SCAYLE | Junta de Castilla y León

SGSI-POL-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

1. INTRODUCCIÓN

La Fundación Centro de Supercomputación de Castilla y León, en adelante **SCAYLE**, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos. El uso de estos sistemas exige establecer pautas y procedimientos para tratar y gestionar los riesgos asociados a la seguridad de la información que puedan afectar a la **disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad**. La gestión de la seguridad de los sistemas de información es un proceso complejo que incluye a personas, tecnologías, normas y procedimientos.

SCAYLE tiene presente que la ciberseguridad 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, calidad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para todos los proyectos.

Para SCAYLE, la seguridad de la información pretende garantizar la calidad de la información y la prestación adecuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar incidentes y reaccionando con presteza a los incidentes para recuperarse lo antes posible, según lo establecido en el artículo 8 del Esquema Nacional de Seguridad (ENS), así que establecerá las medidas técnicas, organizativas y de control que garanticen el logro de los objetivos.

Por lo anterior, SCAYLE establecerá un Sistema de Gestión Integrado (SGI) en su vertiente de Seguridad de la Información (SGSI) como instrumento necesario y facilitador de las operaciones de la fundación para atender las atribuciones y competencias de las que se dota a la entidad en el ámbito de actuación del **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad** y demás normativas de aplicación; entre las que se encuentran las recogidas en apartado de **Marco Normativo** que se integra en esta Política.

El ENS es útil para SCAYLE en la gobernanza y gestión de la tecnología aplicando estándares y buenas prácticas que nos ayuden a responder a los retos y desafíos de la realidad digital en la que estamos inmersos. Esta política de seguridad tomará como base los siguientes principios y directrices, para que las amenazas existentes no se materialicen, o si se materializan no afecten gravemente a la información que se maneja ni a los servicios prestados. Para ello actuará en 4 direcciones fundamentales:

1.1 Prevención

SCAYLE debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán las medidas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Para garantizar el cumplimiento de la política, SCAYLE debe:

- 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 terceros para obtener una evaluación independiente.
- Velar por el mantenimiento y mejora constante de la gestión de la seguridad y la calidad, aportando los recursos necesarios.
- Asumir el establecimiento y revisión periódica de los objetivos de la seguridad de la información y la calidad, persiguiendo el alineamiento con la estrategia, la excelencia, la garantía en la prestación de servicios, la aportación de valor para las partes interesadas y la optimización de costes.
- Asegurarse de que esta Política es comunicada y entendida por todo el personal y puesta a disposición de las partes interesadas, según sea apropiado.

1.2 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.

1.3 Respuesta

SCAYLE:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecerá protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

1.4 Recuperación y Conservación.

SCAYLE garantizará la conservación de los datos e información, para asegurar la disponibilidad de los servicios y dispondrá de los medios, técnicas y procedimientos necesarios que permitan garantizar la recuperación de los servicios más críticos.

2. OBJETIVOS

- Velar por la calidad y seguridad de la información, en sus distintas dimensiones.
- Lograr mayor concienciación de los usuarios respecto a la seguridad de la información.
- Garantizar la prestación continuada de los servicios.
- Asegurar la correcta protección y tratamiento de datos.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes necesarios que se definan para los distintos servicios ofrecidos por SCAYLE.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

3. ALCANCE

3.1 Alcance subjetivo

Los sujetos obligados por esta Política son: todo el personal de SCAYLE y todas aquellas personas, instituciones, entidades y usuarios, sean internos o externos, que tenga acceso a la información, instalaciones o los sistemas del Centro, sea en las instalaciones de SCAYLE o en remoto.

En este ámbito se incluyen los siguientes:

- A todos los departamentos, tanto a sus directivos como a empleados, así como miembros del Patronato.
- A los contratistas, subcontratistas, clientes, proveedores, usuarios o cualquier otra tercera parte que tenga acceso a la información, instalaciones o los sistemas de la organización.

3.2 Alcance objetivo

El alcance objetivo de esta Política comprende todos los sistemas de información[1] de SCAYLE que den soporte a sus servicios y procesos, y afecta a todos los activos de información sustentados en ellos, así como a las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

En este ámbito se contienen entre otros:

[1] Se entiende por "sistema de información" en sentido amplio, como "aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información." (UNE-EN ISO/IEC 27000:2021)

- Las bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- La información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- La información cedida en un marco legal establecido, que se considerará propia para su protección.
- Todos los sistemas utilizados para administrar y gestionar la información sean propios de SCAYLE, alquilados o licenciados por la misma.
- Concretamente, los sistemas de información que dan soporte a los servicios de:

    - Cálculo científico en superordenadores.
    - Cloud Computing.
    - Comunicaciones avanzadas de la red de ciencia y tecnología de Castilla y León (Redcayle).
    - Almacenamiento de datos científicos (Opencayle).
    - Notario Digital.
    - Jornadas y cursos.

Si bien, los servicios que se encuentran dentro del alcance de la certificación del ENS conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad son los siguientes:

- Cálculo científico en superordenadores.
- Cloud Computing.
- Comunicaciones avanzadas de la red de ciencia y tecnología de Castilla y León (Redcayle).
- Jornadas y cursos.

4. MISIÓN DE SCAYLE

La Fundación Centro de Supercomputación Castilla y León (**SCAYLE**) es una entidad pública creada por la Junta de Castilla y León y la Universidad de León, que tiene por objeto la mejora de las tareas de investigación de la universidad, los centros de investigación y las empresas de Castilla y León.

Tiene como Misión principal:

- La mejora de las tareas de investigación de las Universidades, de los Centros de Investigación y de las empresas de Castilla y León, promoviendo acciones de innovación en el mundo de la Sociedad del Conocimiento y proporcionando un entorno de trabajo excelente en las áreas de cálculo intensivo, las comunicaciones y los servicios avanzados, contribuyendo mediante el perfeccionamiento tecnológico al desarrollo económico de la Comunidad y a la mejora de la competitividad de las empresas.

- La gestión de recursos e infraestructuras de tecnologías de la información y de las comunicaciones y los servicios asociados.

5. VIGENCIA

Esta Política de Seguridad de la Información (PSI) la revisó el Comité de Seguridad de la Información y la aprobó la Dirección General de SCAYLE, estableciendo las directrices generales para aplicar el marco legislativo y normativo del Esquema Nacional de Seguridad.

Una vez aprobada, se hará difusión de la misma, poniéndola a disposición tanto de sus empleados y personal interno, como al resto de personas interesadas. Por lo que desde el momento en que se haga pública, la Política será de obligatorio cumplimiento.

Cualquier modificación posterior entrará en vigor inmediatamente después de su aprobación y publicación. Las versiones anteriores quedarán derogadas desde la entrada en vigor de la última versión.

6. REVISIÓN Y EVALUACIÓN

La gestión de la **Política de Seguridad de la Información (PSI)** corresponde al **Comité de Seguridad** de SCAYLE que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente el Comité de Seguridad revisará esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La revisión se orientará, tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información y protección de datos, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc. **La PSI será aprobada por la Dirección General** y difundida para que la conozcan todas las partes afectadas.

7. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de SCAYLE, para ello:

- En SCAYLE se reconoce la importancia de la información y la necesidad de su protección, por constituir un activo estratégico y vital, hasta llegar a

poner en peligro la continuidad de la Institución, o suponer daños muy importantes, si se produce una pérdida total e irreversible de determinados datos.

- SCAYLE implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad y las normativas aplicables en materia de Protección de Datos, y cumple con los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios electrónicos incluidos en el alcance del ENS es de la Dirección General, que pondrá los medios adecuados, sin perjuicio de que el personal empleado o los usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en estas normas y en los procedimientos complementarios. En el punto 10 "**Organización de la Seguridad**" de este mismo documento se describen las funciones y responsabilidades del Comité de Seguridad, que gestionará la seguridad de la información, y de sus miembros.
- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- SCAYLE fija como objetivo realizar el trabajo de forma correcta a la primera y al mínimo coste.
- Se ha identificado a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.
- Se establecerá dentro de la normativa un sistema de clasificación de la información con diferentes niveles.
- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de SCAYLE.
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán sancionarse según la legislación laboral o con el régimen disciplinario de funcionarios y sin perjuicio de otras sanciones a que hubiere lugar, o con sanciones

personalizadas si están vinculados a SCAYLE bajo contratos no laborales, según las cláusulas de dichos contratos en este último caso.

- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a personal y a colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de SCAYLE deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.
- El personal de SCAYLE debe esforzarse en la prevención de errores y en el control efectivo de los mismos. Su prevención tendrá prioridad frente al esfuerzo para corregirlos.
- A través de una planificación y seguimiento adecuados, SCAYLE orienta su organización hacia la consecución de la mejora continua de la eficacia en la calidad, cuidado del medioambiente, e I+D+i de sus servicios. Esta planificación y seguimiento deben estar basados en datos objetivos y realimentados de forma continua.
- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.
- Mediante una planificación adecuada y conveniente de la formación, SCAYLE aumenta la capacidad y destreza de sus empleados en las actividades que realizan para garantizar la satisfacción de las expectativas de las partes interesadas.
- Todos los empleados deberán conocer la política y los objetivos del sistema.
- SCAYLE desarrolla su actividad para tener un impacto mínimo sobre el medioambiente. Además, enfoca su cartera de productos y servicios como modelo de desarrollo sostenible con un aprovechamiento eficiente de los recursos evitando la contaminación del medioambiente.
- SCAYLE se compromete a incorporar tecnologías limpias en la medida de lo posible y diseñar, controlar y mejorar los procesos en pro de la prevención de la contaminación. SCAYLE debe ser un referente en Eficiencia Energética en instalaciones TIC ultra-densas.
- La dirección de SCAYLE mantiene un marcado compromiso con la investigación, el desarrollo y la innovación tecnológica como clave para el desarrollo regional.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.

- Implantar los mecanismos necesarios para que quien acceda o pueda acceder a los activos de información, conozca sus responsabilidades y así se reduzca el riesgo derivado de un uso indebido, logrando concienciar a los usuarios sobre la seguridad de la información.
- Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades del nivel de servicio de sus usuarios.
- Se adoptarán las medidas técnicas y organizativas necesarias para atender los riesgos generados por el tratamiento de datos y así cumplir con la legislación de seguridad y privacidad.

8. PRINCIPIOS BÁSICOS DE SEGURIDAD

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral (art. 6).
b) Gestión de la seguridad basada en los riesgos (art. 7).
c) Prevención, detección, respuesta y conservación (art. 8).
d) Existencia de líneas de defensa (art. 9).
e) Vigilancia continua (art. 10).
f) Reevaluación periódica (art. 10).
g) Diferenciación de responsabilidades (art. 11).

8.1 La seguridad como proceso integral

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad

8.2 Gestión de la seguridad basada en riesgos

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

8.3 Prevención, detección, respuesta y conservación

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

8.4 Existencia de líneas de defensa

El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
b) Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

8.5 Vigilancia continua y reevaluación periódica

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas

8.6 Diferenciación de responsabilidades

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.
La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.
La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

9. REQUISITOS MÍNIMOS DE SEGURIDAD

La Política de Seguridad de la Información (**PSI**) articula la gestión continuada de la seguridad. Se ha establecido de acuerdo con los principios básicos señalados en el capítulo III del Real Decreto 311/2022 y se desarrolla teniendo en cuenta la aplicación de los siguientes requisitos mínimos de seguridad:

- Análisis y gestión de los riesgos (art. 14).
- Gestión de personal (art. 15).
- Profesionalidad (art. 16).
- Autorización y control de los accesos (art. 17).
- Protección de las instalaciones (art. 18).
- Adquisición de productos de seguridad y contratación de servicios de seguridad (art. 19).
- Mínimo privilegio (art. 20).
- Integridad y actualización del sistema (art. 21).
- Protección de información almacenada y en tránsito (art. 22).
- Prevención ante otros sistemas de información interconectados (art. 23).
- Registro de actividad y detección de código dañino (art. 24).
- Incidentes de seguridad (art. 25).
- Continuidad de la actividad (art. 26).
- Mejora continua del proceso de seguridad (art. 27).

10. MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables a SCAYLE en materia de Seguridad de la Información son:

- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad (ENS)**.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).
- 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 (Reglamento general de protección de datos)
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Documentos y Guías CCN-STIC, en especial la Guía "CCN-STIC-821 Normas de seguridad en el ENS", el Anexo I de la Guía "CCN-STIC-822" – Procedimientos de seguridad en el ENS" y la Guía CCN-STIC 801-Responsabilidades y funciones.

11. ORGANIZACIÓN DE LA SEGURIDAD

11.1 Dirección General

La **Dirección General**, desde el cargo del Director/a General de SCAYLE tiene las siguientes funciones en el campo de la seguridad de la información:

- Decidir sobre la creación de un Sistema de Gestión de la Seguridad de la Información.
- Promover el cumplimiento de los marcos normativos que rigen en torno a la seguridad de la información. En particular el Esquema Nacional de Seguridad (ENS).
- Participar en el Comité de Seguridad con el rol o roles que este establezca.
- Velar porque la seguridad de la información se tenga en cuenta en todas las áreas de la organización.

11.2 Comité de Seguridad de la Información

El Comité de Seguridad de la información de SCAYLE, es un órgano colegiado que coordina la seguridad de la información en la entidad y estará formado por:

- **Responsable del Servicio.**
- **Responsable de la Información.**
- **Responsable de Seguridad.**
- **Responsable del Sistema.**
- **Delegado de Protección de Datos**
- **Secretaria/o del Comité de Seguridad de la Información**: en todo caso, Responsable de Seguridad.

En caso de que alguno de los miembros del Comité de Seguridad se encontrase de vacaciones, viaje profesional, baja, congresos, cursos o similares… otro miembro del Comité de Seguridad asumirá sus funciones durante dicha ausencia.

11.2.1 Procedimiento de designación y revisión.

La Dirección de la organización, será quien designe a los miembros del Comité.

La composición del Comité de Seguridad se especificará de forma concreta en el documento de **Composición del comité de Seguridad (SGSI-POL01-A1)**.

Estos nombramientos **se revisarán mínimo cada 2 años** o cuando el puesto quede vacante.

11.3 Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

11.3.1 Comité de Seguridad

El Comité de Seguridad tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de SCAYLE 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 de la información para que sea aprobada por la organización.
- Aprobar 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 SCAYLE y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. 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 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 SCAYLE. 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 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, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la organización.

11.3.2 Responsable de la Información

- Tiene la potestad de determinar los niveles de seguridad de la información.
- Tiene la potestad de aprobar formalmente el nivel de seguridad de la información.
- Tiene la potestad de establecer los requisitos de la información en materia de seguridad.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en

materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

11.3.3 Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Valora las consecuencias de un impacto negativo sobre la seguridad de la información atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

11.3.4 Responsable de Seguridad

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- Velará por que en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilicen, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad

- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de SCAYLE.
- 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.
- Actuar como POC (persona o punto de contacto) de la entidad. Se encargará de analizar y supervisar, tanto el cumplimiento de los requisitos de seguridad de los servicios prestados o soluciones que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dichos servicios.

11.3.5 Responsable del Sistema

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- 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.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

11.3.6 Delegado de Protección de Datos

- 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 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, 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 de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

11.3.7 Secretaria/o del Comité de Seguridad

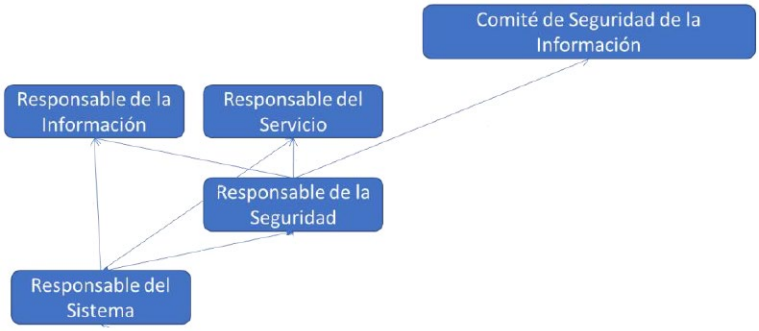
- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Responsabilizarse de la ejecución directa o delegada de las decisiones del Comité.

11.4 Mecanismos de coordinación

Rol. Responsable	Proceso de decisiones - Mecanismos de coordinación
Responsable de la Seguridad y Secretaria/o	El Responsable de Seguridad, debe reportar directamente a la Dirección o a los órganos de gobierno de la entidad y, al Comité de Seguridad de la Información. 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.

	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. Reportará **al Comité de Seguridad**, 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.
Responsable del Sistema	El Responsable del Sistema: **Reportará al Responsable de la Información** de las incidencias funcionales relativas a la información que le compete. **Reportará al Responsable del Servicio** de las incidencias funcionales relativas al servicio que le compete. **Reportará al Responsable de la Seguridad** en materia de seguridad. Así como 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.

Los mecanismos de coordinación se corresponden con los representados en los siguientes gráficos:



El Comité de Seguridad de la Información resolverá los **posibles 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 a la **Dirección General.**

En caso de **conflicto entre los diferentes responsables** de información o de servicio que componen la estructura organizativa de la Política de

Seguridad de la Información de SCAYLE, éste será resuelto por el superior jerárquico de los mismos.

11.5 Comité de Seguridad. Compatibilidades e incompatibilidades

		Organizaciones de reducida dimensión que funcionan de forma autónoma (SCAYLE)				
Rol	**Notas**	R. Sistema	R. Servicio	R. Información	R. Seguridad	Delegado Protección
Responsable del Sistema	El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. A excepción de situaciones insólitas en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica. (art. 13.3. ENS)		No	No	No	Sí
Responsable del Servicio	Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tiene sentido: • Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio. • Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.	No		Sí	No	Sí
Responsable de la Información		No	Sí		No	Sí
Responsable de Seguridad	Ocupará la posición de Secretario del Comité de Seguridad además de las funciones previstas en la normativa. (*) Incompatibilidades: Las descritas anteriormente y las que se incluyen en la normativa, incluida la del Delegado de Protección de Datos El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. A excepción de situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica.	No	Sí	No		Sí
Delegado de Protección Datos	Preferiblemente no deberá coincidir con el rol de Responsable de seguridad (Guía 801 CCN- 113).	Sí	Sí	Sí	NO.	

12. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

12.1 Política de Uso Aceptable

Los sistemas de información y la información se utilizarán solo para los fines y propósitos para los que se han puesto a disposición de los usuarios.

No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

12.2 Seguridad Física del entorno

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

12.2.1 Áreas seguras

Las áreas seguras son los lugares donde se encuentra localizada la información crítica para la organización. Éstas están protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.

- El control de acceso físico a los locales del SCAYLE, así como la seguridad de los entornos de trabajo de oficinas es responsabilidad del área técnica de SCAYLE.
- Solamente el personal autorizado o debidamente identificado podrá acceder a las áreas seguras.
- Ningún proveedor o visitante podrá tener acceso a las instalaciones de SCAYLE, salvo autorización y supervisión por parte de personal de SCAYLE.
- El almacenamiento o manipulación de sustancias peligrosas o inflamables, se realizará en las dependencias alejadas de las zonas seguras.
- Los usuarios velarán siempre por el cumplimiento de la normativa en materia de seguridad y prevención de riesgos laborales, adoptándose las medidas que propongan los servicios encargados del control y revisión de estas materias.

12.2.2 Seguridad de los equipos

- Los equipos se deben situar de forma que se minimice el riesgo de acceso por personal no autorizado a ellos.
- Está prohibido comer, beber o fumar junto a equipos o soportes informáticos. Quedan excluidas los recipientes de bebida con tapa en los puestos de trabajo.
- Los equipos que salgan o permanezcan fuera de los locales de la organización, deberán controlarlos permanentemente, no deberán quedar desatendidos ni fuera del alcance o visión del empleado. La salida de soportes o equipos requerirá autorización expresa de SCAYLE.
- El transporte de equipos portátiles se realizará en bolsas o maletines discretos que gocen preferiblemente de cierres de seguridad.
- Deberá tenerse cuidado durante el transporte de equipos portátiles para evitar superar las condiciones atmosféricas que impidan o dañen su funcionamiento.
- Los equipos, soportes o dispositivos portátiles que deban ser reutilizados por otros usuarios o eliminada la información que contienen, serán entregados al Responsable de Seguridad, quien previa verificación de que la información que contienen ha sido convenientemente salvaguardada, procederá a la eliminación de dicha información mediante dispositivos de borrado seguro. Si el usuario al que se le entregue el uso de un dispositivo, equipo o

soporte reutilizado advirtiera la presencia de información con datos de carácter personal, de usuarios anteriores, informará al Responsable de Seguridad del Centro de Supercomputación.

- Queda expresamente prohibida la salida de equipos, soportes o documentos que contengan datos de carácter personal, por usuarios que no hayan sido previamente autorizados.

12.3 Gestión de Comunicaciones y Operaciones

12.3.1 Procedimientos operativos y responsabilidades

SCAYLE controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red del Centro y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

12.3.2 Protección frente a código malicioso

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de SCAYLE.

Todo software adquirido por la organización sea por compra, donación o cesión, es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Responsable de Seguridad y autorizado por el Pleno.

El Responsable del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

12.3.3 Gestión de la seguridad de la red

Los elementos de red (switch, router...) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

12.3.4 Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

12.4 Control de Acceso

12.4.1 Requisitos del servicio para el control de accesos

- La regla general que aplica el SCAYLE, para determinar el grado de acceso de los usuarios de los sistemas a la información, consiste en conceder únicamente acceso a la información a aquellas personas que lo requieren estrictamente para el desempeño de sus funciones.
- Los usuarios tendrán acceso únicamente a los recursos a los que expresamente hayan sido autorizados.
- El Responsable de Seguridad velará por la implantación de los controles técnicos necesarios para evitar que materialmente se puedan acceder a recursos expresamente no autorizados.

12.4.2 Gestión de accesos de los usuarios

- El acceso a los recursos de SCAYLE se realizará con un proceso previo de identificación y control de acceso, para controlar a quien pueda acceder a la información.
- SCAYLE mantiene listados de usuarios autorizados para el acceso a los recursos de información.

- Los permisos de acceso a la información se conceden considerando los niveles de confidencialidad y de la información y las necesidades operativas del negocio.
- Los permisos de acceso al sistema, instalaciones y /o aplicaciones informáticas, son concedidos por el Responsable de Seguridad a través del procedimiento establecido al efecto.

12.4.3 Responsabilidades del usuario

- El usuario debe respetar la confidencialidad de los datos a los que tenga acceso durante el desempeño de sus funciones, evitando facilitar datos personales o confidenciales a terceros que no estén autorizados para su acceso. Estas obligaciones subsistirán incluso una vez finalizada la relación contractual que ha permitido el acceso del usuario a la información.

- El usuario debe conocer que los sistemas de información son supervisados y monitorizados por el Departamento informático, para garantizar su correcto funcionamiento y seguridad. Por tanto, el usuario debe saber que cualquier información de índole personal que introduzca en los sistemas de información (incluido el correo electrónico) puede ser conocido por otros usuarios que desempeñan esas funciones de supervisión, control y monitorización de los sistemas.

12.4.4 Control de acceso a la red

- Está prohibido obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos de SCAYLE, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Se permitirá el acceso a la red corporativa desde el interior y desde el exterior de las instalaciones, solo a los usuarios que lo necesiten para el desempeño de sus funciones y hayan sido autorizados.
- El envío electrónico de información y la utilización de Internet por parte de los empleados se permite solo en relación con el desempeño de las actividades laborales correspondientes a cada empleado, no se permite su uso para finales distintas a las mencionadas anteriormente.
- Los usuarios con derecho de acceso a la red corporativa desde fuera de las instalaciones de la organización, deberán realizar el acceso desde equipos que hayan sido expresamente verificados y autorizados por el Responsable de Sistemas. En circunstancias excepcionales y siempre que se adopten medidas de seguridad que garanticen la ausencia de virus y malware en los equipos utilizados para la conexión, se podrán emplear equipos no verificados previamente, debiendo comunicar dicha circunstancia al Departamento informático, con carácter previo a su conexión.
- Se informa a los usuarios que existen medidas técnicas parar el control y seguimiento de las conexiones que se realizan a la red,

especialmente las realizadas desde fuera de la organización, así como para el control del uso profesional de Internet y correo electrónico.

- El usuario debe tener presente que las comunicaciones a través de internet no revisten en muchas ocasiones las condiciones idóneas de seguridad, por lo que:
    - No deberán utilizarse para la transmisión de información confidencial o datos de carácter personal. Si fuera necesario la transmisión de este tipo de información a través de Internet, deberá consultarse con el Departamento Técnico, las condiciones técnicas necesarias a aplicar.
    - La transmisión de datos personales y los de nivel alto (como los de salud), a través de redes de telecomunicaciones, se hará cifrando dichos datos o usando cualquier mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

- Queda expresamente prohibido:
    - La visualización de material con contenido sexual, obsceno, ofensivo, racista o que pueda ser considerado ilícito, a través de la red corporativa o servicios de internet de SCAYLE.
    - El uso de sistemas de mensajería instantánea (salvo que se utilice para la comunicación con clientes, proveedores o empleados de la SCAYLE, su uso se ajuste a una finalidad productiva y laboral y haya sido previamente autorizado por el Responsable de Seguridad de SCAYLE).
    - El uso y la instalación de programas que permitan el acceso a redes P2P (emule, edonkey, etc.), así como cualquier otro tipo de acceso a entornos o plataformas que permitan el intercambio de ficheros sin la previa y expresa autorización del Responsable de Seguridad. Este tipo de programas pueden ayudar a superar los sistemas de defensa ante accesos no autorizados y son un canal de entrada de virus y programas espía.
- Los logos, marcas y demás signos distintivos de SCAYLE no podrán ser utilizados por el usuario en Internet salvo que se trate de alguna actividad desarrollada en representación de SCAYLE y se encuentre autorizada.
- El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. se limita a aquéllos que contengan información relacionada con la actividad de SCAYLE o con los cometidos del puesto de trabajo del usuario, salvo en el caso de que se cuente con autorización expresa para ello.
    - SCAYLE podrá establecer filtros para garantizar el cumplimiento de esta obligación.
    - Queda prohibido participar en foros o páginas de debate en Internet, salvo autorización de la Dirección General. SCAYLE no se responsabiliza de la emisión de opiniones personales de los usuarios en Internet o a través del correo electrónico, debiendo abstenerse el Usuario de emitir dichas opiniones empleando recursos, logos o signos distintivos propiedad de SCAYLE.

- Los Usuarios deben tomar conciencia de que cuando acceden a una página de Internet, cada servidor web puede obtener información relacionada con el individuo, la computadora que estuvo utilizando y los otros sitios web que estuvo visitando durante la sesión. Por este motivo, debe mantenerse la discreción al escoger los sitios web que se visitan desde un equipo de SCAYLE.

12.4.5 Información móvil y teletrabajo

Cuando los equipos o la información propiedad de SCAYLE están fuera de las instalaciones, el empleado deberá adoptar las siguientes medidas adicionales de seguridad:

- Los equipos o medios portátiles deberán tener siempre activada la protección antivirus y medidas que impidan o limiten el acceso de personas no autorizadas.
- Los teléfonos móviles, tabletas y demás dispositivos móviles propiedad de SCAYLE con datos personales incluidos en ficheros de SCAYLE, deberán tener un sistema de control de acceso con pin o contraseña.
- En cuanto regresen a las instalaciones de SCAYLE los equipos o medios portátiles, se copiarán los archivos generados fuera de dichas instalaciones eliminando la copia local en el medio portátil.
- Durante la utilización de equipos o dispositivos móviles fuera de las instalaciones de SCAYLE, se evitará su trabajo en lugares expuestos a la vista de personas no autorizadas.
- Deberá tenerse cuidado durante el transporte de equipos portátiles para evitar superar las condiciones atmosféricas que impidan o dañen su funcionamiento.
- Los equipos, soportes o medios portátiles que transporten o almacenen información con datos de carácter personal fuera de las instalaciones de SCAYLE, deberán poseer medidas de seguridad suficientes para impedir el acceso de terceros a dicha información

13. DATOS DE CARÁCTER PERSONAL

SCAYLE solo recogerá datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan recabado.

- SCAYLE adoptará las medidas de índole técnica y organizativas, necesarias para el cumplimiento de la normativa de protección de datos vigente en cada caso.

- La Política de Protección de Datos Personales está publicada en el portal web de SCAYLE.

Todos los sistemas de información de SCAYLE se ajustarán a los requisitos requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado 9. Marco Normativo, de la presente

Política de Seguridad de la Información.Además, se ha nombrado un Delegado de Protección de Datos.

14. ANÁLISIS Y 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 establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

15. GESTIÓN DEL PERSONAL

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

- Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial.
- Dentro de la relación laboral o contractual, se deberán desempeñar siempre las funciones asignadas con profesionalidad, es decir, realizar un ejercicio adecuado de la profesión con capacidad y eficacia. En concreto, se recogerán los mínimos de experiencia y cualificación que debe tener el empleado en la Relación de Puestos de Trabajo".
- Todas las políticas y procedimientos de seguridad deberán comunicarse regularmente a todos los trabajadores y usuarios terceros si procede.
- Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos. Asimismo, cuando los empleados de la entidad o personal externo se encuentren de baja laboral o situación asimilable, se les podrá requerir para que depositen en las dependencias de SCAYLE cualquier dispositivo propiedad de la Fundación que tengan a su disposición y se podrá proceder al bloqueo temporal de su cuenta hasta que finalice la baja laboral o situación asimilable.

15.1 Obligaciones del Personal

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

El incumplimiento de las obligaciones impuestas como usuario pueden ser objeto de sanción disciplinaria por parte de SCAYLE que podría desembocar en el despido, así como a la adopción de acciones jurídicas tendentes a la exigencia de responsabilidades y reparación de los daños y perjuicios causados, de todo lo cual he sido informado de forma adecuada y comprensible.

Todas las personas con responsabilidad dentro de SCAYLE deberán de recibir una formación acorde a la función de responsabilidad que estén ejerciendo dentro de la organización para que puedan desempeñar dicha función de la manera más eficaz y eficiente posible.

16. TERCERAS PARTES

Cuando SCAYLE 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 incidentes de seguridad.
- Se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SCAYLE utilice servicios de terceros o ceda información a terceros:

- Se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a los servicios o información.
- La 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.

Se desarrollará un procedimiento de seguridad en relación con la gestión de proveedores donde se documentan las consideraciones en materia de seguridad de la información en cuanto a:

- La adquisición de nuevos componentes
- La contratación de proveedores

- La gestión de dichos contratos.

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.
- La aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

17. GESTIÓN DE LA CONFIGURACIÓN

La gestión, configuración y actualización del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información se realizará siempre siguiendo los principios de seguridad por defecto y mínimo privilegio.

Los sistemas se configurarán de forma que sean seguros por defecto, es decir, de forma que los usuarios realicen un uso seguro, salvo que conscientemente reduzcan la seguridad o se expongan a riesgos.

Se aplicará por defecto el **principio de mínimo privilegio**.

18. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema por lo que se ha realizado un procedimiento específico de autorización.

Es importante que los sistemas se encuentren al día en relación a las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones, por lo que también se ha establecido que debe mantener el equipamiento y gestionar parches y vulnerabilidades.

19. PROTECCIÓN DE LA INFORMACIÓN

SCAYLE implantará medidas físicas y lógicas para proteger la información allí donde se encuentre almacenada, tanto si se encuentra en un soporte físico o digital. Se realizarán copias de seguridad que aseguren la posibilidad de recuperación en caso de incidente.

19.1 Copias de Seguridad

Los datos deben ser guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente.

19.2 Intercambio de Información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

20. SEGUIMIENTO Y MONITORIZACIÓN

Se definirá una estrategia global de monitorización de sistemas y actividades, identificando los sistemas más críticos y estableciendo los controles oportunos para registrar cualquier evento que debe ser detectado (actividades no autorizadas o funcionamientos inadecuados de sistemas). Los registros deberán ser almacenados convenientemente protegidos contra su modificación o eliminación.

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implica realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida, así como para recomendar cualquier cambio que se estime necesario.

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades no autorizadas. Esto implicará realizar tareas para inspeccionar los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos, y recomendar cualquier cambio que se considere necesario.

21. GESTIÓN DE INCIDENTES DE SEGURIDAD

Cualquier usuario que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente para que se tomen las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a las incidencias en materia de seguridad. Existirán procedimientos que abarquen todos los tipos posibles de incidentes.

El usuario está obligado a notificar los incumplimientos de la presente normativa que detecte, así como cualquier tipo de incidencia, evento o circunstancia que ponga o pueda poner en peligro la seguridad de los datos personales y resto de información incorporados a nuestros ficheros.

El usuario deberá notificar esta circunstancia a través de la cuenta de correo **seguridad@scayle.es** de SCAYLE, debiendo facilitar al menos la siguiente información sobre la incidencia detectada:

- Descripción del hecho o circunstancia que motiva la incidencia.
- Fecha y hora en la que se produjo o se detectó.
- Usuario que notifica la incidencia.

El Departamentos informático, será el responsable de la tramitación de la incidencia que quedará registrada en la aplicación informática empleada al efecto.

El tramitador de la incidencia deberá dejar constancia de los efectos derivados de esta y de las medidas correctoras a aplicar para su subsanación. Si dentro de las medidas correctoras que debieran aplicarse para la subsanación de la incidencia, se incluyeran medidas relativas a la restauración de archivos desde las copias de respaldo o incluso la introducción manual de registros en programas o bases de datos, éstas deberán ser expresamente autorizadas por el Responsable de Seguridad.

A continuación, se exponen algunos ejemplos de incidencias o eventos a notificar:

- Detección de virus.
- Pérdida de equipos o soportes con datos personales.
- Detección de accesos no autorizados a información con datos personales.
- Detección de contraseñas no confidenciales.
- Detección de nombres de usuarios compartidos.
- Salidas de soportes con datos personales no autorizadas.
- Utilización de soportes no autorizados o de forma contraria a las normas de SCAYLE.
- Detección de documentos con datos personales abandonados o destruidos de forma incorrecta.
- Existencia de archivos con documentos que contienen datos personales en armarios o cajones no cerrados.
- Documentos con datos personales olvidados en bandejas de impresión.

Pérdida o robo de documentos con datos personales, etc.

22. GESTIÓN DE LA CONTINUIDAD DEL SERVICIO

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

- Es imprescindible para SCAYLE establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.
- Para garantizar la continuidad de la actividad en estos casos, SCAYLE establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá diversos controles para identificar y reducir riesgos y un procedimiento que limite sus consecuencias y asegure la reanudación de las actividades esenciales en el menor tiempo posible.
- La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia, que deberán probarse y actualizarse regularmente para comprobar su idoneidad.
- La gestión de la continuidad del servicio se incorporará a los procesos de SCAYLE y será responsabilidad de una o varias personas dentro de la entidad.

23. MEJORA CONTINUA

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

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

Para SCAYLE, la gestión adecuada de la ciberseguridad constituye un reto continuo y colectivo al que necesariamente se ha de enfrentar.

24. ESTRUCTURA DOCUMENTAL

La política de seguridad se desarrollará en la documentación de seguridad, que regulará normas específicas de seguridad de la información de un área o aspecto determinado, aprobadas por el Comité de Seguridad de la Información.

Esta documentación del Sistema de Gestión de Seguridad de la Información se estructurará en:

La documentación de seguridad es aprobada por el Comité de Seguridad.

Para clasificar la documentación se utilizan diversas técnicas, recursos e instrumentos archivísticos para almacenar los documentos lógicos y físicos. El

acceso a la documentación dependerá de la clasificación de confidencialidad establecida para cada documento.

La política de seguridad se desarrollará en la documentación de seguridad, que regulará normas específicas de seguridad de la información de un área o aspecto determinado, aprobadas por el Comité de Seguridad de la Información.

La relación jerárquica entre la documentación que se genera o afecta al funcionamiento de la entidad, es la que se muestra en la siguiente pirámide.

1.- **Leyes y reglamentos**: toda normativa externa a la entidad que resulta de aplicación, tanto de la comunidad autónoma, estatal, europea e internacional que resulte de aplicación.

2.- Los Manuales y las Políticas se encontrarán en el mismo nivel jerárquico.

Manuales: contienen descripciones de un tema u objeto, partes o conformaciones para guiar al lector sobre el material que tiene en su poder.

Políticas: representan una declaración de principios de una organización.

Las políticas se pueden considerar como las reglas o leyes que una organización debe cumplir. Las políticas son pautas generales para la acción que vienen determinadas por la gerencia o administración de la empresa y se basan en los objetivos y metas a lograr.

Son más genéricas y no especifican en concreto lo que debe hacerse.

Pueden entenderse como un conjunto de lineamientos y criterios para diseñar las estrategias que guíen a la organización a la consecución de los objetivos y metas planteados. Estas tienen como función primordial precisar la mayor parte de las situaciones que pudieran presentarse o que propicien la toma de decisiones de las autoridades superiores.

3.- Normativa interna: conjunto de lineamientos y criterios para orientar y guiar las actividades que realizan los trabajadores involucrados en sus respectivas

aéreas de trabajo. Las normas son lineamientos imperativos y específicos de acción que persiguen un fin determinado con mayor obligatoriedad en sus interpretaciones y aplicación; tienen como función primordial instruir a los trabajadores sobre cómo realizar determinadas tareas, acciones o actividades. Esto es conforme a los objetivos organizacionales establecidos.

4.- Procedimientos: forma específica de llevar a cabo una actividad o un proceso. Es decir, cuando se tiene un proceso que tiene que ocurrir en una forma concreta, y se especifica cómo sucede, se tiene un procedimiento.

Responde a la pregunta de ¿Cómo ejecutar un proceso?

En los procedimientos se definen los pasos específicos sobre cómo hacer cumplir, cumplir e implementar esas políticas o pasos a seguir para lograr algo.

5.- Instrucciones: Las instrucciones técnicas pueden ser parte de un procedimiento, o pueden ser referenciadas en el procedimiento. Las instrucciones técnicas tienen una estructura similar a los procedimientos y cubren los mismos elementos; pero las instrucciones técnicas detallan las actividades a realizar, enfocándose en la secuencia de cada paso, y en las herramientas y métodos que se utilizarán con la exactitud requerida.

Responden a la pregunta de ¿Cómo ejecutar una tarea?

6.- Registros: Recogerán evidencias de cumplimiento.

Formularios.

Actas: Recogen los acuerdos asumidos.

En concreto la documentación del Sistema de Gestión de Seguridad de la Información se estructurará principalmente en:

- **Primer nivel**: Formado por las políticas de alto nivel, como la presente Política de Seguridad de la Información del ENS.
- **Segundo nivel**: NORMATIVAS.
- **Tercer nivel**: los procedimientos de seguridad que describen cómo realizar tareas, en los que se detalla la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información.
- **Cuarto nivel:** instrucciones.
- **Quinto nivel**: registros, actas, estándares de seguridad, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, anexos, etc.

25. ANEXOS

SGSI-POL-01-A1: Composición Comité de seguridad.