POLITICA DE SEGURIDAD

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día **29 de junio de 2026** por la Dirección General de Sayós&Carrera, S.L., en adelante Sayoscarrera.

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

2 INTRODUCCIÓN

Sayoscarrera 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.

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 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.

Los diferentes departamentos 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.

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

2.1 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.

2.2 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 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 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.

2.3 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 el Equipos de Respuesta a Emergencias (CERT_SC).

2.4 RECUPERACIÓN

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

3 ALCANCE

Esta política se aplica a todos los sistemas TIC de Sayoscarrera y a todos los miembros de la organización, sin excepciones.

4 MISIÓN

Sayoscarrera, fundada en el año 1995 es una empresa de Consultoría e Ingeniería especializada en Tecnologías de la Información y las Comunicaciones.

Nuestro servicio se define como un soporte altamente especializado en Tecnologías de la Información y las Comunicaciones que cubre todo el ciclo de vida de un proyecto, desde la Consultoría, Ingeniería y Dirección de Proyectos, y procesos de soporte en la explotación, Gestión de Costes y Gestión de infraestructuras TIC.

En concreto, contempla:

- Servicios de Consultoría e Ingeniería.
- Servicio de Telecom Expense Management (TEM) y Gestión de costes IT.
- Servicios de Centro de Gestión de Operaciones IT (CGO) y SOC.

Nuestros pilares son la excelencia, el conocimiento y la implicación con el cliente, lo que nos permite planificar y ejecutar estrategias para asegurar el éxito en nuestras actuaciones.

Los objetivos en materia de seguridad que la Sayoscarrera pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de Sayoscarrera respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5 PRINCIPIOS RECTORES DE LA POLÍTICA

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, 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 la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.

- Vigilancia continua y reevaluación periódica: Sayoscarrera implementa medios de detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos. Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6 MARCO NORMATIVO

Adicionalmente al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el marco normativo en materia de seguridad de la información en el que Sayoscarrera desarrolla su actividad se detalla en el “Indice Org.1 - Registro Normativa Aplicable ddmmaaaa.xlsx”, ubicado en:

\\Scfs\recursos\ENS SAYOSCARRERA\REQUERIMIENTOS 808\2 MARCO ORGANIZATIVO\Org.1 - Política de seguridad\Marco legal PSI

Adicionalmente, la presente Política se ha elabordo de acuerdo con las siguientes Guías y Normativas:

- **Guías CCN-STIC**, Detalladas en el Indice de Guías CCN - Art. 5 - Registro de guías CCN ddmmaaa.xlsx, ubicado en:

  \\Scfs\recursos\ENS SAYOSCARRERA\REQUERIMIENTOS 808\1 CUMPLIMIENTO ARTICULOS ENS\Art.5 - GUIAS

- **Guías CCN-STIC – Configuración segura**, Detalladas en el Indice de Guías de Configuración segura, Art. 5 - Registro de guías CONFIGURACION SEGURA ddmmaaaa.xlsx, ubicado en:

  \\Scfs\recursos\ENS SAYOSCARRERA\REQUERIMIENTOS 808\1 CUMPLIMIENTO ARTICULOS ENS\Art.5 - GUIAS

- **Metodología Magertit**
- **UNE-EN-ISO 9001:2015** Sistemas de gestión de la calidad.
- **ISO 27001:2022**

7 ORGANIZACIÓN DE LA SEGURIDAD

La implantación de la Política de Seguridad en Sayoscarrera requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de la Política de Seguridad cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en este capítulo y que contempla los siguientes Comités y Roles:

- Dirección
- Comité de Seguridad TIC
- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad
- Responsable del Sistema
- Administrador de Seguridad
- Administrador del Sistema
- Auditor interno del Sistema
- Delegado de Protección de Datos (DPO)
- Responsable/ Encargado del Tratamiento

7.1 COMITÉ DE SEGURIDAD TIC – FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TIC coordina la seguridad de la información en Sayoscarrera, y estará formado por:

- Responsable de la Seguridad
- Responsable de la Información
- Responsable del Servicio
- Responsable del Tratamiento

El Secretario del Comité de Seguridad TIC será el Responsable de la Seguridad y tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad de la Información.
- 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 TIC reportará a la Dirección de Sayoscarrera.

El Comité de Seguridad TIC se reunirá como mínimo cada 6 meses, y en aquellos casos que sea convocado por la Dirección.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de Sayoscarrera y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la 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, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Elaborar la Normativa de Seguridad de la información.
- 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.
- 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 tales incidentes.
- Promover la realización de las 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 distintos 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 TIC 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.
- Resolver los conflictos de responsabilidad 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.

7.2 ROLES – FUNCIONES Y RESPONSABILIDADES

7.2.1 DIRECCIÓN

Es el máximo responsable de la implantación del ENS.
De la Dirección depende el compromiso de la entidad con la Seguridad y su adecuada implantación, gestión y mantenimiento.

Sus funciones más significativas serán las siguientes:

- Aprueba la Política de Seguridad de la organización.
- Aprueba la Política de Protección de Datos
- Aprueba la Normativa de Seguridad.

- Aprueba el Análisis de Riesgos.
- Aprueba el Riesgo residual.
- Exigir a todo el personal que aplique la seguridad de la información de acuerdo con la Política de Seguridad de la información corporativa, las normativas temáticas, los procedimientos específicos establecidos en la organización así como las Instrucciones Técnicas de Seguridad que se establezcan.

7.2.2 RESPONSABLE DE LA INFORMACIÓN

Sus funciones más significativas serán las siguientes:

- Establecer los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que es responsable.
- Valorar para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Trabajar en colaboración con el Responsable de Seguridad y el Responsable de Sistemas en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

7.2.3 RESPONSABLE DEL SERVICIO

Sus funciones más significativas serán las siguientes:

- Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información.
- Valorar para cada servicio contemplado en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Trabajar en colaboración con el Responsable de Seguridad y el Responsable de Sistemas en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

7.2.4 RESPONSABLE DEL SISTEMA

Sus funciones más significativas serán las siguientes:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Adopción de las medidas correctoras derivadas de las auditorías de seguridad.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.

- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.
- En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada a la Dirección y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos.

7.2.5 RESPONSABLE DE SEGURIDAD

Sus funciones más significativas 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.
- 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.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar 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.
- Notificar a la autoridad competente de referencia y sin dilación indebida, de los incidentes que requeiran notificación.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos prestados por la organización según el criterio de valoración establecido por el artículo 40 del ENS.
- Realizar o instar la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de Sayoscarrera en materia de seguridad.
- Análisis de los informes de auditoria y escalado al Comité y/o Dirección.
- Analizar los riesgos inherentes al despliegue de sistemes de IA, atendiendo a las valoracions del Responsable de la información y del Servicio, y en su caso del DPO.
- Supervisar la implantación de sistemes de IA.
- Supervisar el estado de seguridad del sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.
- Elaborar la normativa de seguridad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar los procedimientos de seguridad elaborados por el Responsable de Sistemas cuando en virtud del contenido definido no requieran la revisión y aprobación del Comité de Seguridad TIC.

- En la gestión de los ciberincidentes, contando con la Dirección, los responsables de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CCN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad.
- Cuando fuese precisa la notificación a las autoridades competentes, esta deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de información ampliada de forma paulatina.
- El Responsable de la Seguridad colaborará con el Delegado de Protección de Datos en la gestión de los incidentes que afecten a datos personales y, en su caso, a la notificación a las autoridades de control y a las personas afectadas.
- Relación con el POC de empresas terceras.
- Cuando actúa como POC de Sayoscarrera:
  - Canalización de las comunicaciones en materia de seguridad e incidentes a la entidad que contrata los servicios de Sayoscarrera.
  - Supervisión del cumplimiento de los requisitos de seguridad del Servicio.
  - Gestión de incidentes de seguridad.

- Elaborar como secretario del Comité de Seguridad TIC los siguientes informes periódicos:
  - Resumen consolidado de las actuaciones llevadas a cabo y en curso dentro del desarrollo del Plan de adecuación del ENS aprobado.
  - Resumen consolidado de los incidentes de seguridad registrados desde la última reunión del Comité.
  - Valoración del estado de la seguridad de los sistemas de información de la organización y la evolución de los niveles de riesgo a los que están expuestos.

7.2.6 ADMINISTRADOR DE SEGURIDAD

Sus funciones más significativas serán las siguientes:

- Comprobar que los controles de seguridad establecidos son adecuadamente observados.
- Comprobar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Comprobar 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la 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.

7.2.7 ADMINISTRADOR DEL SISTEMA

Sus funciones más significativas serán las siguientes:

- La gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, mantenimiento y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Informar al Responsable del Sistema 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.

7.2.8 AUDITOR INTERNO DEL SISTEMA

Sus funciones más significativas serán las siguientes:

- El auditor interno debe comprobar que:
  - Las medidas de seguridad del Anexo II del ENS están implantadas.
  - Las medidas están documentadas, operativas y mantenidas.
  - Existe evidencia de su funcionamiento.
- Realizar auditorías periódicas:
  - Planificar auditorías
  - Ejecutar revisiones técnicas y organizativas
  - Documentar resultados
- Evaluar la eficacia de los controles de seguridad:
  - Revisar logs

  - Revisar controles de acceso
  - Revisar monitorización
  - Revisar gestión de vulnerabilidades
- Verificar la documentación de seguridad.
- Evaluar la gestión de incidentes de seguridad
- Verificar la trazabilidad y monitorización
- Evaluar la segregación de funciones
- Proponer acciones correctivas y su seguimiento
- Elaborar el informe de auditoría y entregarlos al Responsable de seguridad

7.2.9 DELEGADO DE PROTECCIÓN DE DATOS (DPO)

La obligatoriedad de nombrar un DPO (o Delegado de Protección de Datos - DPD) viene determinada en el art. 37 del REGLAMENTO (RGPD) y en el art. 34 de la Ley Orgánica 3/2018.

Sayoscarrera, por la actividad que desarrolla no entra en ninguno de los supuestos de obligatoriedad, no obstante, de forma voluntaria, se designa la figura del DPO.

De acuerdo a lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.

La Dirección de Sayós&Carrera, S.L., ha determinado que la designación de la figura legal del DPO recaiga en la compañía externa **nifled tic&law (NIFLED, S.L.),** con CIF B-62.689.674 y con domicilio social en avenida de les Corts Catalanes, nº 5, 1º, Sant Cugat del Vallés, 08173 (Barcelona) como asesores legales expertos en el ámbito de la protección de datos personales y privacidad.

7.3 PROCEDIMIENTOS DE DESIGNACIÓN

Es función de la Dirección de la entidad designar:

- Al Responsable de la Información.
- Al Responsable del Servicio, pudiendo ser el mismo que el Responsable de la Información.
- Al Responsable de la Seguridad, que debe reportar directamente a la Dirección y, al Comité de Seguridad TIC.

- Al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de Seguridad.
- Al Administrador de Seguridad
- Al Aministrador del Sistema
- Al Auditor interno del Sistema

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

En la fecha de aprobación y entrada en vigor de la persente Política de seguridad, las personas nombradas en cada uno de los roles son:

- Dirección General: RXX – xxxxxxxxxxx
- Responsable de la Información/ Servicio
  - Área consultoria e Ingeniería: MXX – xxxxxxxxxxx
  - Área gestión de costes TEM: JXX – xxxxxxxxxxx
  - Área de CGO-SOC: MXX – xxxxxxxxxxx
  - Área Gestión RRHH: RXX – xxxxxxxxxxx
  - Área Gestión Económica: RXX – xxxxxxxxxxx
  - Área Gestión SSII: MXX – xxxxxxxxxxx
  - Área Gestión Comercial: RXX – xxxxxxxxxxx

- Responsable de Seguridad: DXX – xxxxxxxxxxx
- Responsable del Sistema: SXX – xxxxxxxxxxx

- Administrador del Sistema: JXX – xxxxxxxxxxx
- Administrador de Seguridad: MXX – xxxxxxxxxxx
- Auditor del Sistema (contingència): RXX – xxxxxxxxxxx
- Delegado de Protección de Datos (DPO): nifled tic&law (externalizado)
- Responsable/ Encargado del Tratamiento: RXX – xxxxxxxxxxx

7.4 RESOLUCUÓN DE CONFLICTOS

En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias

7.5 MATRIZ RACI

La matriz RACI adjunta relaciona las responsabilidades de los diferentes Roles en las Tareas principales establecidas en la Política de Seguridad:

Tarea	DIR	RINFO	RSERV	RSEG	RSIS	AS	Todos los recursos
Niveles de seguridad requeridos por la información		A	I	R	C		
Niveles de seguridad requeridos por el servicio		I	A	R	C		
Determinación de la categoría del sistema	A	I	I	R	I		
Análisis de riesgos	A	I	I	R	C		
Declaración de aplicabilidad		I	I	A/R	C		
Medidas de seguridad adicionales		I	I	A/R	C		
Configuración de seguridad		I	I	A	C	R	
Aceptación de riesgo residual	A	C	C	R	I		
Documentación de seguridad				A/R	C	I	
Política de seguridad	A	C	C	R	C		Conocer
Normativa de seguridad	A	C	C	R	C	I	Conocer y acatar
Procedimientos de seguridad		I	I	C	A/R	I	
Implantación de las medidas de seguridad		I	I	C	A/R	R	
Supervisión de las medidas de seguridad				A	I	R	
Estado de seguridad del sistema	I	I	I	A	I	R	
Planes de mejora de la seguridad		I	I	A/R	C		
Planes de concienciación y formación		I	I	A/R	C		Conocer y acatar
Planes de continuidad		I	I	C	A/R		
Suspensión cautelar del servicio (nota 1)	I	I	I	A	R		
Seguridad en el ciclo de vida				C	A		

Leyenda:

A: Toma la decisión (y responde de ello). Autoriza (el trabajo a realizar) y Aprueba (el trabajo finalizado y, a partir de ese momento, se hace responsable de él. Debe asegurar que se ejecutan las tareas.
R: Realiza el trabajo (previamente autorizado por A) y es responsable por su realización. Es quien debe ejecutar las tareas.
C: Se le consulta antes de tomar la decisión. Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I: Se le informa de las decisiones tomadas. Debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

(Nota 1) Debemos entender la “suspensión cautelar del servicio” como una respuesta ágil ante un problema de seguridad detectado, y de corta duración. Si fuera de larga duración, la aprobación de la suspensión debería recaer en la Dirección de la organización, siendo consultados los RINFO, RSERV y RSEG, y siendo responsable de su ejecución el RSIS.

7.6 REPORTES Y FLUJOS DE INFORMACIÓN

- El Administrador de Seguridad, reportará al Responsable del Sistema, según su dependencia funcional, de los incidentes relativos a la Seguridad del sistema y de las acciones de configuración, actualización o corrección.
- El Responsable del Sistema reportará al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- El Responsable del Sistema reportará al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- El Responsable del Sistema reportará al Responsable de la Seguridad de las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema y le entregará un resumen consolidado de los incidentes de seguridad.
- El Administrador de Seguridad proporcionará al Responsable del Sistema un resumen consolidado de los incidentes de seguridad.
- El Responsable de la Seguridad reportará al Responsable de la Información las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Responsable de la Seguridad reportará al Responsable del Servicio las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- El Responsable de Seguridad reportará al Comité de Seguridad TIC, en su calidad de Secretario, entregando un resumen consolidado de actuaciones en materia de seguridad y de los incidentes relativos a la seguridad de la información, e informándole del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

7.7 RESPONSABILIDADES

- La responsabilidad legal y la especificación de las necesidades o requisitos, corresponde a la Dirección de la organización y a los Responsables del tratamiento, Responsables de la Información y Responsables del Servicio,
- La supervisión corresponde al Responsable de la Seguridad y al Delegado de Protección de Datos (DPO), en sus respectivos ámbitos.
- La operación del sistema de información corresponde al Responsable del Sistema.

7.8 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

8 DATOS DE CARÁCTER PERSONAL

Sayoscarrera trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. Sayoscarrera deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

Sayoscarrera.ha aprobado una Política de protección de datos personales que establece los principios y pautas de actuación que deben regir en la Compañía en materia de protección de datos personales, garantizando, en todo caso, el cumplimiento de la legislación vigente aplicable.

En particular, la Política de protección de datos personales tiene la finalidad de garantizar el derecho a la protección de sus datos de todas las personas físicas que se relacionan con la Compañía, asegurando el respeto del derecho al honor, la privacidad y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, procedentes de diferentes fuentes y con fines diversos en función de su actividad empresarial.

La Política de protección de datos personales se aplicará a todo el personal de la Compañía, a sus administradores, directivos y empleados, así como a todas las personas externas a ellas que se relacionen con la Compañía, independientemente de la naturaleza jurídica del vínculo que les una con Sayoscarrera como, por ejemplo, clientes, proveedores, auxiliares y colaboradores.

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos (DPO), y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

9 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 se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

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

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.
Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos (DPO), además se coordinarán los planes del tratamiento del riesgo.

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de la **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.

Toda la información accesible por todo el personal de Sayoscarrera, se encuentra en el portal ENS

Adicionalmente el desrrollo los aspectos técnicos específicos relacionados con la gestión, administración y operación de los sistemas de información y comunicaciones se detalla en la **Normativa de seguridad IT**
La normativa de seguridad IT estará disponible en la intranet, de acceso restringido.

11 OBLIGACIONES DEL PERSONAL

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

Todos los miembros de Sayoscarrera atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de Sayoscarrera 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

12 TERCERAS PARTES

Cuando Sayoscarrera preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad.

Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando Sayoscarrera 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, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.
Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que Sayoscarrera pueda

supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte.

Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos.

Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación.

El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

13 GESTIÓN DE INCIDENTES DE SEGURIDAD

Sayoscarrera dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

14 ESTRUCTURA DE LA INFORMCIÓN

La información vinculada al ENS reside en un Repositorio centralizado.

15 MODIFICACIONES DE LA POLITICA Y ENTRADA EN VIGOR

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

Barcelona a **29 de junio de 2026**

DocuSigned by:
Rosa Artisó Carrera
EEC7F6B056204A8...

Rosa Artisó Carrera

Directora General