
# Política de Seguridad de la Información

## CONTROL DE VERSIONES

| Versión | Fecha | Descripción |
|---|---|---|
| 1.0 | 22/07/2024 | Elaboración del Documento de Política de Seguridad de la Información |
| 2.0 | 22/08/2026 | Adaptación de la política a los requisitos de la norma ISO / IEC 27001:2022: apartado 6. Objetivos |
| | | |

| ELABORADO | REVISADO | APROBADO |
|---|---|---|
| Comité de Seguridad | Responsable de Seguridad | Comité de Seguridad / Dirección |

## LISTA DE DISTRIBUCIÓN

| Fecha | Entidad | Justificación |
|---|---|---|
| 22/07/2024 | AT3W Group | Adecuación al ENS |
| 22/08/2026 | AT3W Group | Adecuación a la ISO / IEC 27001:2022 |
| | | |

# ÍNDICE

# 1 Aprobación y entrada en vigor

La presente Política de Seguridad ha sido aprobada el día 22 de julio de 2024 por parte de la Dirección de APLICACIONES TECNOLÓGICAS.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. Será revisada, junto a las propuestas de actualización o mantenimiento de esta, con una periodicidad mínima anual.

# 2 Introducción

APLICACIONES TECNOLÓGICAS 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 seguridad de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad 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 departamentos 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.

De este modo, APLICACIONES TECNOLÓGICAS, tiene presente que la seguridad es una parte integral de cada etapa del ciclo de vida de los sistemas TIC con que desarrollan sus funciones, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Mediante la presente Política APLICACIONES TECNOLÓGICAS ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), reconociendo como activos estratégicos la información que maneja, los servicios que presta y los sistemas TIC que soportan aquélla y hacen posible estos.

APLICACIONES TECNOLÓGICAS se compromete a establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información conforme a los requisitos de ISO/IEC 27001:2022 Sistemas de gestión de seguridad de la información.

Esta Política protege a la información, servicios y sistemas TIC contra las amenazas existentes y persigue garantizar la continuidad operativa de aquéllos, minimizar los riesgos de daños que puedan sufrir y asegurar el eficiente cumplimiento de los objetivos de APLICACIONES TECNOLÓGICAS.

Para ello, APLICACIONES TECNOLÓGICAS, actuará preventivamente, supervisando la actividad diaria para detectar cualquier incidente, y reaccionará con presteza a las brechas de seguridad detectadas e incidentes cuando se produzcan, con la aplicación de las medidas de seguridad que en cada caso corresponda, entre otras las que se relaciona a continuación.

## 2.1 Prevención

APLICACIONES TECNOLÓGICAS debe 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 debe implementarse las medidas mínimas de seguridad determinadas por el ENS/ISO 27001, 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, APLICACIONES TECNOLÓGICAS:

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

## 2.2 Detección

APLICACIONES TECNOLÓGICAS establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia, según lo dispuesto en el Artículo 10 del ENS (reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

## 2.3 Respuesta

APLICACIONES TECNOLÓGICAS, establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados a las posibles partes interesadas (clientes, proveedores, grupos inversores, etc.).
- 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) y con la Agencia Española de Protección de Datos (AEPD).

## 2.4 Recuperación

Para garantizar la disponibilidad de los servicios, APLICACIONES TECNOLÓGICAS dispondrá de los medios y técnicas que garanticen la recuperación de los servicios más críticos.

# 3 Alcance

Esta Política se aplica a los sistemas de información de APLICACIONES TECNOLÓGICAS que dan **soporte a los servicios de adquisición, operación, explotación y mantenimiento de datos provenientes de sensores remotos y el servicio de puesta en marcha y mantenimiento de software médico**, que se prestan dentro de la organización, por aquel personal que interviene de manera directa o indirecta en la prestación de dichos servicios, ya sea interno o externo a la organización.

# 4 Principios básicos de seguridad de la información

Los principios básicos son directrices fundamentales de seguridad que se tendrán presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Alcance estratégico:** la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de APLICACIONES TECNOLÓGICAS, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- **Responsabilidad determinada:** en los sistemas TIC se determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral:** la seguridad se concibe y desarrolla como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos:** el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** el establecimiento de medidas de prevención, detección, respuesta y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- **Mejora continua:** las medidas de seguridad se evaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado, para lo que APLICACIONES TECNOLÓGICAS podrá contar con el apoyo de servicios externos especializados.
- **Seguridad por defecto:** los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

# 5 Misión, visión y valores de la organización

Aplicaciones Tecnológicas S.A. es una empresa tecnológica española fuertemente internacionalizada. Fundada en 1986, cuenta con un equipo humano multidisciplinar, con gran experiencia en diferentes sectores, formado por expertos en ingeniería, física, electrónica, comunicaciones, IT, IoT, ciencia de datos y nuevas tecnologías.

Exportamos a más de 100 países tecnología inteligente desarrollada por nuestro departamento de I+D+i y fabricada en España en instalaciones de producción propias.

**I+D+i: Transformation through innovation**

El desarrollo continuo de nuevos productos, servicios y procesos es parte inseparable del ADN de Aplicaciones Tecnológicas. Porque el servicio de calidad al cliente empieza ofreciéndoles productos innovadores que respondan a sus necesidades.

Esta apuesta por el I+D se materializa con más del 50% del personal técnico dedicado a proyectos de investigación y un 12% de inversión en I+D en los últimos 10 años.

**Somos fabricantes**

En Aplicaciones Tecnológicas S.A. no solo desarrollamos productos, procesos y servicios en nuestras áreas de especialización y distintas divisiones, sino que nos encargamos de la industrialización, certificación y fabricación completas de los mismos.

Por eso, innovamos e invertimos de forma constante con el objetivo último de asegurar que ofrecemos la mayor calidad a nuestros clientes. A tal fin, contamos con más de 6.000 m² de instalaciones dedicadas a producción y logística, dotadas con maquinaria de última generación.

# 6 Objetivos

Con el fin de garantizar la protección efectiva de la información y de los recursos corporativos necesarios para el correcto funcionamiento de los servicios prestados por APLICACIONES TECNOLÓGICAS, tanto de amenazas externas como internas y definiendo dicha protección en términos de calidad y seguridad, se establecen los siguientes objetivos y principios básicos:

- Cumplir los requisitos legales y contractuales aplicables al desarrollo de sus funciones en la organización y la protección de datos de carácter personal y la continuidad de los procesos de negocio.

- Difundir entre todo el personal la necesidad y obligatoriedad de cumplir y hacer cumplir las políticas y normativas aplicables en materia de seguridad de la información, individualmente en función de sus tareas dentro de la organización.
- Restringir el uso tanto de la información en sí como de los sistemas que la procesan a aquellas tareas necesarias para el correcto desempeño del trabajo de cada persona, estando prohibido el uso en beneficio particular de ningún activo de APLICACIONES TECNOLÓGICAS.
- En el caso de la información, considerada como uno de los activos principales de APLICACIONES TECNOLÓGICAS, es deber de todo el personal mantener el secreto respecto a la misma y no divulgarla a terceros, salvo que las comunicaciones formen parte imprescindible de la relación laboral y en cumplimiento de las debidas garantías de confidencialidad establecidas.
- La presente Política proporciona el marco para el establecimiento, seguimiento y revisión de los objetivos de seguridad de la información, que serán definidos de forma coherente con los objetivos estratégicos de la organización, los riesgos identificados y los requisitos aplicables.

# 7 Marco normativo y legal

El marco normativo relevante en que se desarrollan las actividades de APLICACIONES TECNOLÓGICAS y, en particular, la prestación de sus servicios electrónicos está integrado por las normas indicadas en el F-6000 Listado de normas de aplicación, algunas de las cuales corresponde con las siguientes normas españolas y europeas:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ISO/IEC 27001:2022 Sistemas de gestión de seguridad de la información
- Entre otras

Además de lo descrito anterior, se dispondrá de un procedimiento de identificación de la legislación aplicable y de actualización permanente de un registro donde se conservan referencias a dichas normas actualizadas.

# 8 Organización de la seguridad

## 8.1 Criterios utilizados para la Organización de la Seguridad de la Información

APLICACIONES TECNOLÓGICAS, teniendo en cuenta lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS" y en la ISO/IEC 27001:2022 Sistemas de gestión de seguridad de la información, para organizar la seguridad de la información emprenderá las siguientes acciones:

- **Designará roles de seguridad:** Responsables de Servicios, Responsables de Información, Responsable de Seguridad de la Información, Responsable del Sistema.
- **Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información.** Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

## 8.2 Comité de Seguridad

Con el fin de facilitar la gestión de la seguridad en APLICACIONES TECNOLÓGICAS, la Dirección aprueba mediante la presente política, la conformación de un Comité de Seguridad de la Información (en adelante CSI), dedicado a la gestión y coordinación de todas las actividades relacionadas con la seguridad de los sistemas de información en la organización, ejerciendo las siguientes funciones:

- Aprobar las propuestas de modificación y actualización permanente de la PSI.
- Aprobar las Normativas y Procedimientos de Seguridad de la información que puedan derivar de la Política de Seguridad.
- Velar e impulsar el cumplimiento de la PSI, así como su desarrollo normativo.
- Atender las inquietudes en materia de seguridad de la información de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua en la gestión de la seguridad de la información.
- Impulsar la formación y concienciación.
- Resolver los conflictos que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Analizar los informes facilitados por el responsable de seguridad relativos al resultado de los análisis de riesgos, de las auditorías realizadas, de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.

Revisar la información aportada por el responsable de seguridad de la información relativa a los incidentes de seguridad.

El Comité de Seguridad de la Información está compuesto por los siguientes miembros:

- Responsable de la información: Dirección
- Responsable de Seguridad: Dirección de Sistemas TIC
- Responsable del Servicio: Responsable del I+D+i
- Responsable de sistemas: Subdirección de Sistemas TIC
- Responsable de sistemas I+D+i: Responsable IOT
- Administrador: Subdirección de Sistemas TIC
- Responsable de Calidad, Documentación y Sistemas de Gestión

El CSI se reunirá con carácter ordinario, al menos, una vez al año. Por razones de urgencia podría reunirse cuando su presidente lo establezca.

## 8.3 Roles y responsabilidades en materia de seguridad

### 8.3.1 Responsable de la Información

El Responsable de la Información (information owner) tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección; es el responsable último de cualquier error o negligencia que lleve a un incidente de seguridad. Tiene la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS/ISO 27001, la potestad de determinar los niveles de seguridad de la información.

Dentro de su ámbito de actuación, tendrá las siguientes funciones:

- Determinar los requisitos de seguridad de la información que tratan.
- Validar y aceptar el riesgo residual resultante del análisis de riesgos.
- Validar la normativa para el tratamiento de la información de la cual es responsable.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de los que es responsable, especialmente la incorporación de nueva Información a su cargo.
- Impulsar y perseguir la consecución de la seguridad de la información dentro del ámbito de sus competencias.

El Responsable de la Información puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).

Aunque la aprobación formal de los niveles de seguridad corresponda al Responsable de la Información, se podrá recabar una propuesta al Responsable de la Seguridad y se considerará la opinión del Responsable del Sistema.

### 8.3.2 Responsable de Seguridad

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- En caso de ciberataque de especial gravedad o cuando detecte deficiencias o brechas de seguridad que entienda supongan grave riesgo para los objetivos que la presente política pretende alcanzar, impulsará las acciones correctoras que estime necesarias, incluso mediante contratación de emergencia, dando cuenta de las mismas al Comité de Seguridad de la Información en la siguiente sesión que celebre.

En el desempeño de sus funciones, el Responsable de Seguridad de la Información contará con el apoyo de técnicos ámbito TIC y/o de servicios externos especializados.

### 8.3.3 Responsable del Servicio

El Responsable del Servicio tiene la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS/ISO 27001, la potestad de determinar los niveles de seguridad de los servicios.

El Responsable del Servicio deberá establecer los requisitos de los servicios en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad. El Responsable del Servicio determinará los niveles de seguridad de los servicios.

Dentro de su ámbito de actuación, tendrá las siguientes funciones:

- Determina los requisitos de seguridad de los servicios prestados.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Validar y aceptar el riesgo residual resultante del análisis de riesgos.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto al servicio o servicios de los que es responsable, especialmente la incorporación de nuevos servicios a su cargo.
- Validar la normativa para la prestación del servicio del cual es responsable.

El Responsable del Servicio puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se podrá recabar una propuesta al Responsable de la Seguridad y se considerará la opinión del Responsable del Sistema.

### 8.3.4 Responsable de Sistemas

Serán funciones del Responsable de Sistemas:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Elaborando los procedimientos operativos necesarios.
- 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 específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador 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.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.

- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

### 8.3.5 Responsable de Sistemas I+D+i

Serán funciones del Responsable de Sistemas I+D+i:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener los sistemas de información que soportan la adquisición, procesamiento, almacenamiento y explotación de datos de sensores remotos durante todo su ciclo de vida.
- Elaborar, mantener y aplicar los procedimientos operativos necesarios para garantizar el funcionamiento seguro y continuo de los sistemas.
- Definir y mantener la topología, arquitectura y configuración de los sistemas de información asociados a los servicios de sensores remotos.
- Proponer y aplicar medidas técnicas y organizativas para la protección de la información tratada.
- Gestionar las autorizaciones de acceso a los sistemas de información, garantizando el principio de mínimo privilegio.
- Supervisar y monitorizar la actividad de los usuarios para verificar su adecuación a los permisos concedidos.
- Aprobar y controlar los cambios en la configuración de los sistemas de información.
- Asegurar que cualquier modificación (hardware, software o configuraciones) se realiza conforme a procedimientos aprobados y sin comprometer la seguridad.
- Detectar, registrar y colaborar en la gestión de incidentes de seguridad que afecten a los sistemas de información.

- Informar al Responsable de Seguridad de cualquier anomalía, vulnerabilidad o compromiso detectado.
- Participar en la investigación y resolución de incidentes conforme a los procedimientos establecidos.

### 8.3.6 Administrador de sistemas

Serán funciones del Administrador de Sistemas:

- Gestionar, operar y mantener los sistemas de información, garantizando su correcto funcionamiento, disponibilidad y rendimiento durante todo su ciclo de vida.
- Ejecutar los procedimientos operativos establecidos, asegurando su adecuación a las políticas y normas de seguridad.
- Administrar la configuración de los sistemas de información, incluyendo hardware, software, redes y componentes asociados.
- Controlar y aplicar los cambios autorizados, garantizando que no se comprometa la seguridad ni la integridad del sistema.
- Gestionar las altas, bajas y modificaciones de usuarios, así como sus permisos y privilegios, conforme al principio de mínimo privilegio.
- Implementar y mantener los mecanismos de autenticación, autorización y control de acceso.
- Supervisar el funcionamiento de los sistemas y servicios mediante herramientas de monitorización.
- Gestionar los registros de actividad (logs), garantizando su integridad, disponibilidad y revisión periódica.
- Aplicar y mantener las medidas de seguridad técnicas definidas en el marco del ENS/ISO 27001.
- Asegurar la correcta implementación de controles de protección, detección y respuesta ante incidentes.
- Identificar, evaluar y corregir vulnerabilidades en los sistemas.
- Gestionar la actualización y parcheo de software y sistemas, conforme a los procedimientos establecidos.
- Detectar, registrar y notificar incidentes de seguridad.
- Colaborar en su análisis, contención, resolución y recuperación, siguiendo los procedimientos definidos.
- Informar al Responsable de Seguridad de cualquier anomalía, riesgo o incumplimiento detectado.

- Proporcionar la información necesaria para la gestión de la seguridad y la toma de decisiones.

#### 8.3.7 Responsable de Calidad, Documentación y Sistemas de Gestión

- Verificar que la organización cumple con el Esquema Nacional de Seguridad (ENS) y de la ISO / *IEC 2700:2022 Sistemas de gestión de seguridad de la información.*
- Asegurar la alineación con otras normas aplicables (ej. ISO 9001, y otras ISO implantadas).
- Comprobar que los procedimientos y políticas están actualizados y aprobados formalmente.
- Garantizar la trazabilidad y el control de versiones.
- Verificar que la documentación cumple los requisitos de calidad y auditoría.
- Planificar y coordinar auditorías ENS/ISO 27001.
- Acompañar en auditorías de certificación o conformidad.
- Definir y monitorizar indicadores de desempeño del sistema ENS/ISO 27001.
- Colaborar en la revisión del análisis y tratamiento de riesgos.
- Verificar que los controles implantados son coherentes con el nivel de riesgo.
- Asegurar que las decisiones del comité quedan registradas.
- Promover la cultura de calidad y seguridad en la organización.
- Fomentar la mejora continua y la prevención frente a la corrección.

### 8.4 Procedimiento de designación y renovación

Los roles y responsabilidades en materia de seguridad de la información serán designados por la Dirección de APLICACIONES TECNOLÓGICAS a propuesta del Comité de Seguridad de la Información. De igual forma, la Dirección es la encargada de la designación de los distintos miembros que formarán el Comité de Seguridad de la Información.

Asimismo, la Dirección se reserva el derecho de la revisión y renovación de las asignaciones y responsabilidades en cualquier momento.

# 9 Datos de carácter personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD) así como lo exigido de las medidas de seguridad

en el tratamiento de datos de carácter personal exigido en la ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDDGG).

El Registro de Actividades de Tratamiento recoge los tratamientos de datos personales que realiza APLICACIONES TECNOLÓGICAS, así como el resto de información pertinente, como la base jurídica del tratamiento, las finalidades, los plazos de conservación y los destinatarios (cesiones de datos personales).

Todos los sistemas de información de APLICACIONES TECNOLÓGICAS 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 registro de actividades de tratamiento. Las medidas de seguridad implementadas dependerán del análisis de riesgos realizado y tendrán como objetivo reducir el nivel de riesgo mediante la aplicación de medidas técnicas de seguridad relacionadas con las directrices del ENS , de la ISO 27001 y de las medidas legales relacionadas con los artículos del RGPD.

# 10 Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis de riesgos, identificando las amenazas y evaluando 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.

El Responsable de Seguridad de la Información será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará la metodología MAGERIT v3 - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

# 11 Obligaciones del personal

Todo el personal de APLICACIONES TECNOLÓGICAS, interno o externo, que utilice o tenga acceso a la información y/o a los sistemas tecnológicos o de información corporativos, tiene las siguientes obligaciones:

- Conocer, cumplir y hacer cumplir esta Política de Seguridad de la Información y las Normativas de Seguridad y procedimientos que la desarrollan y que le afecten.
- Atender a las acciones de concienciación en materia de seguridad de la información que se realicen.
- Utilizar los servicios y sistemas de información, así como la información en ellos contenida y a la que tengan acceso, con una finalidad profesional acorde a las tareas encomendadas en función de su puesto de trabajo y a los fines y propósitos que motivaron la concesión del acceso.
- Velar por la confidencialidad de la información a la que tenga acceso según la clasificación y características de la misma.
- Notificar eventos que puedan suponer una brecha de seguridad o evidencien una debilidad que pueda implicar posteriores brechas.
- Colaborar en la resolución de brechas de seguridad y en la realización de acciones preventivas cuando sea necesaria su participación
- Participar en la estructura de gestión de la seguridad de la información cuando corresponda según las competencias y funciones de su puesto de trabajo.
- No realizar acciones intencionadas o negligentes que puedan perjudicar la seguridad de los sistemas tecnológicos o la información que contienen.

Asimismo, queda bajo la responsabilidad de los usuarios hacer un uso proporcional, adecuado y justificado de los medios puestos a su disposición para el desarrollo de sus funciones. Cualquier uso indebido, podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

# 12 Desarrollo de la política de seguridad de la información

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas).

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

1. **Primer nivel normativo:** Constituido por la presente Política de Seguridad de la Información.
2. **Segundo nivel normativo:** Constituido por el conjunto de normas que complementan la política y uniformizan la utilización de aspectos concretos del sistema de información, indicando su uso correcto y las responsabilidades de los diferentes usuarios, técnicos y administradores.
3. **Tercer nivel normativo:** constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

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

Esta normativa de seguridad estará a disposición, y fácilmente accesible, de todos los miembros de la organización que necesiten conocerla.

# 13 Relación con terceros

Cuando APLICACIONES TECNOLÓGICAS preste servicios a otras organizaciones o maneje información de otras organizaciones, 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando APLICACIONES TECNOLÓGICAS utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de las Normativas de Seguridad aplicables a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la 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 de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información 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.

# 14 Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas o, cuando procedan, externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de las normas y procedimientos

Firmado: Dirección


Fecha 20 de agosto de 2026