de datos personales en la Unión Europea, establece principios y requisitos para el tratamiento de información personal.
- **Reglamento (UE) 910/2014 (eIDAS):** Regula la identificación electrónica y los servicios de confianza en transacciones electrónicas dentro del mercado interior.
- **Reglamento (UE) 2019/881 (Reglamento de Ciberseguridad):** Fortalece la ciberseguridad en la UE y establece un marco para la certificación de la seguridad de las TIC, además de reforzar el papel de la Agencia de la Unión Europea para la Ciberseguridad (ENISA).
- **Reglamento (UE) 2690/2024:** Por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.

Otras Regulaciones Relevantes

- **Ley 25/2007, de 18 de octubre:** Regula la conservación de datos generados o tratados en comunicaciones electrónicas para fines de seguridad y defensa.
- **Real Decreto Legislativo 1/1996, de 12 de abril:** Regula la propiedad intelectual, incluyendo aspectos de protección de software y derechos digitales.
- **Real Decreto 424/2005, de 15 de abril:** Aunque con menor relevancia en la actualidad, establece condiciones para la prestación de servicios de comunicaciones electrónicas y protección de los usuarios.

En el marco de Certificaciones

- ISO 9001:2015, Sistemas de Gestión de la Calidad
- ISO 14001:2015, Sistemas de Gestión Ambiental
- ISO 13485:2013, Sistemas de Gestión de la Calidad de productos sanitarios
- ISO 45001:2018, Sistemas de Gestión de seguridad y salud en el trabajo.
- Norma UNE-EN ISO/IEC 27001:2017 - Sistemas de Gestión de Seguridad de la Información (SGSI) - Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

- UNE-EN ISO/IEC 27002:2017 -Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)

5. ROLES: FUNCIONES Y RESPONSABILIDADES

5.1. RESPONSABLE DE INFORMACIÓN

El Responsable de Información es el encargado de establecer los requisitos de seguridad para la información tratada en los sistemas de la organización, asegurando su adecuada clasificación, protección y cumplimiento normativo.

Funciones y Responsabilidades:

- Definir los requisitos de seguridad de la información, conforme a los criterios de categorización del Anexo I del ENS, asegurando su correcta clasificación y protección.
- Aprobar los niveles de seguridad de la información, garantizando su alineación con los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad del ENS.
- Participar en el Comité de Seguridad de la Información, contribuyendo a la definición y supervisión de estrategias de seguridad.
- Supervisar la protección de los activos de información, asegurando la implementación de controles adecuados y su cumplimiento.
- Garantizar el cumplimiento de la normativa vigente en la gestión de la información, incluyendo derechos de acceso y protección de datos.
- Coordinar con el Responsable de Seguridad la gestión de riesgos, promoviendo medidas preventivas y correctivas ante incidentes.
- Mantener actualizados los registros de gestión de la información, garantizando la trazabilidad de las decisiones adoptadas.

5.2. RESPONSABLE DEL SERVICIO

El Responsable del Servicio define y supervisa los requisitos de seguridad de los servicios prestados, garantizando su resiliencia y alineación con ENS y NIS2.

Funciones y Responsabilidades:

- Determinar los requisitos de seguridad de los servicios prestados, conforme al Anexo I del ENS, asegurando la identificación y protección de los servicios esenciales.
- Aprobar los niveles de seguridad de los servicios, alineándolos con los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Participar en el Comité de Seguridad de la Información, colaborando en la definición de estrategias de seguridad.
- Garantizar la seguridad de los activos asociados a los servicios, implementando controles que aseguren su continuidad y resiliencia operativa.
- Supervisar el cumplimiento de la normativa vigente y derechos de usuarios/clientes.
- Coordinar con el Responsable de Seguridad la gestión de riesgos en la prestación de servicios, promoviendo medidas de mitigación.
- Supervisar el cumplimiento de acuerdos con proveedores críticos, asegurando que cumplen con ENS y NIS2.
- Mantener registros actualizados sobre la seguridad de los servicios, asegurando la trazabilidad de decisiones y acciones.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

5.3. RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad garantiza la aplicación de las medidas de seguridad establecidas en el Anexo II del ENS, supervisando su implementación y asegurando la alineación con NIS2.

Gestión de Seguridad de la Información:

- Determinar las decisiones de seguridad necesarias para el cumplimiento del ENS y NIS2.
- Mantener la seguridad de la información y servicios prestados, asegurando su alineación con la Política de Seguridad de la Información.
- Elaborar, actualizar y mantener la Declaración de Aplicabilidad del ENS, asegurando su alineación con la normativa vigente y su revisión periódica. Será responsable de su supervisión continua, incluyendo la documentación de los controles implementados, las justificaciones de exclusión y su aprobación por la Dirección
- Desarrollar políticas, normativas y procedimientos de seguridad, alineados con ENS y NIS2.
- Supervisar la ejecución de auditorías de seguridad periódicas, asegurando su cumplimiento normativo.

Supervisión de la gestión de vulnerabilidades:

- Supervisar el proceso de gestión de actualizaciones y parches de seguridad, asegurando que se cumplen los plazos establecidos y que se priorizan las actualizaciones críticas.
- Realizar revisiones periódicas del estado de parches y actualizaciones en los sistemas de información, identificando posibles brechas de seguridad.
- Coordinar con el Responsable del Sistema la implementación de medidas de mitigación para vulnerabilidades no parcheadas, como la segmentación de redes o la aplicación de controles de acceso adicionales.
- Notificar a la Dirección cualquier retraso significativo en la aplicación de parches críticos, junto con una evaluación de riesgos y un plan de acción.

Gestión de Incidentes y Relación con Autoridades:

- Gestionar el Registro de Incidentes y Riesgos, asegurando su documentación y análisis de causas.
- Coordinar la respuesta ante ciberincidentes, asegurando la correcta aplicación del Plan de Respuesta a Incidentes.
- Notificar incidentes graves a CCN-CERT o INCIBE en un plazo máximo de 24 horas desde su detección, según lo establecido en la Directiva NIS2 y el RD 311/2022.
- Coordinar con el CSIRT de referencia (CCN-CERT o INCIBE) en la gestión y mitigación de incidentes.

Supervisión de Terceros y Auditorías:

- Evaluar el cumplimiento de seguridad en proveedores críticos, asegurando su adecuación a ENS y NIS2.
- Coordinar auditorías de seguridad en terceros, verificando la aplicación de controles de seguridad contratados.

Responsabilidades compartidas con el Responsable del Sistema:

♦ Supervisión y Aplicación del ENS y NIS2

- Asegurar que la clasificación de activos y su categorización cumplen con ENS (Anexo I RD 311/2022).
- Coordinar la actualización de controles y medidas de seguridad conforme a ENS y NIS2.

♦ Gestión y Control de Accesos

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

- Definir y aplicar controles de acceso adecuados a la clasificación de la información.
- Supervisar que las configuraciones de seguridad cumplen con ENS y NIS2.

♦ **Participación en el Comité de Seguridad de la Información**

- Convocar y dirigir reuniones, asegurando el seguimiento de medidas de seguridad.
- Aportar información clave para la toma de decisiones en seguridad.

5.4. RESPONSABLE DEL SISTEMA

El Responsable del Sistema es el encargado de gestionar y supervisar el ciclo de vida del sistema de información, asegurando su alineación con las medidas de seguridad del ENS (RD 311/2022) y la Directiva NIS2.

Gestión del Ciclo de Vida del Sistema:

- Desarrollar, operar y mantener el sistema de información, asegurando su alineación con ENS y NIS2.
- Definir la topología y gestión del sistema, estableciendo criterios de uso y servicios disponibles.
- Determinar la configuración de hardware y software, asegurando su cumplimiento con ENS.
- Aprobar modificaciones en la configuración del sistema, garantizando que cumplen con ENS y NIS2.
- Implementar y controlar medidas de seguridad en el sistema, integrándolas con la estrategia global de seguridad.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.

Gestión de actualizaciones y parches de seguridad:

- Establecer un proceso formal para la identificación, evaluación e implementación de actualizaciones y parches de seguridad en todos los sistemas de información.
- Asegurar que las actualizaciones críticas se implementen en un plazo máximo de 30 días desde su publicación, o en un plazo menor si el riesgo asociado lo requiere.
- Mantener un inventario actualizado de todos los sistemas y software, incluyendo versiones y fechas de última actualización.
- Realizar pruebas de compatibilidad antes de implementar actualizaciones en entornos productivos, para minimizar el riesgo de interrupciones en los servicios.
- Coordinar con el Responsable de Seguridad la evaluación de riesgos asociados a vulnerabilidades no parcheadas y la implementación de medidas compensatorias cuando no sea posible aplicar un parche de inmediato.

Supervisión Técnica de Seguridad:

- Aplicar medidas de seguridad en desarrollo, instalación y pruebas.
- Elaborar y actualizar la documentación de seguridad del sistema, incluyendo la evaluación de riesgos conforme a ENS y NIS2.
- Coordinar la supervisión de logs de seguridad y monitorización, asegurando su correcta implementación.
- Gestionar configuraciones y auditorías técnicas, verificando el cumplimiento de requisitos ENS y NIS2.

Responsabilidades compartidas con el Responsable de Seguridad:

♦ **Cumplimiento del ENS y NIS2**

- Supervisar la actualización de controles y categorización de activos conforme a ENS y NIS2.
- Realizar análisis y gestión de riesgos del sistema, conforme al Anexo I del ENS.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

♦ **Gestión de Incidentes y Continuidad**

- Establecer planes de contingencia y emergencia, realizando simulaciones conforme a ENS y NIS2.
- Acordar la suspensión de servicios o accesos si se detectan deficiencias graves de seguridad, en coordinación con el Responsable de Seguridad.

♦ **Participación en el Comité de Seguridad**

- Formar parte del Comité de Seguridad de la Información.
- Participar en la revisión y actualización de medidas de seguridad aplicables al sistema de información.

6. GESTIÓN DE VULNERABILIDADES

1. Identificación y Evaluación

AGENOR MANTENIMIENTOS, S.A., establecerá un proceso periódico de detección, análisis y gestión de vulnerabilidades en sus sistemas de información.

Se emplearán herramientas de análisis de vulnerabilidades, así como pruebas de penetración basadas en estándares reconocidos. Los resultados de estas pruebas y revisiones serán documentados y revisados periódicamente.

El Responsable de Seguridad supervisará estos procesos, asegurando su alineación con los requisitos del ENS y la Directiva NIS2.

2. Corrección y Mitigación

Las vulnerabilidades detectadas serán evaluadas y clasificadas según su criticidad e impacto en la organización.

Plazos de corrección:

Críticas: Corrección en un máximo de 30 días.

Altas: Corrección en un máximo de 60 días.

Medias o bajas: Corrección en un máximo de 90 días.

Estos plazos podrán ajustarse en función de la evolución de las amenazas y el contexto de seguridad de la organización.

Se priorizarán las vulnerabilidades críticas y de alto riesgo, aplicando medidas de mitigación inmediatas (como segmentación de redes, restricciones de acceso o reforzamiento de monitorización) en caso de que no puedan corregirse en el plazo establecido.

El Responsable de Seguridad garantizará que las actualizaciones de seguridad y parches se implementen de manera controlada, previa evaluación de riesgos, evitando impactos negativos en los sistemas.

3. Supervisión y Mejora Continua

Se realizará una revisión anual del proceso de gestión de vulnerabilidades, con la participación del Comité de Seguridad, para identificar áreas de mejora y optimización.

Esta revisión incluirá:

Análisis de métricas, como el porcentaje de vulnerabilidades corregidas en plazo.

Evaluación del cumplimiento de plazos de corrección y su efectividad.

Evaluación de tendencias de amenazas para ajustar procedimientos.

Actualización de estrategias basadas en lecciones aprendidas.

Todas las vulnerabilidades detectadas, junto con las acciones tomadas, serán registradas en el Registro de Incidentes y Riesgos, asegurando trazabilidad y supervisión efectiva.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

4. Notificación de Vulnerabilidades

Todo el personal deberá reportar de inmediato cualquier vulnerabilidad o anomalía detectada en los sistemas.

Plazos internos de notificación:

Vulnerabilidades críticas: Notificación interna en un máximo de 24 horas.

Vulnerabilidades de alto riesgo: Notificación interna en un máximo de 48 horas.

Estos plazos podrán ajustarse en función de la criticidad de las vulnerabilidades y el contexto de seguridad de la organización.

En caso de vulnerabilidades críticas que puedan comprometer la seguridad de la organización, AGENOR MANTENIMIENTOS, S.A., notificará a las autoridades competentes (CCN-CERT o INCIBE) conforme a:

- Anexo II del ENS: Requiere implementar medidas de protección contra vulnerabilidades y gestionar su mitigación dentro del marco de seguridad definido.
- Artículo 25 del ENS (RD 311/2022): Establece la necesidad de gestionar incidentes de seguridad, incluyendo la detección, análisis y respuesta ante vulnerabilidades que puedan generar un impacto grave.
- Directiva NIS2 (Artículo 23.4): Establece la obligación de notificar incidentes significativos en un plazo máximo de 24 horas a la autoridad competente. Obliga a notificar a la autoridad competente únicamente en casos donde el incidente tenga un impacto significativo en la prestación de servicios esenciales.

La evaluación del impacto y la decisión de notificación serán responsabilidad del **Responsable de Seguridad**, en coordinación con el Comité de Seguridad de la Información

7. DATOS DE CARACTER PERSONAL

AGENOR MANTENIMIENTOS, S.A., trata datos de carácter personal y mantiene un "registro de actividades de tratamiento", accesible únicamente para personas autorizadas. Este registro recoge los tratamientos realizados, los datos afectados y los responsables de su gestión.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa vigente para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, conforme al Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y las medidas establecidas en el Esquema Nacional de Seguridad (ENS).

AGENOR MANTENIMIENTOS, S.A., cuenta con un **Responsable de Protección de Datos (RPD/DPO)**, cuya función es garantizar el cumplimiento de la normativa en materia de protección de datos personales, conforme al RGPD y la LOPDGDD. El RPD/DPO actúa como punto de contacto con la Agencia Española de Protección de Datos (AEPD) y asesora a la organización en la aplicación de medidas para un tratamiento seguro de los datos personales.

8. OBLIGACIONES DEL PERSONAL

Todos los trabajadores de **AGENOR MANTENIMIENTOS, S.A.**, tienen la obligación de conocer y cumplir con esta Política de Seguridad de la Información. El Comité de Seguridad garantizará que la información sobre las responsabilidades en materia de seguridad llegue a los empleados de manera clara y accesible.

Se establecerá un programa de concienciación continua sobre seguridad de la información, dirigido a todos los miembros de la Organización, con especial atención a los nuevos empleados.

El personal con funciones en el uso, operación o administración de sistemas TIC dentro del alcance del ENS deberá recibir formación específica en seguridad antes de asumir sus responsabilidades. Esta formación será obligatoria tanto en la asignación inicial como en caso de cambios de puesto o nuevas funciones que impliquen el manejo de sistemas críticos o información sensible.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

9. TERCERAS PARTES

Las terceras partes que accedan a los sistemas de **AGENOR MANTENIMIENTOS, S.A.**, o gestionen información de la organización deberán cumplir con los requisitos de seguridad equivalentes a los establecidos en el ENS y la Directiva NIS2.

Para ello, deberán:

- Firmar acuerdos de confidencialidad y protección de la información, garantizando el cumplimiento de la normativa aplicable.
- Aplicar medidas de seguridad alineadas con ENS y NIS2, incluyendo controles técnicos, organizativos y de gestión de riesgos adecuados.
- Someterse a auditorías periódicas cuando sea aplicable, para verificar su alineación con las medidas de seguridad exigidas.

Proveedores Críticos: Los **proveedores críticos** son aquellos que desempeñan funciones esenciales para la organización, como proveedores de servicios que soportan sistemas clave, gestionan información sensible o están involucrados en procesos críticos para la continuidad del negocio. Estos proveedores estarán sujetos a requisitos adicionales de seguridad, debiendo demostrar el cumplimiento de las medidas establecidas en el ENS y la Directiva NIS2, y podrán ser objeto de supervisión por parte del Responsable de Seguridad. La supervisión de proveedores críticos debe realizarse periódicamente mediante auditorías o revisiones de cumplimiento, en línea con ENS y NIS2.

Cuando la Organización utilice servicios de terceros o ceda información a terceros, estos deberán adherirse a esta Política de Seguridad. Las terceras partes podrán desarrollar sus propios procedimientos operativos para cumplir con los requisitos exigidos, siempre que garanticen un nivel de seguridad equivalente o superior al establecido en la normativa aplicable.

Si una tercera parte no puede satisfacer alguno de los requisitos de seguridad establecidos en esta Política, el Responsable de Seguridad deberá elaborar un informe detallando los riesgos asociados y las medidas compensatorias necesarias para minimizar su impacto.

10. HISTORIAL DE REVISIONES

Esta Política será revisada al menos una vez al año, o siempre que se produzcan cambios normativos, tecnológicos o estratégicos que impacten en la seguridad de la información. La revisión será realizada por la Dirección, en coordinación con el Responsable de Seguridad y el Comité de Seguridad de la Información.

Se documentarán todas las modificaciones realizadas, justificando los cambios en base a auditorías, incidentes de seguridad, actualizaciones normativas o evaluaciones de riesgos. La **Declaración de Aplicabilidad del ENS** será revisada en cada actualización significativa, asegurando su coherencia con los controles de seguridad aplicados y su correcta trazabilidad.

La versión actualizada de la Política será comunicada a todo el personal de la organización y estará disponible para su consulta por las partes interesadas bajo solicitud.

Revisión	Fecha	Razón Modificación
1.0	02/03/2025	Creación del Documento

La Dirección se asegura que la Política de Seguridad de la Información es entendida, implantada y mantenida al día en todos los niveles de la Organización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código documento:	PO-001. Rev.1
		Fecha aprobación:	02/03/2025

En Tudela (Navarra) a 02 de Marzo de 2025


 T. 948 84 84 27 - F. 948 84 86 17
 agenor@agenormantenimientos.com
 www.agenormantenimientos.com

Fdo.: Sr. Rodríguez, J.A.
 Dirección