POLÍTICA DE SEGURIDAD

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día **20 de noviembre de 2023** 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.

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.

5 MARCO NORMATIVO

El marco normativo en materia de seguridad de la información en el que Sayoscarrera desarrolla su actividad, esencialmente, es el siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional 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 y por el que se deroga la Directiva 95/46/CE
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantia de derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

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

- Guías CCN-STIC:

  - 201 Organización y gestión para la seguridad de las TIC
  - 402 Organización y gestión para la seguridad de las TIC
  - 800 Glosario de términos
  - 801 Responsabilidades y funciones
  - 802 Auditoria del ENS
  - 803 Valoración de sistemes
  - 804 Guía de implantación del ENS
  - 805 Política de Seguridad de la información
  - 806 Plan de Adecuación al ENS
  - 807 Criptología de empleo del ENS/Nueva
  - 808 Verificación del cumplimiento de las medidas en el ENS/Nueva
  - 809 Declaración y Certificaciónde Conformidad con el ENS/Nueva
  - 811 Interconexión con el ENS
  - 812 Seguridad en servicios web
  - 814 Seguridad en servicios de correo
  - 815 Métricas e indicadores
  - 817 Gestión de ciberincidentes
  - 818 Herramientas de seguridad
  - 820 Protección contra denegación de servicio
  - 821 Normas de Seguridad del ENS
  - 822 Procedimientos de Seguridad
  - 823 Cloud Computing
  - 824 Informe Nacional del estado de Seguridad (INES)
  - 825 Certificaciones 27001

- 830 Ámbito de aplicación del ENS
- 835 Borrado de metadatos en el marco del ENS

- Metodología Magertit

- UNE-EN-ISO 9001:2015 Sistemas de gestión de la calidad.

6 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
- Delegado de Protección de Datos (DPO)
- Responsable/ Encargado del Tratamiento

6.1 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.
- 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.

6.2 ROLES – FUNCIONES Y RESPONSABILIDADES

6.2.1 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 Normativa de Seguridad.
- Aprueba el Análisis de Riesgos.
- Aprueba el Riesgo residual.

6.2.2 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.

6.2.3 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.

6.2.4 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.
- 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.

6.2.5 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.
- 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.
- 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.

6.2.6 ADMINISTRADOR DE SEGURIDAD

Sus funciones más significativas serán las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración 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 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.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- 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.

6.2.7 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.

6.3 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, a propuesta del Responsable 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: Rosa Artisó Carrera
- Responsable de la Información/ Servicio
  - Área consultoria e Ingeniería: Director Área Consultoria e Ingeniería
  - Área gestión de costes TEM: Director Área TEM
  - Área de CGO-SOC: Director Área Consultoria e Ingeniería
  - Área Gestión RRHH: Directora Administración
  - Área Gestión Económica: Directora Administración
  - Área Gestión SSII: Director Área Consultoria e Ingeniería
  - Área Gestión Comercial: Directora Administración

- Responsable de Seguridad: DXX
- Responsable del Sistema: SXX
- Responsable del Sistema (contingència): RXX

- Administrador de Seguridad: JXX
- Administrador de Seguridad: MXX
- Delegado de Protección de Datos (DPO): nifled tic&law
- Responsable/ Encargado del Tratamiento: Rosa Artisó Carrera

6.4 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
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	
Normativa de seguridad	A	C	C	R	C	I
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	
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.

6.5 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.

6.6 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.

6.7 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.

7 DATOS DE CARÁCTER PERSONAL

Sayos&Carrera, S.L. 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 Sayos&Carrera, S.L., como, por ejemplo, clientes, proveedores, auxiliares y colaboradores.

8 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

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

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

9 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.

10 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.

11 TERCERAS PARTES

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

Cuando 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.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

12 ESTRUCTURA DE LA INFORMCIÓN

La información vinculada al ENS reside en un Repositorio centralizado.

13 REVISIÓN DE LA POLÍTICA DE SEGURIDAD

Con una periodicidad mínima de 1 año, o bien cuando existan cambios que así lo requieran, el Responsable de Seguridad revisarà la Política de Seguridad y propondrá a la Dirección su aprobación.

Una vez aprovada, se informarà a todos los empleades y colaboradores de Sayoscarrera de la existencia en el Repositorio de una nueva versión.

Barcelona a **20 de noviembre de 2023**

Rosa Artisó Carrera

Directora General