FRANCISCO JAVIER CALVO GALLEGO, SECRETARIO GENERAL DE LA UNIVERSIDAD INTERNACIONAL DE ANDALUCÍA

INFORMA

Acuerdo 37/2023, del Consejo de Gobierno de la Universidad Internacional de Andalucía, de 26 de mayo de 2023, por el que se aprueba la Política de Seguridad y Privacidad de la Información.

El Consejo de Gobierno de la Universidad Internacional de Andalucía, reunido el 26 de mayo de 2023, **aprueba la Política de Seguridad y Privacidad de la Información de la Universidad Internacional de Andalucía, y ordena su publicación en el BOUNIA,** conforme se recoge en el siguiente Anexo.

ANEXO: POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIA

0. Aprobación y Entrada en Vigor

Conforme a lo establecido en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS en adelante), esta Política de Seguridad y Privacidad de la Información de la Universidad Internacional de Andalucía (UNIA en adelante), entendida como el conjunto de directrices que rigen la forma en la que esta organización gestiona y protege la información que trata y los servicios que presta, ha sido aprobada por el Consejo de Gobierno de la UNIA como máximo órgano de gobierno y administración de esta Universidad, al amparo de lo establecido en el artículo 10 del Texto Refundido de su Ley de creación, aprobado mediante Decreto Legislativo 2/2013, de 8 de enero, y el artículo 20 de sus Estatutos aprobados por el artículo único del Decreto 236/2011, de 12 de julio.

Esta Política será objeto de publicación en el Boletín Oficial de la UNIA (en adelante BOUNIA) y entrará en vigor al día siguiente de la misma.

1. Introducción

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece en su artículo 12, apartado 2: *'Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente'*.

La UNIA es una universidad pública del Sistema Universitario Andaluz, con vocación internacional y de cooperación solidaria interuniversitaria, especialmente con América Latina y el Magreb, que responde con calidad, agilidad, innovación y flexibilidad a los retos emergentes de la sociedad y a las necesidades de la comunidad universitaria y del entorno socioeconómico y productivo.

La UNIA hace uso de los Sistemas de las Tecnologías de la Información y la Comunicación (en adelante TIC) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados, contra las amenazas o los incidentes que puedan afectar a los principios básicos de la seguridad de la información: confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

En este sentido, su Código ético, aprobado por Acuerdo 45/2022, del Consejo de Gobierno de la Universidad Internacional de Andalucía, de 15 de junio de 2022 (BOUNIA núm. 9, de 23 de junio de 2022) establece expresamente que no se utilizará la información y los datos que afecten a la intimidad, los derechos económicos de las personas o a cualquier otra información confidencial de la universidad con fines privados, ni se harán públicos indebidamente; en segundo lugar, que los documentos de trabajo y la información a la que deba accederse en la gestión universitaria se utilizará para fines exclusivamente institucionales, manteniendo la debida reserva y confidencialidad; y, en tercer lugar, que estos deberes han de mantenerse durante y después de haber prestado el servicio, incluso después de finalizar la vinculación con la universidad.

Para hacer frente a las amenazas antes señaladas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno y que garantice la prestación continua de los servicios. Esto implica aplicar las medidas mínimas de seguridad definidas por el Esquema Nacional de Seguridad (ENS), así como: realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes en el ámbito de las tecnologías de la información y de las comunicaciones que garantice la continuidad de los servicios prestados.

Todas las unidades administrativas de la universidad deben tener presente que la Seguridad de la Información 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 TIC.

2. Principios Básicos de Seguridad

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información.

Además de los contemplados en el capítulo II del ENS, se establecen expresamente los siguientes:

- **Alcance Estratégico**: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

- **Responsabilidad Determinada**: En los Sistemas TIC, se nombrarán al Responsable de la Información, quien determina los requisitos de seguridad de la información tratada; al Responsable del Servicio, quien determina los requisitos de seguridad de los servicios prestados; al Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, quien determina las decisiones para satisfacer los requisitos de seguridad. A estos efectos se asumen las definiciones establecidas en el artículo 13.2 del ENS.

- **Seguridad Integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los Sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los Sistemas TIC. Se prestará la máxima atención a la concienciación de las personas y, en especial, de los responsables que intervengan en los procesos. Además, y conforme a lo establecido en los artículos 8 y 9 del ENS, la seguridad de nuestro sistema contemplará, no solo múltiples capas de seguridad organizativas, físicas y lógicas, sino también acciones relativas a la prevención, detección y respuesta, al objeto de minimizar nuestras vulnerabilidades y lograr que las amenazas no se materialicen o que, en caso de hacerlo, no afecten gravemente a la información o servicios que se manejan o prestan.

- **Gestión de Riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza

de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia, eficiencia y posibilidades económicas de la UNIA respecto de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales teniendo siempre presente lo establecido en el artículo 3 del ENS.

- **Proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- **Mejora continua**: Las medidas de seguridad se revaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

- **Seguridad por Defecto**: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

3. Objetivos de la Seguridad de la Información

La UNIA establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la integridad, confidencialidad y disponibilidad de la información.

- Lograr la plena concienciación y formación de los usuarios respecto a la seguridad de la información.

- Gestión de activos de información: los activos de información de la UNIA se encontrarán inventariados y categorizados y estarán asociados a un responsable.

- Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca y sea formado en sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido, pretendiendo la plena concienciación de los usuarios respecto a la seguridad de la información.

- Seguridad física: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

- Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará

registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

- Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

- Garantizar la prestación continuada de los servicios: 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 de nivel de servicio de sus usuarios.

- Protección de datos: se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad, así como la normativa nacional y europea de protección de datos.

- Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

4. Alcance

Esta Política de Seguridad se aplicará a los Sistemas de Información de la UNIA, relacionados con el ejercicio de sus competencias, y a todos los usuarios con acceso a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad.

El respeto y cumplimiento estricto de esta normativa se exigirá igualmente a aquellas personas o entidades con las que pudiera relacionarse jurídicamente la UNIA y que, en cumplimiento del correspondiente programa obligacional de obligaciones, pudiera tener acceso a esta información y/o sistemas. La referencia a esta Política deberá incorporarse, en su caso, a los contratos, convenios u otras formas de instrumentación jurídica de la que pudiera derivarse este acceso.

Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad y su Normativa General de Utilización de los Recursos y Sistemas de Información derivada, siendo responsabilidad del Comité de la Seguridad y Privacidad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. Medidas

Para la UNIA, el objetivo de la Seguridad de la Información es garantizar la integridad, confidencialidad y disponibilidad de la información y la prestación continuada de los servicios, actuando de forma preventiva, supervisando la actividad diaria y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 7 del ENS.

Para ello, la UNIA plantea la aplicación de las medidas que se relacionan a continuación.

5.1. Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la UNIA implementará las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los perfiles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la UNIA 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 parte de terceros con el fin de obtener una evaluación independiente.

5.2. Detección

La UNIA establecerá controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto artículo 10 del Real Decreto 311/2022 (Vigilancia continua y reevaluación periódica). Cuando se detecte una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado artículo 9 del Real Decreto 311/2022 - Existencia de líneas de defensa), se establecerán los mecanismos de análisis y reporte necesarios para que lleguen, de manera regular, a los Responsables de la Seguridad y del Sistema.

5.3. Respuesta

La UNIA, establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

5.4. Recuperación

Para garantizar la disponibilidad de los servicios, la UNIA se compromete a proporcionar los medios y técnicas necesarias que permitan la recuperación de los servicios más críticos.

6. Marco Normativo

El marco normativo en que se desarrollan las actividades de la UNIA y, en particular, la prestación de sus servicios electrónicos está integrado por las siguientes normas:

- De ámbito Europeo:

- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas del mercado interior (Idas) y normas de ejecución.
- 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.
- Directiva (UE) 2016/1148 del Parlamento Europeo y el Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
- Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

- De ámbito Estatal:
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDyGDD).
  - Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
  - Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
  - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
  - Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
  - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
  - Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
  - Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
  - 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.
  - Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno.
  - Ley 39/2105, de 1 de octubre, de Procedimiento Administrativo Común.
  - 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 el que se aprueba la Instrucción Técnica de Seguridad de Informe de Estado de Seguridad.
- Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 3/2022, de 24 de febrero, de convivencia universitaria

- De ámbito Autonómico:
  - Decreto Legislativo 1/2013, de 8 de enero, por el que se aprueba el Texto Refundido de la Ley Andaluza de Universidades.
  - Decreto Legislativo 2/2013, de 8 de enero, por el que se aprueba el Texto Refundido de la ley de creación de la Universidad Internacional de Andalucía.
  - Decreto 236/2011, de 12 de julio, por el que se aprueban los Estatutos de la UNIA.
  - Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

- De ámbito Interno:
  - Acuerdo 23/2022 del Consejo de Gobierno de la UNIA, de 6 de abril de 2022 (BOUNIA núm. 5/2022 de 20 de abril), por el que se aprueba el Reglamento de Administración Electrónica de la UNIA.
  - Otras normas que en la actualidad o en el futuro, de carácter general o interno, resulten de aplicación a la Universidad en el marco de esta Política de Seguridad de la Información.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la UNIA, derivadas de las anteriores y publicadas en la sede electrónica comprendidas dentro del ámbito de aplicación de la presente Política de Seguridad.

7. Organización de la Seguridad de la Información

7.1. Criterios utilizados para la Organización de la Seguridad de la Información

La UNIA, con el objeto de organizar la seguridad de la información y teniendo en cuenta lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS" y la Guía de Adecuación al ENS para Universidades, emprenderá las siguientes acciones:

a) Designará los perfiles de seguridad: Responsable de la Información, Responsable del Servicio, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.

b) Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad y Privacidad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2. Perfiles y Órganos de la Seguridad de la Información

7.2.1. Comité de Seguridad y Privacidad de la Información

El **Comité de Seguridad y Privacidad de la Información** (en adelante Comité de Seguridad) estará constituido por:

- Presidente: Rector/a o persona en quien delegue.
- Secretario: Responsable de la Seguridad de la Información o persona en quien delegue.
- Responsable del Servicio: Gerente de la UNIA.
- Responsable de la Información: titular de la Secretaría General de la UNIA.
- Responsable de la Seguridad de la Información: Vicerrector/a o asimilado con competencias en Transformación Digital de la UNIA.
- Responsable del Sistema: Director/a del Área de Gestión de las TIC.
- Administrador de la Seguridad: personal de la UNIA con competencias en la materia, designado a propuesta del responsable de la seguridad de la información y que ejerza como Gestor de la Seguridad de la Información.
- Delegado de Protección de Datos: Delegado/a de Protección de Datos de la UNIA.

Los Responsables de la Información y del Servicio serán convocados por la Presidencia, en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de la universidad.

A instancias de la Presidencia, el Secretario del Comité de Seguridad realizará las convocatorias y levantará acta de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir, en calidad de asesores, las personas que en cada caso estime pertinente su Presidente.

7.2.2. Comisión Permanente del Comité de Seguridad

En el marco del ENS, los miembros del Comité de Seguridad que constituirán la **Comisión Permanente del Comité de Seguridad** (en adelante Comisión Permanente), serán los siguientes:

- Presidente: Responsable de la Seguridad de la Información.
- Secretario: Administrador de la Seguridad.
- Responsable del Sistema.
- Delegado de Protección de Datos.

El Delegado de Protección de Datos participará en las reuniones de la Comisión Permanente cuando en la misma vayan a abordarse cuestiones relacionadas con la Privacidad de la Información, así como siempre que se requiera su participación.

La Comisión Permanente abordará los asuntos que requieran de una actuación directa e inmediata y que no puedan tratarse, en primera instancia, por el Comité de Seguridad, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones.

La Comisión Permanente podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en la Comisión Permanente serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad.

Las reuniones de trabajo de sus miembros serán convocadas por la Presidencia, quien recabará los acuerdos alcanzados y dará cuenta al Comité de Seguridad, para en caso de ser necesario, proceder a su aprobación.

7.3. Responsabilidades de los Perfiles Asociados al ENS

7.3.1. Responsables de la Información y del Servicio

Serán funciones de los Responsables de la Información y del Servicio:

- Establecer y elevar para su aprobación al Comité de Seguridad los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de la Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la Información y los Servicios.
- Valorar los niveles de riesgo residual que afectan a la Información y los Servicios para su aceptación en el seno de la comisión
- Poner en comunicación del Responsable de la Seguridad cualquier variación respecto a la Información y los Servicios de los que son responsables, especialmente la incorporación de nuevos Servicios o Información a su cargo, y darán traslado de dichos cambios al Comité de Seguridad en su siguiente reunión.

7.3.2. Responsable de la Seguridad de la Información

Serán competencias del Responsable de la Seguridad de la Información:

- Mantener y verificar el nivel adecuado de seguridad de la información manejada (sin menoscabo de las competencias del Delegado de Protección de Datos[1]) y de los servicios electrónicos prestados por los Sistemas de Información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información (sin menoscabo de las competencias del Delegado de Protección de Datos[1]) dentro de su ámbito de responsabilidad.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias y elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o del Comité de Seguridad.

1 ***RGPD Artículo 39: Funciones del Delegado de Protección de Datos***

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y que no sean competencia del Comité de Seguridad) y poner en conocimiento del Comité de Seguridad las modificaciones que se hayan realizado a lo largo del periodo en curso.

7.3.3. Responsable del Sistema

Serán competencias del Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable de la Seguridad y/o Comité de Seguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables del sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

7.3.4. Administrador de la Seguridad de la Información

Dependerá del Responsable de la Seguridad y lo asesorará en materia de Seguridad y Privacidad de la Información, siendo sus funciones más significativas las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

- La aplicación (o asegurar su aplicación) de los Procedimientos Operativos de Seguridad (POS) aprobados para manejar el Sistema de Información.
- Asegurar que los Controles de Seguridad establecidos son adecuadamente observados.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la Seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de Seguridad del Sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el Sistema.
- Informar al Responsable de la Seguridad y al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la Seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.4. Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos (sin menoscabo de las funciones reconocidas en el RGPD[2]):

- Informar y asesorar a la UNIA, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en la SGSI.07 Normativa General de Utilización de los Recursos y Sistemas de Información y de las Políticas Internas de la UNIA, en materia de protección de datos, 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 supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
  - Recabar información para determinar las actividades de tratamiento.
  - Analizar y comprobar la conformidad de las actividades de tratamiento.
  - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
  - Recabar información para supervisar el registro de las operaciones de tratamiento.
  - Asesorar en el principio de la protección de datos por diseño y por defecto.
  - Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
  - Priorizar actividades en base a los riesgos.

2 ***RGPD Artículo 39: Funciones del Delegado de Protección de Datos***

- Asesorar al Responsable de Tratamiento sobre las áreas a someter a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

7.5. Comité de la Seguridad y Privacidad de la Información

Serán funciones del Comité de la Seguridad y Privacidad de la Información:

a) Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.

b) Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.

c) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

d) Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.

e) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

f) Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.

g) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

h) Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.

i) Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.

j) Aprobar la Normativa General de Utilización de los Recursos y Sistemas de Información para todo el personal.

k) Aprobar el Mapa de Normativa, con la lista de Normativas y Procedimientos de Seguridad para la implantación y cumplimiento del ENS.

Periodicidad de las Reuniones y Adopción de Acuerdos:

1. Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el proceso y posibilitar su adecuado seguimiento, el Comité de Seguridad deberá reunirse con carácter semestral.
2. Una vez alcanzada la conformidad con el ENS de los servicios prestados por la universidad, el Comité de Seguridad se reunirá al menos una vez al año, siendo lo recomendable hacerlo con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
3. En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.

4. Las decisiones se adoptarán por consenso de sus miembros.

7.6. Comisión Permanente del Comité de Seguridad

Serán funciones de la Comisión Permanente del Comité de la Seguridad de la Información:

a) Las funciones propias de cada miembro como pertenecientes al Comité de Seguridad.

b) Elevar al Comité de Seguridad directrices y recomendaciones.

c) Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.

d) Elevar al Comité de Seguridad las propuestas de modificaciones a la Normativa General de Utilización de los Recursos y Sistemas de Información para todo el personal.

e) Elevar al Comité de Seguridad propuestas de Mapa de Normativa, con la lista de Normativas y Procedimientos de Seguridad para la implantación y cumplimiento del ENS.

f) Atender cuestiones urgentes relativas a la Seguridad de la Información.

Periodicidad de las Reuniones y Adopción de Acuerdos:

1. Se reunirá ante situaciones sobrevenidas que requieran de unas actuaciones ágiles y/o toma de decisiones menores.
2. Las reuniones se convocarán a iniciativa de su Presidencia, a través del Secretario.
3. Las decisiones se adoptarán por consenso de sus miembros.

7.7. Procedimiento de Designación

La creación del Comité de Seguridad y de su Comisión Permanente, el nombramiento de sus integrantes y la designación de los responsables identificados en esta Política de Seguridad, se realizará por el Rector de la UNIA.

El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

8. Datos Personales

La UNIA sólo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y estos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. En todo caso cumplirá rigurosamente los principios de tratamiento y el resto de normas establecidas legal o reglamentariamente. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

9. Obligaciones del Personal

Todo el personal de la UNIA, comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

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

10. Gestión de Riesgos

Todos los sistemas afectados por la presente Política de Seguridad están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

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.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos del ENS, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

11. Notificación de Incidentes

De conformidad con lo dispuesto en los artículos 25 y 33 ENS, la UNIA notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

12. Desarrollo de la Política de la Seguridad y Privacidad de la Información

La presente Política de Seguridad será complementada por medio de diversa normativa y recomendaciones de seguridad (Normativa General de Utilización de los Recursos y Sistemas de Información, Procedimientos Técnicos de Seguridad, Informes, Registros y Evidencias Electrónicas). Corresponde al Comité de Seguridad su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre Seguridad y Privacidad de la Información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) **Primer Nivel Normativo**: constituido por la presente "ENS.01 Política de Seguridad y Privacidad de la Información", la "SGSI.07 Normativa General de Utilización de los Recursos y Sistemas de Información", y las directrices generales de seguridad aplicables a los organismos o unidades de la universidad a los que sean de aplicación dichos documentos.

b) **Segundo Nivel Normativo**: constituido por las normas de seguridad derivadas de las anteriores.

c) **Tercer Nivel Normativo**: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad y Privacidad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Consejo de Gobierno de la UNIA la aprobación de la Política de Seguridad y Privacidad de la Información y la Normativa General de Utilización de los Recursos y Sistemas de Información, siendo el Comité de Seguridad el órgano responsable de la aprobación de los restantes documentos, y de su difusión para el conocimiento de las partes afectadas.

Del mismo modo, la presente Política de Seguridad y Privacidad de la Información complementa la Normativa existente, en la UNIA, en materia de Protección de Datos.

La Normativa de Seguridad de la Información y, muy especialmente, la Política de Seguridad y Privacidad de la Información y la Normativa General de Utilización de los Recursos y Sistemas de Información, será conocida y estará a disposición de todos los miembros de la Comunidad Universitaria; en particular para aquellos que utilicen, operen o administren los Sistemas de Información y Comunicaciones. Estará disponible para su consulta en la Web de la Universidad, en el Portal del BOUNIA, y será custodiada por la Secretaría General de la UNIA.

13. Terceras partes

Cuando la UNIA preste servicios o maneje información de otros organismos, se les hará participe de esta Política de Seguridad. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la UNIA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esta normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se requerirá que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

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

14. 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 implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad.

b) Revisión de los servicios e información y su categorización

c) Realización de auditorías internas o, cuando procedan, externas.

d) Revisión de las medidas de seguridad.

e) Revisión y actualización de las normas y procedimientos.

Disposición derogatoria única

A la entrada en vigor de esta Política de Seguridad y Privacidad de la Información, quedará derogada expresamente la Política de Seguridad en la Información de la Universidad Internacional de Andalucía, aprobada por Acuerdo de Consejo de Gobierno 51/2018, de 12 de junio de 2018; así como cuantas otras normas, acuerdos o instrucciones de cualquier órgano de esta Universidad que se opongan a lo dispuesto en la misma.