UNIVERSIDAD DE LA RIOJA

POLÍTICA DE SEGURIDAD

(Aprobado en Consejo de Gobierno en sesión celebrada el 7 de febrero de 2019 y modificada en Consejo de Gobierno de 18 de marzo de 2022)

1. Introducción

1.1 Justificación de la Política de Seguridad de la Información

La Universidad de La Rioja, (en adelante **UR**) 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.

Los **objetivos** de la seguridad de la información son:

- Cumplir la legislación de seguridad y privacidad.
- Garantizar la calidad y protección de la información.
- Garantizar la prestación continuada de los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

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. Es por ello que el Esquema Nacional de Seguridad (Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010 de 8 de enero, ENS en adelante), en su artículo 11 establece que “Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente”.

Esto implica que las diferentes áreas de UR 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.

Todas las áreas 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. Las unidades deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

2. Objeto

El objeto del presente documento es establecer las bases generales de la seguridad de la información en la Organización.

3. Alcance

Esta Política se aplicará a los sistemas de información de la UR que dan soporte al ejercicio de derechos y el cumplimiento de deberes a través de medios electrónicos dentro del marco de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, así como de la Ley 40/2015 de Régimen Jurídico del Sector Público.

4. Misión y servicios prestados

La Misión de la Universidad de La Rioja es la prestación del servicio público de la educación superior mediante la investigación, la docencia y el estudio, de acuerdo con los principios de libertad, solidaridad

y pluralidad ideológica.

5. Marco normativo

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades de la Administración en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Ley 39/2015, de 1 de junio, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- El Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante) en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD, en adelante).
- El Reglamento General de Protección de Datos 679/2016, del Parlamento Europeo y del Consejo del 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 esos datos y por el que se deroga la Directiva 95/46/CE.

6. Responsabilidades

	Revisa	Aprueba
Política de Seguridad	Responsable de Seguridad	Consejo de Gobierno

7. Organización de la Seguridad

7.1 Definición de Roles

Tal como indica el artículo 12 del ENS, La seguridad deberá comprometer a todos los miembros de la organización. La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. Se establecen por tanto los siguientes roles en la organización relacionados con la Seguridad de la Información:

Rol	Funciones
Consejo de Gobierno	Órganos colegiados o unipersonales que deciden la misión y los objetivos de la Organización.
Comité de Seguridad	Órganos colegiados o unipersonales que toman decisiones que concretan cómo alcanzar los objetivos marcados por los órganos de gobierno.

Rol	Funciones
Responsable de la Información	A nivel de gobierno. Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la Organización.
Responsable de Servicio	A nivel de gobierno o, en ocasiones baja a nivel ejecutivo. Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la Organización.
Responsable de Seguridad	A nivel ejecutivo. Funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información.
Responsable del Sistema	A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día
Administrador de seguridad	Persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Además, la UR contará con los siguientes roles:

Rol	Funciones
Responsable Seguridad Física	A nivel operacional. Encargado de implantar las medidas de seguridad que le competan.
Responsable de Gestión de Personal	A nivel operacional. Encargado de implantar las medidas de seguridad que le competan.

Junto a los anteriores y en aras del cumplimiento de los requisitos derivados del cumplimiento del Reglamento General de Protección de Datos, también interviene el siguiente rol:

Rol	Funciones
Delegado de Protección de Datos	Responsable de informar, asesorar, supervisar, cooperar y actuar en materia de protección de datos, a todos los niveles de la organización.

7.2 Jerarquía en el proceso de decisiones y mecanismos de coordinación

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

El Responsable del Sistema:

1. Informa al Responsable de la Información y del Servicio tanto de las incidencias funcionales relativas a la información como al servicio que le compete.

2. Da cuenta al Responsable de la Seguridad de la Información:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
    - Resumen consolidado de los incidentes de seguridad.
    - Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad:

1. Informa al Responsable de la Información y del Servicio de las decisiones e incidentes en materia de seguridad que afecten tanto a la información como 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.

2. Informa al Responsable del Servicio. Da cuenta al Comité de Seguridad de la Información:
    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

3. Da cuenta al Consejo de Gobierno, según lo acordado en el Comité de Seguridad de la Información.
    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

7.3 Procedimientos de Designación de Personas

El Rector nombrará mediante resolución al:

- Responsable de la Información, que recae en el titular de la Secretaría General de la UR.
- Responsable del Servicio, que recae en el titular de la Gerencia.
- Responsable de la Seguridad de la Información.
- Responsable del Sistema, que debe reportar directamente al Comité de Seguridad de la Información y recae en el titular con competencias en gestión y tratamiento de la Información.
- Administrador/es de Seguridad del Sistema, a propuesta del Responsable del Sistema, de entre el personal de los Servicios Informáticos con funciones en el ámbito de la seguridad.
- Responsable de Seguridad Física, seleccionado entre el personal de la UR con competencias en materia de la seguridad física.
- Responsable de Gestión de Personal, seleccionado entre el personal de la UR con competencias en gestión del personal.
- Delegado de Protección de Datos, seleccionado entre el personal de la UR.

7.4 Consejo de Gobierno

El Consejo de Gobierno de la UR se ha comprometido con la implantación y el mantenimiento del Sistema de Gestión de la Seguridad de la Información y como evidencia de ello se encuentra el documento de Política de Seguridad de la Información, además de formar parte la Dirección del Comité de Seguridad de la Información.

La función de Dirección asociada al Consejo de Gobierno la desempeñará el SECRETARIO GENERAL quien entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde que se alcancen.

Función	Detalle
Nombrar	• Designar los diferentes roles encargados de la gestión de la seguridad.
Objetivos	• Fijar y aprobar anualmente unos objetivos de nivel de riesgo aceptable. Los objetivos deben ser vigentes y estar alineados con el propósito y la estrategia de la Organización, ser medibles o estimables y coherentes con las presentes Directrices. El Comité de Seguridad seguirá y reportará anualmente la evolución de dichos objetivos.
Aprobar	• Aprobar el Plan de Adecuación al ENS. • Aprobar la Política de Seguridad así como las revisiones de la misma. • Aprobar, tras cada proceso de Apreciación del Riesgo que se realice, del Plan de Tratamiento del Riesgo que se elabore, que puede incluir la aplicación de controles, la transferencia a terceros, evitar riesgos – lo que deriva generalmente en la realización de cambios en procesos -, o bien la asunción de determinados riesgos.
Recursos	• Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema Integrado de Gestión.

7.5 Comité de Seguridad de la Información

Se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

Presidente:	Responsable de la Información
Secretario:	Responsable de Seguridad de la Información
5 Vocales:	Responsable del Servicio
	Responsable del Sistema
	Director del Servicio de Asesoría Jurídica
	Administrador de la Seguridad del Sistema
	Delegado de Protección de Datos

A requerimiento del Comité se convocará cualesquiera otros Jefes de Servicio o Área y responsables, cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por la LOPD.

Funciones del Secretario. Corresponde al **Secretario/a del Comité de Seguridad** de la Información:

- 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
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Funciones de los Vocales. Corresponde a los **Vocales del Comité de Seguridad** de la Información:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Votaciones. Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

Funciones del Comité de Seguridad de la Información son las siguientes:

- Atender las inquietudes del Consejo de Dirección.
- Informar regularmente del estado de la seguridad de la información al Consejo de 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 la 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 Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de 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 diferentes planes que puedan realizarse en diferentes áreas.
- Velar por que 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.
- Recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
- Se asesorará de los temas que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:
- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría interna y/o externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.
- Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente, en caso de ocurrencia de incidentes de seguridad de la información.

Función	*Detalle*
Informar	• Atender las inquietudes del Consejo de Dirección • Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.
Promover	• Promover la mejora continua del Sistema de Gestión de la 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.
Coordinar	• 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.

Función	Detalle
	• 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.
Elaborar	• Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección. • Elaborar la estrategia de evolución de la Organización en lo que respecta a la seguridad de la información.
Aprobar	• Aprobar la normativa de seguridad de la información. • Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información • Aprobar planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
Controlar	• Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. • Velar por que 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.

7.6 Responsable de la Información

Le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

7.7 Responsable del Servicio

Le corresponden las siguientes funciones:

- Gestión de la seguridad.
    - Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
    - Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.

- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

7.8 Responsable de Seguridad de la Información

Le corresponden las siguientes funciones:

- Política, Normativa y Procedimientos.
  - Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por Dirección.
  - Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
  - Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Comité de Seguridad.
  - Reportará directamente al Comité de Seguridad de la Información.
  - Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
  - Actúa como Secretario del Comité de Seguridad.
  - Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Gestión de la Seguridad.
  - Mantendrá 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 Organización.
  - Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
  - Realizará el Análisis de Riesgos.
  - Facilitará al Responsable de Información y al Responsable del Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
  - Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
  - Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
  - Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.

- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Colaborará con el DPD para que las políticas de seguridad implantadas en la UR estén alineadas con los requerimientos que el RGPD dispone en cuanto a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

- Formación y concienciación.
  - Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
  - Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.

El Responsable de la Seguridad de la Información podrá ser asesorado en el ejercicio de sus funciones por un técnico especialista del Servicio de Tecnologías de la Información.

7.9 Responsable del Sistema

Le corresponden las siguientes funciones:

- Gestión de la seguridad.
  - Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
  - 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 con el Responsable de la Seguridad antes de ser ejecutada.
- Monitorizar.
  - Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Planes de continuidad.
  - Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
  - Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.
- Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.

En caso de ocurrencia de incidentes de seguridad de la información:

- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves.

7.10 Administrador de la Seguridad del Sistema

Le corresponden las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- 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.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida. Informar a los Responsables de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

En caso de ocurrencia de incidentes de seguridad de la información:

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo. Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

7.11 Responsable de Seguridad Física

Le corresponderá implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

7.12 Responsable de Gestión de Personal

Le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

7.13 Delegado de Protección de Datos

Asumirá las atribuciones previstas en el artículo 39 del Reglamento General de Protección de Datos anteriormente indicado y, en particular, asumirá la función de informar y asesorar a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en relación a la protección de datos.

El Delegado de Protección de Datos asume, además, las siguientes funciones:

- 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 y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- supervisar el cumplimiento de lo dispuesto en el 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, y realizar consultas, en su caso, sobre cualquier otro asunto.

8. Datos de carácter personal

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades de Tratamiento de la UR recoge los tratamientos afectados y los responsables correspondientes. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades de Tratamiento.

9. Gestión de riesgos

9.1 Justificación

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

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

9.2 Criterios de Evaluación de Riesgos

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

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

9.3 Directrices de Tratamiento

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las

necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9.4 Proceso de Aceptación del Riesgo Residual

Los riesgos residuales serán **determinados** por el Responsable de Seguridad de la Información.

Los niveles de **Riesgo residuales** esperados sobre cada **Información** tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de esa Información.

Los niveles de **Riesgo residuales** esperados sobre cada **Servicio** tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de ese Servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

9.5 Necesidad de realizar o actualizar las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

4. Regularmente, al menos una vez al año.
5. Cuando se produzcan cambios significativos en la información manejada.
6. Cuando se produzcan cambios significativos en los servicios prestados.
7. Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
8. Cuando ocurra un incidente grave de seguridad.
9. Cuando se reporten vulnerabilidades graves.

10. Gestión de incidentes de seguridad

10.1 Prevención de incidentes

Las unidades 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. El ENS a través de su artículo 19 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 17 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello las unidades 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, las unidades deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- 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.

10.2 Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

10. Sistemas de detección de intrusos a nivel de red.
11. Sistemas de detección de intrusos a nivel sistema.

10.3 Respuesta ante incidentes

Se desarrollarán procedimientos específicos que determinen los criterios generales a la hora de gestionar los incidentes de seguridad. Estos procedimientos darán respuesta, como mínimo, a los siguientes requerimientos:

12. Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
13. Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
14. Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

10.4 Recuperación ante incidentes y planes de continuidad

Para garantizar la disponibilidad de los servicios críticos, las unidades, coordinadas con los servicios TIC, colaborarán en el desarrollo de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

11. Obligaciones del personal

Los miembros de la organización 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a los miembros de la organización, 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 cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

12. Terceras partes

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen 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.

13. estructura normativa y desarrollo de la política de seguridad

La estructura jerárquica de la documentación de seguridad es la siguiente:

Documento	Detalle
Política	• Define las metas y expectativas de seguridad. • Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. • Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio. • Debe ser escrita por personas expertas en la materia o por el Responsable de Seguridad y aprobada por el Comité de Seguridad.
Procedimiento	• Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. • Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad. • Debe ser elaborado por el Responsable del Sistema y aprobado por el Responsable de Seguridad.
Instrucciones técnicas	• Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución. • Pueden ser elaborados por el Responsable del Sistema o Administrador del Sistema y deben ser aprobados por el Responsable de Seguridad.
Guías	• Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. • Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas. • Deben ser aprobadas por el Responsable de Seguridad.

14. Revisión y aprobación de la política de seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

15. Documentación complementaria

La Política de Seguridad de la Información se cumplimentará con documentos más precisos que ayudan a llevar a cabo lo propuesto. Para ello se utilizarán:

- Normas de seguridad.
- Guías de seguridad.
- Procedimientos de seguridad.

Las **normas** uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las **guías** tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los **procedimientos** [operativos] de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Anexo. Glosario de términos

Análisis de riesgos
Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal
Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Gestión de incidentes
Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos
Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad
Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Política de seguridad
Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad
Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información
Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad
El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio
Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema
Persona que se encarga de la explotación del sistema de información.

Servicio
Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información
Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición.