



UNIVERSIDAD
DE ALMERÍA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE ALMERÍA

Aprobada en Consejo de Gobierno de 05/11/2025

Comisión de Seguridad Informática y Protección de Datos

CONTENIDO

| | |
|--|-----------|
| 1. INTRODUCCIÓN | 3 |
| 1.1. PREVENCIÓN | 4 |
| 1.2. DETECCIÓN..... | 4 |
| 1.3. RESPUESTA..... | 5 |
| 1.4. RECUPERACIÓN..... | 5 |
| 2. MISIÓN DE LA UNIVERSIDAD DE ALMERÍA..... | 5 |
| 3. PRINCIPIOS BÁSICOS | 6 |
| 4. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN..... | 7 |
| 5. ALCANCE..... | 9 |
| 6. MARCO NORMATIVO | 11 |
| 7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN..... | 12 |
| 7.1. RESPONSABLE DE LA INFORMACIÓN | 13 |
| 7.2. RESPONSABLE DE LOS SERVICIOS TIC..... | 13 |
| 7.3. RESPONSABLE DE SEGURIDAD..... | 13 |
| 7.4. RESPONSABLES DEL SISTEMA IT | 14 |
| 7.5. ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA..... | 15 |
| 7.6. COMITÉ DE GESTIÓN DEL ENS..... | 16 |
| 7.7. DELEGADO DE PROTECCIÓN DE DATOS..... | 16 |
| 8. DATOS PERSONALES..... | 17 |
| 9. OBLIGACIONES DEL PERSONAL | 17 |
| 10. GESTIÓN DE RIESGOS..... | 18 |
| 11. NOTIFICACIÓN DE INCIDENTES..... | 18 |
| 12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN..... | 19 |
| 13. TERCERAS PARTES | 19 |
| 14. MEJORA CONTINUA, MODIFICACIONES Y DEROGACIÓN..... | 20 |
| 15. APROBACIÓN Y ENTRADA EN VIGOR..... | 20 |

1. INTRODUCCIÓN

Esta Política de Seguridad de la Información se elabora en cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), que sustituye al Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, que en su artículo 12 establece la obligación para las administraciones públicas de disponer de una política de seguridad e indica los requisitos mínimos que debe cumplir.

Esta Política de Seguridad sigue también las indicaciones de la Guía CCN-STIC-801 y la Guía de adecuación al ENS para Universidades (CCN-STIC 881) del Centro Criptológico Nacional, en el que se establece un marco común de seguridad de la información en las universidades públicas.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La Universidad de Almería, hace uso de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos institucionales. En consecuencia, 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.

Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que la organización y su personal debe aplicar las medidas mínimas de seguridad exigidas por el citado RD 311/2022, 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.

La organización debe 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.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

1.1. PREVENCIÓN

La organización 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 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, la organización 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.

1.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada 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 produzca una desviación significativa de los parámetros que se hayan prestablecido como normales.

1.3. RESPUESTA

La Universidad de Almería debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Establecer mecanismos para la restauración de la información y los servicios que pudieran haberse visto afectados.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la UAL.
- 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) reconocidos a nivel nacional: Iris-CERT, CCN-CERT...

1.4. RECUPERACIÓN

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

2. MISIÓN DE LA UNIVERSIDAD DE ALMERÍA

Según se refleja en los Estatutos, la Universidad de Almería es una institución de derecho público, dotada de personalidad jurídica y patrimonio propio, a la que corresponde el servicio público de la educación superior mediante la docencia, el estudio y la investigación, con plena autonomía y de acuerdo con la Constitución Española y las leyes.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifestar la necesidad de disponer de una infraestructura TIC que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

A su vez, cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. PRINCIPIOS BÁSICOS

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. Se establecen los siguientes:

- **Alcance estratégico.** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la Universidad en todas las áreas (gestión administrativa y tecnológica, investigación y docencia), 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 identificará:
 - Responsable de la Información, que determina los requisitos de seguridad de la información tratada;
 - Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados;
 - Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios;
 - Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **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.

- **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 y el coste 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.
- **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 reevaluarán 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.

4. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

La Universidad de Almería establece como objetivos de la seguridad de la información los siguientes:

- **Garantizar la calidad y protección de la información.**
- **Lograr la plena concienciación de todos los usuarios respecto a la seguridad de la información:** Estos están integrados por el personal docente e investigador, personal técnico, de gestión y de administración y servicios, estudiantado y cualesquiera otros relacionados con los sistemas de información de la universidad.
- **Gestión de activos de información:** Los activos de información de la universidad 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 reciba la correspondiente información sobre sus responsabilidades y una formación adecuada de modo que se reduzca el riesgo derivado de su uso indebido, logrando 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, así como para su notificación a terceros en el marco de procedimientos de colaboración o en cumplimiento de obligaciones legales.
- **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 acuerdo con las necesidades de nivel de servicio de sus usuarios.

- **Protección de datos:** En el tratamiento de datos personales, pseudonimizados o anonimizados y en aquellos tratamientos de datos personales orientados a diseñar procesos que repercutan en las personas, se adoptarán las medidas técnicas y organizativas necesarias para diseñar los tratamientos y gestionar los riesgos garantizando el cumplimiento del RGPD y de cualquier otra normativa de desarrollo y el pleno ejercicio de los derechos.
- **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.

5. ALCANCE

Esta Política de seguridad de la información se aplicará a los sistemas de información de la Universidad de Almería relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad. Todos ellos tienen la obligación de conocer y cumplir esta Política y la normativa de seguridad derivada.

Debido pues, a la misión de la entidad reflejada en el apartado 2º de este documento, la Organización desplegará y desarrollará la aplicación de la presente política de seguridad sobre todo el conjunto del sistema de información.

En base a ello, la organización aplicará la presente política sobre el grueso de los sistemas TIC que gestiona de manera centralizada a través del Área de Tecnologías de la Información y las Comunicaciones, y específicamente sobre todos aquellos sistemas que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

De forma concreta la presente política de seguridad es aplicable sobre los siguientes servicios y los sistemas TIC que los conforman:

- **Sistema ERP¹ Institucional:**
 - Gestión Académica

¹ ERP = Sistema de Planificación de Recursos Empresariales (del inglés, *Enterprise Resource Planning*)

- Gestión Económica
- Gestión de RR.HH.
- Gestión de la Investigación
- Campus Virtual
- Información DATAWAREHOUSE
- **Sistema de Administración Electrónica:**
 - Servicio de Administración Electrónica
- **Sistema de Servicios Universitarios Académicos**
 - Docencia Virtual
 - Aulas Virtuales
 - Atención al Usuario
 - Servicio de calidad
 - Gestión de espacios
 - Servicio repositorio de información
 - Servicio de prácticas y búsqueda de empleo
 - Servicio de gestión de Biblioteca
 - Servicio Editorial
 - GESCURSA Gestión de Cursos
- **Sistema de Servicios Universitarios Adicionales**
 - Servicio de marketing
 - Gestión de residuos
 - Gestión de envío postal
 - Servicio a antiguos alumnos
 - Servicio de Deportes
 - Servicio de alojamiento UAL

Adicionalmente, y aun entendiéndose que los siguientes servicios no se encuentran directamente en el alcance marcado por el Esquema Nacional de Seguridad, debido a su importancia en la comunidad universitaria, se acuerda extender el alcance al siguiente servicio de la UAL:

- **Sistema Web Institucional**
 - Servicio Web institucional
 - Servicio Web de información

6. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas en relación con la protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, la UAL podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
- Ley 17/2022, de 5 de septiembre, por la que se modifica la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Estatutos de la Universidad de Almería, aprobados por Decreto 225/2018, de 18 de diciembre, de la Junta de Andalucía.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.
- 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 14/2007, de 3 de julio, de Investigación biomédica.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

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

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se organiza la seguridad de la información a través del Responsable de la información, Responsable de los Servicios TIC, Responsable de Seguridad, Responsable del Sistema IT, del Administrador de la Seguridad del Sistema, Comité de Gestión del ENS y Delegado de protección de datos (Comisión de Seguridad Informática y Protección de Datos).

7.1. RESPONSABLE DE LA INFORMACIÓN

El **Secretario General** tendrá el rol de responsable de la información de la Organización, con las siguientes funciones:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y el de sistema en el mantenimiento de los sistemas catalogados según el Anexo I del ENS.

7.2. RESPONSABLE DE LOS SERVICIOS TIC

El **miembro del Equipo de Gobierno con competencias en TIC** tendrá el rol de responsable de los servicios TIC de la Organización, con las siguientes funciones:

- Establecimiento de los requisitos de los servicios TIC en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y el de sistema en el mantenimiento de los sistemas catalogados según el Anexo I del ENS.

7.3. RESPONSABLE DE SEGURIDAD

El **Director del Área de Tecnologías de la Información y las Comunicaciones** tendrá el rol de responsable de seguridad de la Organización, con las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Promover la formación y concienciación del Área de Tecnologías de la Información y las Comunicaciones dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del Sistema.
- Elaboración de la normativa de seguridad de la entidad.

7.4. RESPONSABLES DEL SISTEMA IT

Se designa a los **Jefes de Servicio del Área de Tecnologías de la Información y las Comunicaciones** en el rol de Responsables del Sistema de la Organización. Dentro de sus áreas de actuación tendrán las siguientes funciones:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.

- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

7.5. ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA

El **Administrador de Servicios de Red y Seguridad TIC** tendrá el rol de Administrador de la Seguridad del Sistema. Teniendo por funciones las siguientes:

- Verificar la aprobación de los procedimientos operativos de seguridad.
- Asegurar el cumplimiento de los controles de seguridad.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

- Supervisar la monitorización del estado de la seguridad del sistema.
- Informar a los Responsables de Seguridad y 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.

7.6.COMITÉ DE GESTIÓN DEL ENS

Las funciones del **Comité de Gestión del ENS** las asume la actual **Comisión de Seguridad Informática y Protección de Datos**, en adelante Comisión de Seguridad.

La Comisión de Seguridad tendrá informado al Equipo de Gobierno. Las funciones de la Comisión de Seguridad en relación con el ENS son:

- Divulgación de la política y normativa de seguridad de la Organización.
- Aprobación de la normativa de seguridad de la Organización.
- Revisión anual de la política de seguridad.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
 - o Tareas de adecuación
 - o Análisis de Riesgos
 - o Auditoría Bienal

7.7.DELEGADO DE PROTECCIÓN DE DATOS

Será una persona con conocimiento especializado en Derecho y en la práctica en materia de protección de datos. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

El Delegado de Protección de Datos debe desempeñar sus tareas y funciones con total independencia.

Las funciones del Delegado se encuentran especificadas en el artículo 39 del *RGPD*, siendo las

siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RGPD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- 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 del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

8. DATOS PERSONALES

La UAL realiza tratamientos en los que hace uso de datos de carácter personal, adoptando, en cada caso, las medidas de seguridad adecuadas, siguiendo las directrices del Reglamento Europeo de Protección de Datos, las indicaciones del Delegado de Protección de Datos, y manteniendo la suficiente diligencia para cumplir con el principio de responsabilidad que establece la actual normativa de seguridad.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de la UAL tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad de la Comisión de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los trabajadores de la UAL atenderán a una acción de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de acciones en

concienciación continua para atender a todos los miembros de la UAL, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de la UAL.

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.

10. 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 cada dos años
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves
- Cuando así lo indique el Delegado de Protección de Datos

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

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

11. NOTIFICACIÓN DE INCIDENTES

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la Universidad de Almería, notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios

prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet, a través del portal de administración electrónica (<http://ae.ual.es>), y de la página web de la Comisión de Seguridad (<http://seguridad.ual.es>)

Así mismo podrá encontrarse impresa en el Área de Tecnologías de la Información y las Comunicaciones.

13. TERCERAS PARTES

De acuerdo con el ENS, los sistemas de información de las entidades del sector privado incluirán la obligación de contar con una política de seguridad (artículo 12 ENS), cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 (ENS) deberá ser aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Así pues, los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación del ENS, contemplarán todos aquellos requisitos necesarios para asegurar la conformidad de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

Por lo tanto, cuando la UAL preste servicios a otros organismos o maneje información de otros o utilice servicios de terceros o ceda información a terceros, no solo se les hará partícipes de esta Política de Seguridad de la Información, sino que establecerá canales para informar y coordinar los respectivos Comités de Coordinación del ENS, estableciendo procedimientos de actuación para la reacción ante incidentes de seguridad, al menos al mismo nivel que el establecido en esta Política y en el ENS como marco de referencia.

Sólo en el caso de que algún aspecto de la Política de Seguridad no pueda ser satisfecho por una tercera parte, tal y como se indica en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad del tercero, para que precise los riesgos en que se podría incurrir y la forma de tratarlos.

Dicho informe deberá ser aprobado o no, por los responsables de la información y los servicios afectados, mediante informe motivado, antes de seguir adelante, pudiendo solicitar asesoramiento del Delegado de Protección de Datos, y en última instancia acudir a la Comisión de Seguridad, para obtener el visto bueno al tratamiento.

14. MEJORA CONTINUA, MODIFICACIONES Y DEROGACIÓN

Será misión de la Comisión de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de su revisión o mantenimiento. La Política será aprobada por Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

Queda derogada la anterior Política de Seguridad de la Información, que fue aprobada por el Consejo de Gobierno de la Universidad de Almería, en fecha 18 de junio de 2018, así como las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Política de Seguridad de la Información.

15. APROBACIÓN Y ENTRADA EN VIGOR

Esta política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación por el Consejo de Gobierno de Universidad de Almería (en adelante, UAL) y hasta que sea reemplazada por una nueva Política.