Omniloy

Your medical copilot

Sistema de Gestión Integrado

OM - SGENS – Política de Seguridad bajo ENS

Revisión: 1.1

Última revisión: 27/01/2026

ÍNDICE

2. Aprobación y entrada en vigor

El texto fue aprobado por primera vez el día 27 de enero de 2026 por la Dirección.

Esta Política de Seguridad de la Información bajo el Esquema Nacional de Seguridad es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

3. Introducción

OMNILOY es la marca comercial a la que pertenecen **Omniloy S.L.**

OMNILOY depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Esta política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II del ENS y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los diferentes departamentos y Unidades de Negocio de **OMNILOY** deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Todos los integrantes de **OMNILOY** deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Todos los integrantes de **OMNILOY** deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo correspondiente.

3.1. Prevención

Todos los integrantes de **OMNILOY** deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

Para ello deben implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política, todos los integrantes de **OMNILOY** deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo correspondiente.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo correspondiente del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3. Respuesta

Todos los integrantes de **OMNILOY** deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

3.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, todos los integrantes de **OMNILOY** deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4. Alcance

El Sistema de Información de **OMNILOY** (Omniloy S.L) que soporta los servicios IT de implantación, soporte y mantenimiento de aplicaciones de Inteligencia Artificial, conforme con la categoría y la declaración de aplicabilidad vigente.

5. Propósito, Misión, Visión y Valores

- **Propósito**
  Mejorar el acceso y la experiencia sanitaria, ayudando a que cada interacción entre paciente y sistema de salud sea más rápida, segura y útil, mediante agentes de IA confiables que reducen fricción operativa y aumentan la calidad del servicio.
- **Misión**
  Diseñar, desplegar y operar agentes de IA (voz y texto) que automaticen de forma segura procesos clínicos, integrándose con los sistemas del cliente nativamente y cumpliendo los estándares mas altos de calidad y seguridad.
- **Visión**
  Ser la plataforma de referencia para agentes de IA confiables en salud: escalable internacionalmente, auditables, interoperables y reconocidos por elevar la eficiencia de los centros y la satisfacción de pacientes, manteniendo siempre la seguridad, la privacidad y la calidad asistencial como principios no negociables.
- **Valores:**
  - 1. **Seguridad y privacidad por diseño**: Protegemos datos y sistemas desde el diseño, minimización, control de acceso, trazabilidad, y arquitectura alineada con buenas prácticas de seguridad.
  - 2. **Calidad y cumplimiento:** Operamos con mentalidad de producto sanitario, procesos, evidencias, mejora continua y orientación a auditorías y requisitos normativos.
  - 3. **Confiabilidad y transparencia**: Sistemas auditables, explicables donde aplique, con monitorización y métricas claras.
  - 4. **Enfoque clínico y centrado en el paciente:** La utilidad real y la seguridad del paciente guían decisiones: lenguaje claro, accesibilidad y reducción de errores operativos.

6. Marco normativo

OMNILOY ha establecido un procedimiento para la identificación de la legislación vigente que permite identificar los cambios normativos aplicables, así como la generación de un registro que permite conocer el estado de la normativa jurídica actualizado que indica la situación en que se encuentran las normas relacionadas con la ciberseguridad y protección de datos.

Marco normativo establecido por las principales normas en relación con la ciberseguridad y la protección de datos:

- **Real Decreto 311/2022, de 3 de mayo**, por el que se regula el Esquema Nacional de Seguridad. Deroga al Real Decreto 3/2010, de 8 de enero BOE de 29 de enero de 2010.
- **Ley Orgánica 3/2018, de 5 de diciembre,** de Protección de Datos Personales y garantía de los derechos digitales.
- **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.
- **Real Decreto-ley 12/2018, de 7 de septiembre**, de seguridad de las redes y sistemas de la información.

Adicionalmente, el resto del marco legislativo, bajo el que Omniloy desarrolla las actividades dentro del alcance se encuentra disponible en el documento de registro de la legislación vigente.

7. Organización de la seguridad

7.1. Roles funciones y responsabilidades

7.1.1. Responsable de Seguridad (de la información)

Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Las dos funciones esenciales del Responsable de Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Además de ello:

- Elaborar y proponer para aprobación por la organización las Políticas de Seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las Políticas de Seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- ~~A~~probar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.

7.1.2. Responsable del Sistema (CIO)

Tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

- Definir las políticas de acceso de usuarios al Sistema.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

7.1.3. Responsable de la información

Tiene las siguientes funciones:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad.
- Aprobar formalmente el nivel de Seguridad de la Información.
- Promover que el tratamiento de los datos personales efectuados por **OMNILOY**, se efectúe de forma respetuosa con la normativa.
- Determinar los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Aprobación previa de la implementación de las medidas técnicas del sistema.

7.1.4. Responsable del servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad de los servicios.

7.2. Comité de Seguridad de la Información

El Comité de Seguridad de la Información coordina la seguridad de la información de la organización y cuyas funciones son:

- Atender las inquietudes de la Dirección en esta materia.
- Cuando corresponda informar a la Dirección del estado de la seguridad de la información.
- Promover la mejora continua del SGSI.
- Participar en la elaboración de estrategias respecto a la seguridad de la información.
- Cuando sea necesario, coordinar esfuerzos en esta materia.
- Participar cuando sea necesario en la revisión en políticas y directrices sobre la seguridad de la información.
- Promover la realización de auditorías sobre seguridad de la información.
- Promover que la seguridad de la información sea tenida en cuenta en el desarrollo de la actividad de la organización.

7.2.1. Composición

El Comité de Seguridad de la Información se ha constituido con los siguientes miembros:

- Responsable de la Seguridad.
- Responsable del Sistema.
- Responsable/s de la Información y el Servicio.
- Responsable del Área de Personas.
- Director de Comunicación.
- Director de Innovación y Calidad.
- Delegada de Protección de Datos.

A las reuniones del Comité de Seguridad de la Información podrán ser invitadas otros miembros de la organización o vinculados a esta que se consideren adecuados para tratar distintos asuntos relacionados con la seguridad de la información.

El Comité de Seguridad de la Información, se reunirá de manera ordinaria con una periodicidad mínima de una vez al año, de forma extraordinaria se reunirá cuando sea requerido por algunos de sus miembros, especialmente si se ha producido un incidente de seguridad con transcendencia relevante para la organización.

- Las reuniones del Comité de Seguridad de la Información serán documentadas en un registro en el que se recogerá las siguiente información: asistentes, fecha, asuntos tratados, acuerdos alcanzados…

7.3. Procedimiento de designación

El Responsable de Seguridad, el Responsable del Sistema y el Responsable de la Información y del Servicio han sido designados por la Dirección, y permanecerán en su cargo hasta que la Dirección lo considere oportuno. El resto de los responsables y directores serán asignados en función de las necesidades operativas y organizativas de la organización.

7.4. Delegación de funciones

Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el Comité, a propuesta del Responsable de Seguridad, podrá designar Responsables de Seguridad Delegados, en el número que considere necesario, que tendrán dependencia funcional directa del responsable de seguridad y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

8. Datos de carácter personal

OMNILOY trata datos de carácter personal. Las Políticas y procesos del Sistema de Gestión de Protección de Datos, integradas en el Sistema de Gestión, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de la empresa se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

9. Gestión de riesgos

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

Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Se ha establecido una metodología para realizar el análisis de riesgos, dicha metodología se aplica en base la identificación de activos, valoración de activos, dimensiones de seguridad de los activos, amenazas, impacto y riesgo.

10. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información complementa a las políticas de seguridad de **OMNILOY** en diferentes materias de seguridad de la información:

- Clasificación de la Información.
- Control de accesos.
- Dispositivos móviles.
- Encriptación de datos.
- Gestión de usuarios.
- Operaciones de sistemas.
- Pantallas Limpias.
- Recuperación de desastres.
- Respaldo y restauración.
- Seguridad de los proveedores.
- Uso aceptable de activos de la información.
- Controles criptográficos.
- Directrices de seguridad bajo ENS.
- Limpieza de documentos.

Materias de seguridad de la información de carácter personal

- Acción en Brechas de Seguridad.
- Conservación de datos de carácter personal.
- Evaluación de Impacto de Protección de Datos.
- Inventario y Registro de Actividades de Tratamiento de Datos.
- Obtención de Consentimiento.
- Transferencias Internacionales de Datos Personales.
- Uso de la imagen personal.
- Ejercicio de los Derechos.
- Calidad de datos de carácter personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad está disponible para los miembros de la organización en la intranet corporativa.

11. Obligaciones del personal

Todos los miembros de **OMNILOY** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad. Así, se contará con los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de **OMNILOY**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. Terceras partes

Cuando **OMNILOY** preste servicios a otros organismos o maneje información de otros organismos, bajo demanda de estos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **OMNILOY** utilice servicios de terceros o ceda información a terceros, bajo las directrices de ENS, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

13. Estructuración de la documentación

El sistema documental está formado por la presente Política de Seguridad y las Normativas y Procedimientos de Seguridad de **OMNILOY**, así como por las instrucciones técnicas que derivan de ellos. Adicionalmente, puede que algunos procedimientos internos (de gestión de personas, procedimientos operativos, etc.) incluyan aspectos relacionados con los requisitos de seguridad marcados por el ENS.

El Comité de Seguridad se responsabiliza de que este conjunto de documentos que forman parte del sistema documental de **OMNILOY** sean revisados con una periodicidad mínima anual y, si procede, actualizados siempre que sea necesario.

Asimismo, **OMNILOY** ha definido diferentes categorías y criterios de clasificación de la información, en base a los criterios establecidos en el Anexo I del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Para ello, se debe atender a lo establecido en el documento sobre la normalización de la información documentada.

Todos estos documentos se encuentran dentro del repositorio documental de la organización, accesible únicamente para el personal autorizado.