POLÍTICA DE SEGURIDAD

EDICIÓN	CAMBIO	FECHA
00	Edición inicial	01/03/2023
01	Cambio de Plantilla, Logos y de los Roles del Comité de Seguridad	13/05/2024
02	Actualización según la Guía CCN STIC 805 Política de Seguridad, junio 2025	19/08/2025
03	Uso de firmas electrónicas.	29/09/2025
04	Inclusión de requisitos de la ISO 27001:2022 Gestión de los Sistemas de Seguridad de la Información	02/12/2025
05	Actualización y adecuación formal de la estructura y controles según los requisitos de la Guía CCN-STIC 805 de junio de 2025 para el nivel ALTO	11/05/2026

Contenido

2. ALCANCE DE LA POLÍTICA:

La política aplica a todos los sistemas de información, al personal y a los prestadores de servicios de la organización

3. DECLARACIÓN DE PRINCIPIOS

ALGORITMOS PROCESOS Y DISEÑOS, S.A. (APD) es una organización con una marcada orientación tecnológica, nacida con vocación innovadora y con una visión enfocada en aportar soluciones de valor al entorno empresarial. Desde sus inicios, la compañía ha mantenido un compromiso firme con la calidad, la evolución tecnológica y la adaptación continua a las necesidades de sus clientes.

La actividad de APD se estructura sobre diferentes áreas estratégicas relacionadas con la tecnología, la transformación digital, el desarrollo de soluciones especializadas tecnológicas, la ciberseguridad y la prestación de servicios técnicos profesionales. Esta diversificación permite a la organización ofrecer una respuesta integral, flexible y alineada con los retos actuales del mercado.

APD fundamenta su actuación en principios de innovación, profesionalidad, compromiso, seguridad y mejora continua, orientando sus capacidades al crecimiento sostenible, la excelencia operativa y la generación de confianza en clientes, colaboradores y demás partes interesadas.

Actualmente, APD mantiene presencia en más de 20 países a través de una red de oficinas, distribuidores y socios tecnológicos, consolidando su liderazgo en soluciones de alto valor añadido.

Debido a nuestra actividad, en **APD** somos conscientes de que la información es un activo con un elevado valor para nuestra organización y requiere, por lo tanto, una protección y gestión adecuadas con el fin de dar continuidad a nuestra línea de negocio y minimizar los posibles daños ocasionados por fallos a la integridad, disponibilidad y confidencialidad de la información. Así mismo, tanto la legislación vigente relativa a la protección de datos personales (RGPD y LOPDGDD), como el compromiso de **APD** con nuestros clientes nos hace especialmente sensibles al tratamiento de los datos personales a los que tenemos acceso en el ejercicio de nuestra actividad.

Para ello, **APD** establece un conjunto de actividades de gestión que tienen como objetivo preservar los principios de Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad, así como Conformidad Regulatoria de la información. A su vez, estos principios se definen de la siguiente manera:

- Confidencialidad: es la propiedad que permite garantizar que el acceso a la información solamente puede ser ejercido por las personas autorizadas para ello.
- Integridad: es la propiedad de salvaguardar la exactitud y completitud de los activos de información.
- Disponibilidad: es la cualidad que garantiza que las personas autorizadas pueden acceder a la información y procesarla en cualquier momento en que sea necesario.
- Autenticidad: es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad: es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- Conformidad Regulatoria: es la propiedad que asegura que la información es gestionada de acuerdo a los principios éticos, profesionales y legales establecidos por las regulaciones que son aplicables en cada contexto.

Los sistemas deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en 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 deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad y el Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022, 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.

Los diferentes departamentos de la organización deben cerciorarse de que la seguridad 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.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

Dentro del amparo de lo anterior, se encuentra embebida la protección de la privacidad. Nuestros sistemas tratan datos personales sensible y por ello, la protección de la privacidad se erige como un pilar esencial en el marco del ENS y el Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022 y se constituye como una necesidad social que las empresas deben respetar y proteger, así como objeto de legislación y/o regulación específica en todo el mundo.

4. OBJETIVOS GENERALES

La Política de Seguridad proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas, legales y organizativas que se requieran para garantizar la seguridad de la información y la privacidad, cumpliendo el marco legal de aplicación y las políticas globales y específicas de firma, así como los procedimientos definidos.

Estas actuaciones desde el punto de vista de la seguridad y privacidad son seleccionadas e implantadas basándose en el análisis de riesgos y el equilibrio entre riesgo aceptable y coste de las medidas.

El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información y datos frente a amenazas, internas o externas, deliberadas o accidentales.

La información y datos pueden existir en una variedad de formatos, con soportes tanto electrónicos como el papel u otros medios, e incluye a veces datos críticos acerca de las operaciones, estrategias o actividades de **APD** y de sus clientes e incluso, en su caso, datos de carácter sensible que establece la normativa de protección de datos de carácter personal. La pérdida, corrupción, o sustracción de información o de los sistemas que la gestionan tiene un impacto elevado en nuestra Firma.

APD está convencida de que una gestión eficaz de la Seguridad de la Información y de la Privacidad es un elemento habilitador para que la organización comprenda completamente y actúe de modo adecuado a los riesgos a los que la información es expuesta, así como para poder responder y adaptarse de manera eficiente a los crecientes requerimientos de organismos reguladores, leyes, y por supuesto sus clientes.

5. COMPROMISO DE LA ALTA DIRECCIÓN

El propósito del Sistema de Seguridad de la Información es garantizar que los riesgos de la seguridad de la información y privacidad sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, asumible y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para ello, la dirección declara el compromiso de **APD** para:

- Establecer como objetivo primordial los sistemas de seguridad de la información que dan soporte a **la implantación y mantenimiento de equipos y aplicaciones informáticas**, con absoluto respeto a los estándares de calidad, preservando la

información, con especial atención a la sensibilidad de los datos personales tratados, con todas las medidas necesarias a su alcance.

- Aplicar el principio de mejora continua a todos los procesos de la organización, con el objetivo adicional de conseguir el mayor grado de satisfacción de los clientes.
- Asegurar el cumplimiento de los requisitos legales y reglamentarios que sean de aplicación (en particular la relativa a la protección de los datos personales), así como los que la organización haya asumido de manera voluntaria en el desarrollo de la Responsabilidad Social Corporativa y en el Código de Conducta.
- Potenciar la participación, la comunicación, la información y la formación del equipo profesional con el objetivo de que se sienta partícipe del trabajo de la organización en su conjunto.
- Promover el compromiso de responsabilidad entre los componentes del equipo de acuerdo con los requisitos de calidad, así como los relativos a la privacidad y seguridad de la información acordados tanto internamente como con los clientes, mediante acciones de formación y concienciación adecuadas y regulares.
- Asegurar la continuidad del negocio desarrollando planes de continuidad conformes a metodologías reconocidas.
- Realizar y revisar periódicamente un análisis de riesgos basados en métodos reconocidos que nos permitan establecer el nivel tanto de privacidad de los datos personales como de seguridad de la información a nivel general y de los proyectos y servicios en marcha y minimizar los riesgos mediante el desarrollo de políticas específicas, soluciones técnicas y acuerdos contractuales con organizaciones especializadas.
- Compromiso de información a partes interesadas.
- Selección de proveedores y subcontratistas en base a criterios relacionados con la privacidad y seguridad de la información.
- Establecer y cumplir los requisitos contractuales con las partes interesadas.
- Promover una cultura de mejora continua en la gestión de la seguridad de la información e implementar mejoras basadas en el análisis de incidentes, auditorías y revisiones periódicas
- Gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.
- Asegurar la protección de los derechos de propiedad intelectual
- Establecer periódicamente un conjunto de objetivos e indicadores, que permitan a la dirección llevar a cabo un adecuado seguimiento de los niveles de servicio ofrecidos y las actividades de gestión.

La dirección de **APD** se compromete a apoyar y promover los principios establecidos en esta Política, para lo que pide al personal de **APD** que asuma y se atenga a las previsiones del sistema de gestión documentado para el ENS y la ISO 27001:2022.

6. PRINCIPIOS DE LA SEGURIDAD

Siguiendo las directrices del capítulo II, los principios básicos por los que **APD** se rige son los siguientes:

a) Seguridad como proceso integral, constituido por todos los elementos relacionados con el sistema de información, prestando especial importancia a la concienciación de todos los participantes.
b) Gestión de la seguridad basada en los riesgos, tal y como se describe en el apartado 10 del presente documento.
c) Prevención, detección, respuesta y conservación. Desarrollado en el apartado 6 del presente documento.
d) Existencia de líneas de defensa constituida por múltiples capas de seguridad organizadas en medidas de naturaleza organizativa, física y lógica.
e) Vigilancia continua y Reevaluación periódica, que permita la detección de comportamientos anómalos y su respuesta, así como medir su evolución mediante la detección de vulnerabilidades y las deficiencias en la configuración, verificando periódicamente su eficacia, pudiendo llegar a un replanteamiento de nuestro diseño de seguridad.
f) Diferenciación de responsabilidades, tal y como se desarrolla en el apartado 7 del presente documento.

Para ello, aplicaremos 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.

Estos requisitos mínimos se encuentran en proporción a los riesgos identificados en nuestros sistemas, de conformidad con lo dispuesto en el artículo 28 y se desarrollan en los documentos del sistema de gestión del ENS y el Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022

7. GESTIÓN DE LA DOCUMENTACIÓN

Esta Política de Seguridad complementa las políticas de seguridad de **APD** en diferentes materias y 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 documentación relativa a la Seguridad de la Información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel (Política): Aprobada por la Alta Dirección (CEO) y revisada anualmente.
- Segundo nivel (Normativas y Procedimientos): Deben ser aprobados formalmente por el Comité de Seguridad.
- Tercer nivel (Registros y Evidencias): Gestionados por el Responsable del Sistema y el de Seguridad

El personal tendrá acceso a la información relevante en el siguiente repositorio

\\ficheros\ens\PUBLICA

8. GESTIÓN DE INCIDENTES

8.1 Prevención

Los departamentos 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 los departamentos deben implementar 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, los departamentos 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.

8.2 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 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 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.

8.3 Respuesta

Los departamentos 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).

8.4 Recuperación

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

9. ORGANIZACIÓN DE LA SEGURIDAD

9.1 Comité de Seguridad

Los integrantes del Comité de Seguridad serán designados en un acta fundacional, donde se indicará la persona designada y el cargo que deberá ostentar.

El Secretario del Comité de Seguridad será el RESPONSABLE DE SEGURIDAD y tendrá como funciones

- Convoca las reuniones del Comité de Seguridad.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- El Comité de Seguridad reportará al Director General.

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.

- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Cuando existan discrepancias técnicas u operativas entre los distintos roles de responsabilidad del sistema, el Comité de Seguridad de la Información será el encargado de dirimir y resolver dichos conflictos mediante un análisis del impacto y del riesgo residual. Se contemplarán procedimientos específicos de resolución adaptados a las singularidades normativas de cada área de actividad, garantizando siempre que ninguna decisión ejecutiva vulnere los requisitos mínimos de seguridad exigidos por el nivel ALTO del ENS.
- Realizar el Análisis de Contexto de la organización al menos una vez al año.

9.2 Roles: Funciones y responsabilidades

Se detallarán a continuación las funciones de los responsables de la organización:

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.
- Aprobar la categorización del sistema con respecto a la información.
- Validar los requisitos de seguridad en sus respectivas dimensiones (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad)
- Los que se vayan indicando en los documentos dentro del alcance del ENS y del Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar la categorización del sistema con respecto a los servicios.
- Validar los requisitos de seguridad en sus respectivas dimensiones (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad)
- Los que se vayan indicando en los documentos dentro del alcance del ENS y del Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022.

Responsable de la Seguridad

Sus funciones serán las siguientes

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a 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.
- Aprobar la declaración de aplicabilidad.

- Canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que se presta o solución que provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio (POC).
- Los que se vayan indicando en los documentos dentro del alcance del ENS y del Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022.

El Responsable de la Seguridad será el secretario del Comité de Seguridad con las funciones indicadas en el apartado 7.2 de la presente política.

De conformidad con el principio de "segregación de funciones y tareas" recogido en el art. 10 del ENS, el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema.

Responsable del Sistema

Sus funciones serán las siguientes:

- 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.
- Potestad para 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.
- Los que se vayan indicando en los documentos dentro del alcance del ENS y del Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022.

Responsable de Privacidad

Sus funciones serán las siguientes:

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de **APD** en materia de protección de datos de carácter personal.
- Coordinar, junto con el Responsable de Seguridad, el cumplimiento del ENS con respecto a la protección de datos de carácter personal.

9.3 Procedimientos de designación

La designación del Responsable de Seguridad compete exclusivamente al Comité de Seguridad. Dicho nombramiento se revisará cada dos años, o bien cuando se requiera la sustitución de los encargados por ausencias de larga duración o bajas que puedan comprometer la operatividad del sistema.

Igualmente, el resto de los cargos indicados en el apartado anterior será designado por el Comité de Seguridad mediante acta de reunión.

9.4 Revisión de la Política de Seguridad

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Alta Dirección y difundida para que la conozcan todas las partes afectadas.

10 DATOS DE CARÁCTER PERSONAL

APD, en la prestación de su servicio, trata datos de carácter personal especialmente sensibles.

La documentación relativa, a la que tendrán acceso sólo las personas autorizadas, recoge los registros de actividad de tratamiento de datos afectados y los responsables correspondientes. Todos los sistemas de información de **APD** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal.

En lo que respecta de manera específica a la protección de los datos personales, **APD** se compromete a cumplir con los principios indicados en la legislación de referencia. Estos son:

- Principio de "licitud, transparencia y lealtad". Los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de "finalidad". Los datos deben ser tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otro lado, se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de "minimización de datos". Aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.
- Principio de "exactitud". Disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.
- Principio de "limitación del plazo de conservación". La conservación de los datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento.
- Principio de "seguridad" Realizar un análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.
- Principio de "responsabilidad activa" o "responsabilidad demostrada". Mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que podamos garantizar y demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.
- Dirigir, apoyar y supervisar el sistema de gestión de la seguridad de la información, según lo establecido en el RD 311.2022 y posteriores modificaciones, y buscar se alcancen los objetivos del mismo y según el Sistema de Gestión de Seguridad de la Información, según los requisitos de la ISO 27001:2022.

11 .GESTIÓN DE RIESGOS

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

- Cuando ocurran cambios significativos en la tecnología subyacente o en el entorno de amenazas.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La presente política determina las estrategias de tratamiento de riesgos y formaliza el protocolo de aceptación del riesgo residual, exigiendo una autorización explícita y motivada de la dirección para todo riesgo que supere el umbral de tolerancia institucional.

12 CONCIENCIACIÓN Y FORMACIÓN

Es responsabilidad de la organización lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de y a todas las actividades, de acuerdo con el principio de Seguridad como proceso integral recogido en el Artículo 6 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Por ello, **APD** cuenta con una sistemática implementada en todas las áreas de la organización para formar, informar y concienciar a todo el personal con respecto a su implicación en la consecución de los objetivos de seguridad.

13 OBLIGACIONES DEL PERSONAL

Todos los miembros de **APD** tienen la obligación de conocer y cumplir esta Política de Seguridad y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **APD** atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **APD** en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas 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.

14 TERCERAS PARTES

Cuando **APD** preste servicios a otras organizaciones públicas o privadas o maneje información de otras organizaciones públicas o privadas, se les hará partícipes de esta Política de Seguridad, 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 **APD** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Las terceras partes asumirán de forma contractual las obligaciones de esta normativa, pudiendo implantar sus propios procedimientos para satisfacerlas. Para garantizar la coordinación, se definirán protocolos 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.

En la adquisición de derechos de uso de activos y servicios en la nube, se garantizará el cumplimiento de los requisitos establecidos en las medidas de seguridad del Anexo II del ENS para el nivel ALTO, así como las directrices específicas de la Guía CCN-STIC correspondiente y las normativas internas de desarrollo seguro.

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.

15 LEGISLACIÓN APLICABLE

A continuación, se detallan las leyes que se consideran aplicables al SGSI, junto con una definición del área responsable de evaluar su impacto en la organización.

Ley / Regulación	Responsabilidad
Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas	Responsable de Seguridad
Ley 40/2015, de 1 de octubre, establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades	Responsable de Seguridad
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	Responsable de Seguridad
Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal	Responsable de Seguridad
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	Responsable de Seguridad
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	Responsable de Seguridad
Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI)	Responsable de Seguridad
Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.	Responsable de Seguridad
REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE	Responsable de Seguridad
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	Responsable de Seguridad

Además del marco legislativo general, **APD** ha desarrollado el proceso PRSI09 Cumplimiento legal y normativo y el registro AX01_PRSI09. A través de estos, **APD** actualiza la legislación aplicable y verifica su cumplimiento.