ACG186/2: Aprobación de la Política de Seguridad de la Información de la Universidad de Granada

- Aprobado en la sesión ordinaria del Consejo de Gobierno de 26 de octubre de 2022

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE GRANADA

ÍNDICE

1. Introducción: Justificación y medidas.

El adecuado cumplimiento del servicio público de la educación superior por parte de las Universidades se fundamenta en los sistemas de información basados en Tecnologías de Información y Comunicaciones (TIC). Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a 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 las universidades deben aplicar las medidas mínimas de seguridad exigidas 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 ciberincidentes para garantizar la continuidad de los servicios prestados. La complejidad es aún mayor teniendo en cuenta el desarrollo continuado de las TIC en los últimos años, que ha supuesto una significativa incidencia en la progresión hacia sociedades digitalizadas, en las que el tratamiento de la información con adecuadas garantías se erige en un pilar esencial para preservar el ingente tráfico de datos, sean personales o no, que se produce a nivel global.

La Universidad de Granada depende de los sistemas TIC para alcanzar sus fines y objetivos; y todas las unidades administrativas de la universidad deben tener presente 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 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público impuso la implantación definitiva de la Administración electrónica, con una doble garantía:

1. La interoperabilidad en la toma de decisiones: Esquema Nacional de Interoperabilidad, que implica la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos, garantizando el derecho de los ciudadanos a comunicarse con las Administraciones Públicas a través de medios electrónicos en condiciones de igualdad en el marco del respeto al principio de neutralidad tecnológica.
2. La garantía de la seguridad de la información tratada: Esquema Nacional de Seguridad (en adelante ENS), ampliando su ámbito de aplicación a todo el sector público, al que pertenecen las universidades.

El objeto del ENS es establecer la política de seguridad en la utilización de medios electrónicos y debe actualizarse de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos estándares

internacionales sobre seguridad y auditoría y la consolidación de las infraestructuras que le sirven de apoyo. Así lo establecía el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, que ha sido derogado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Este último es fruto de la progresiva transformación digital de la sociedad, el vertiginoso avance de las tecnologías de aplicación y el nuevo contexto de la ciberseguridad. Todo ello pone de manifiesto un incremento de los riesgos y amenazas de los sistemas de información en el ciberespacio, que exigen un nuevo marco regulatorio que sea capaz de dar respuesta a los mismos y garantice la preservación de los derechos. En este sentido, tanto la Estrategia de Seguridad Nacional 2017, aprobada por Real Decreto 1008/2017, de 1 de diciembre, como la Estrategia de Seguridad Nacional 2021, aprobada por Real Decreto 1150/2021, de 28 de diciembre, identifican al ciberespacio como un espacio común global, carente de fronteras físicas y de fácil accesibilidad, donde es difícil la atribución de cualquier acción irregular o delictiva, dada la débil regulación y la ausencia de soberanía. De conformidad con lo dispuesto en el artículo 2 del Real Decreto 311/2022, el ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Junto a ello, la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13, incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

La aprobación del 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, en adelante RGPD), de plena aplicación desde el 25 de mayo de 2018, ha supuesto un punto de inflexión importante, al regular el derecho fundamental a la protección de datos personales en una norma con eficacia directa en todos los Estados miembros de la Unión Europea, y especialmente al implicar una modificación sustancial del enfoque de la gestión de la privacidad, lo que hace que las sinergias entre seguridad de la información y protección de datos sean imprescindibles.

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, estableció es su disposición adicional primera que dichas medidas se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del RGPD 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. Además, dicha disposición adicional ordena la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales.

La Universidad de Granada, conforme a lo dispuesto en el artículo 11 del Real Decreto 3/2010 (modificado por el Real Decreto 951/2015, de 23 de octubre), y con la finalidad de fundamentar la confianza en que los sistemas de información en el seno de la Universidad prestan sus servicios y custodian la información de acuerdo con las especificaciones funcionales del ENS, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas, aprobó mediante Resolución del Rector de 18 de septiembre de 2013, la Política de Seguridad de la Información de la Institución, que fue modificada por Resolución de la Rectora de 21 de marzo de 2017, como documento estructural de garantía de los sistemas de información de la Universidad, en el marco estratégico y operativo que supone la implementación y cumplimiento del ENS.

En el contexto regulatorio actual se hace preciso actualizar la política de seguridad integrando la política de protección de datos, teniendo en cuenta, además, lo dispuesto en el artículo 99 del RGPD, en cuanto que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos de dicho Reglamento. Ello implica que desde la Universidad se adopten políticas internas y las medidas adecuadas para cumplir en particular con los principios de protección de datos desde el diseño y por defecto. Entre tales medidas, el artículo 24 RGPD incluye la aplicación de las oportunas políticas de protección de datos.

La presente política de seguridad de la información se constituye en el documento base mediante el cual se define el marco de referencia que permite la gestión de la seguridad de la información y de la protección de datos en el contexto de las actividades de tratamiento con datos personales y los sistemas de información de la Universidad de Granada. En ella se establecen las medidas, organización y funciones correspondientes a cada ámbito específico de competencia.

La Universidad de Granada, a través de la presente Política de Seguridad, de conformidad con lo dispuesto en el artículo 7 del ENS, da cumplimiento al objetivo de la Seguridad de la Información garantizando la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, con la aplicación de las medidas que se relacionan a continuación.

1.1 Prevención.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de Granada 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 roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Para garantizar el cumplimiento de esta Política, la Universidad de Granada:

- Autorizará los sistemas antes de entrar en operación.
- Evaluará regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicitará la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

1.2 Detección.

La Universidad de Granada, 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 de conformidad con lo dispuesto en el artículo 10 del ENS (reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

1.3 Respuesta.

La Universidad de Granada, podrá adoptar las siguientes medidas:

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

1.4 Recuperación.

Para garantizar la disponibilidad de los servicios, la Universidad de Granada dispondrá de los medios y técnicas necesarios que permitan garantizar la recuperación de los servicios más críticos.

2. Misión de la Universidad de Granada.

La Universidad de Granada, fundada en 1531 y con presencia en dos continentes, es una institución pública de educación superior comprometida con los valores de inclusión, igualdad de oportunidades, respeto a la diversidad de las personas y desarrollo sostenible; que desde la pluralidad intelectual y la excelencia en el desarrollo de sus funciones busca realizar contribuciones significativas a los desafíos a los que se enfrenta la humanidad, formando personas íntegras, generando valor para la sociedad y liderando la transformación tecnológica, económica y social a través del conocimiento y la difusión de la cultura y de su patrimonio.

La Universidad de Granada pone a disposición de la ciudadanía la realización de trámites online y nuevas vías de participación que garanticen el desarrollo y la eficacia de sus funciones y cometidos.

Al potenciar el uso de las nuevas tecnologías en la Universidad de Granada, se persigue fomentar la relación electrónica entre todos los actores (docentes, estudiantes, investigadores, personal de administración y servicios, y otros) con la Universidad.

3. Principios básicos.

Los principios básicos son las 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, 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 determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el 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, a los cambios normativos y, en su caso, a las recomendaciones del Comité de Seguridad de la Información y la/el Delegada de Protección de Datos de la Universidad. 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.
- Formación y concienciación en seguridad. Se establecerán programas de concienciación y formación continua en materia de seguridad de la información para atender a la comunidad universitaria.

4. Objetivos de la Seguridad de la Información.

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

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- 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, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un 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.
- 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 con 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 de datos personales, con especial atención a las categorías especiales de datos, para cumplir la legislación de seguridad y privacidad.
- 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 y, en su caso, en materia de protección de datos personales.

5. Objeto y alcance.

La política de seguridad de la información tiene por objeto, conforme a lo establecido en el Real Decreto 311/2022 y lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, establecer los objetivos, las directrices, las medidas y la organización para gestionar y proteger la información que trata la Universidad de Granada, así como los servicios que

presta. En concreto, define:

- La misión de la Universidad.
- El marco regulatorio en el que se desarrollarán las actividades.
- Las funciones de seguridad, definiendo los deberes y responsabilidades.
- La estructura y composición de los órganos de gobernanza en el ámbito de la gestión y coordinación de la seguridad, su ámbito de responsabilidad y la relación con otras áreas de la Universidad.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- La gestión de los riesgos.

La Política de Seguridad de la Universidad de Granada y sus documentos complementarios se aplicarán a todos los sistemas de información de la Universidad, a sus servicios centrales y periféricos, a sus centros y departamentos y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable la Universidad de Granada. También se aplicarán 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 de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

Se consideran sistemas TIC de la Universidad todos aquellos sistemas que emplean tecnologías de la información y de las comunicaciones para recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir datos e información.

No se considerará sistema TIC de la Universidad a aquellos ordenadores personales financiados a título individual, no inventariados a nombre de la Universidad, aunque pudieran ocasionalmente ser usados para labores propias de investigación, docencia o gestión. Por tanto, quedan fuera de este ámbito dichos elementos. En estos casos, la Universidad se reserva el derecho de proporcionar acceso a la red de este tipo de recursos ajenos a la misma si no se proporcionan unos mínimos requisitos de seguridad o existen indicios o evidencias de un incidente potencial de seguridad que pueda comprometer o bien a seguridad de la información de los sistemas TIC o bien su buen nombre o imagen corporativa.

6. Marco normativo.

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

- 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.

- Artículo 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- 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.
- 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 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.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Universidad de Granada, derivadas de las anteriores y publicadas en la sede electrónica comprendidas dentro del ámbito de aplicación de la presente Política; así como las que adopte esta Universidad en materia de Privacidad y Protección de Datos.

Esta política de seguridad se adaptará a cualquier modificación normativa en la materia.

7. Organización de la Seguridad de la Información.

7.1. Acciones para la organización de la Seguridad de la información.

El mantenimiento y gestión de la seguridad de la información va íntimamente ligado al establecimiento de una organización de seguridad, que compromete a todos los miembros de la Universidad.

La Universidad de Granada, 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, para organizar la seguridad de la información, emprenderá las siguientes acciones:

1. Designará roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegada/o de Protección de Datos.
2. Constituirá un órgano 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 de la Información.

7.2. Roles y órganos de la Seguridad de la Información de la Universidad de Granada.

7.2.1. Roles asociados a la Seguridad de la Información.

En la Universidad de Granada, en el marco del ENS, los roles de la Seguridad de la Información serán los siguientes:

- Responsable de los Servicios: Gerente de la Universidad de Granada.
- Responsables de la Información: Secretaria/o General de la Universidad de Granada.
- Responsable de Seguridad de la Información: Persona designada por la Rectora o Rector, a propuesta del Comité de Seguridad de la Información. El Responsable de la Seguridad no podrá ser un órgano de gobierno unipersonal de la universidad y no deberá tener ninguna responsabilidad sobre la prestación de los servicios TIC, ni deberá estar bajo la dependencia jerárquica del Responsable del Sistema (y viceversa).

- Responsable del Sistema: Directora o Director del Centro de Servicios Informáticos y Redes de Comunicación.
- Administradores de la seguridad del sistema: Las/los Jefes de Servicio del Centro de Servicios de Informática y Redes de Comunicaciones relacionados con la materia, y en general las personas encargadas de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de esta política de seguridad.

7.2.1.1. Responsable de la Información.

Le corresponderán las siguientes funciones:

- Determinar los requisitos de la información tratada.
- Velar por el buen uso de la información y, por tanto, de su protección.
- Elevar para su aprobación al Comité de Seguridad de la Información, a propuesta del Responsable de Seguridad de la Información y con la conformidad del Responsable del Sistema, los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información), dentro del marco establecido en el Anexo I del RD ENS.
- Valorar las solicitudes relativas al ejercicio de los derechos de acceso a la información y a los datos personales de cuyo tratamiento sea responsable la Universidad de Granada, con el asesoramiento de la Delegada o Delegado de Protección de Datos.
- Poner en conocimiento del Responsable de Seguridad de la Información cualquier variación respecto a los niveles de seguridad de la Información.

7.2.1.2. Responsable de los Servicios.

Serán funciones del Responsable de los Servicios:

- Determinar los requisitos de los servicios prestados.
- Establecer los requisitos del servicio en materia de seguridad de la información, incluyendo los correspondientes a interoperabilidad, accesibilidad y disponibilidad.
- Elevar para su aprobación al Comité de Seguridad de la Información, a propuesta del Responsable de Seguridad de la Información y con la conformidad del Responsable del Sistema, los requisitos de seguridad aplicables a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del Real Decreto que regula el ENS.
- Dictaminar respecto a los derechos de acceso a los servicios.
- Poner en conocimiento del Responsable de Seguridad de la Información cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios.

7.2.1.3. Responsable de Seguridad de la Información.

Serán funciones del Responsable de Seguridad de la Información:

- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, e informar al respecto.
- Supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos e informar sobre estas cuestiones.

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
- 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 del ENS.
- Elevar al Comité de Seguridad la aprobación de cambios y el establecimiento de otros requisitos del sistema de seguridad.

7.2.1.4. Responsable del Sistema.

Serán funciones del Responsable del Sistema:

- Desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Disponer, como medida provisional o cautelar, con las garantías correspondientes, la suspensión del acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Proporcionar asesoramiento para las/los Jefes de Servicio del Centro de Servicios de Informática y Redes de Comunicaciones relacionados con la materia determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad de la Información y/o Comité de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de 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.

7.2.1.5. Administradores de la seguridad del sistema.

Serán funciones de los administradores de la seguridad del sistema:

- Gestionar, configurar y actualizar, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- Gestionar 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.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de la Información 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.

7.2.2. Órganos de Seguridad de la Información.

Los órganos de seguridad de la Información de la Universidad de Granada serán los siguientes:

7.2.2.1. Comité de seguridad de la Información.

El Comité de Seguridad de la Información (CSI) estará integrado por los siguientes miembros:

- Presidencia: Secretaria/o General o persona en quien delegue.
- Secretario/a del Comité: Responsable de Seguridad de la Información.
- Vocales:
    - Responsable de los Servicios.
    - Responsable de la Información.
    - Responsable de Sistema.
    - Delegada/o de la Rectora para la Universidad Digital o, en su caso, la persona que ostente dichas competencias.
    - Subdirector/a del CSIRC.
    - Delegada/o de Protección de datos, que asistirá con voz, pero sin voto.
- Podrán asistir como invitados las personas que se considere oportuno para los temas en cuestión, con voz, pero sin voto.

Serán funciones del Comité de Seguridad de la Información:

- Informar regularmente del estado de la seguridad de la información al Rectorado.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Universidad de Granada en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para que sea aprobada por el Consejo de Gobierno.
- Proponer la normativa de seguridad de la información y la Normativa de Uso de

Medios electrónicos para su aprobación por Consejo de Gobierno.

- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Universidad de Granada y adoptar las medidas que sean necesarias y posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes (ciberincidentes) de seguridad y proponer/adoptar 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 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 Universidad de Granada. En particular velará por la coordinación de los diferentes planes que puedan implantarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los sistemas de información 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 de información.
- Resolver los conflictos que puedan surgir entre los diferentes responsables en el ejercicio de sus funciones, o, en su caso, derivando la resolución del asunto a los órganos correspondientes.
- Aprobar documentos, como guías e instrucciones técnicas que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Periodicidad de las reuniones y adopción de acuerdos:

- El Comité de Seguridad de la Información se reunirá, al menos, dos veces al año 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.
- En cualquier caso, las reuniones se convocarán por su Presidenta/e, a través del Secretario/a, a su iniciativa o por mayoría de sus vocales.
- Las decisiones se adoptarán por consenso de los vocales.

7.2.2.2. Oficina de Seguridad de la Información.

La Universidad de Granada habilitará las unidades funcionales o administrativas necesarias para el efectivo desarrollo de las competencias y funciones en materia de seguridad de la información. Al respecto, se creará una Oficina de Seguridad de la Información, en el plazo previsto en la Disposición Transitoria Única del Real Decreto núm. 311/2022, con las funciones de apoyo administrativo al Responsable de seguridad de la información.

7.2.2.3. Delegada/o de Protección de Datos.

Serán funciones de la Delegada/o de Protección de Datos:

- Informar y asesorar a la Universidad de Granada, y a los usuarios que se ocupen del tratamiento de datos personales, 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 normativa de seguridad y de las políticas internas de la Universidad de Granada en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con el Consejo de Transparencia y Protección de Datos de Andalucía cuando éste lo requiera, actuando como punto de contacto con éste, y en su caso con la Agencia Española de Protección de Datos, para cuestiones relativas al tratamiento de datos personales.

La Delegada/o 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 al realizar una evaluación de impacto de operaciones de tratamiento en la protección de datos personales, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.
- Asesorar al Responsable del tratamiento sobre áreas a someter a auditoría, actividades de formación a realizar en materia de protección de datos personales y operaciones de tratamiento a las que dedicar más tiempo y recursos.

7.2.3 Procedimientos de designación.

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por la Rectora o Rector de la Universidad de Granada.

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

8. Gestión de riesgos.

Todos los sistemas afectados por la presente Política de Seguridad de la Información 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:

- Al menos una vez al año.
- 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 y, en su caso, de la Oficina de Protección de Datos.

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 de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, enero, 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.

9. Datos Personales.

La Universidad de Granada solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos, y adoptará una Política de Privacidad y Protección de Datos personales adecuada a la normativa vigente en la materia.

10. Notificación de incidentes.

De conformidad con lo dispuesto en el artículo 33 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, la Universidad de Granada 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.

11. Desarrollo de la Política de Seguridad de la Información.

La presente Política de Seguridad de la Información será desarrollada, en su caso, a través de los oportunos reglamentos, guías y recomendaciones.

Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario, mejoras a la misma. Asimismo, corresponde al Comité la propuesta al Consejo de Gobierno de la aprobación de las normas oportunas para este desarrollo.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de la Universidad de Granada en materia de protección de datos. Ambas estarán a disposición de todos los miembros de la Universidad y serán objeto de la debida publicidad.

12. Terceras partes.

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

Cuando la Universidad de Granada utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la normativa de seguridad que ataña a 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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando ello implique el encargo de tratamiento de datos personales a terceros, la Universidad y el tercero deberán formalizar el correspondiente contrato o acto jurídico de encargo de tratamiento, con el contenido mínimo establecido en el artículo 28 del RGPD. La Universidad, como responsable del tratamiento, deberá velar por que el encargado ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos establecidos en la normativa de protección de datos y se garantice la protección de los derechos de los interesados.

Cuando algún aspecto de esta Política de Seguridad de la Información 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. 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:

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

Aprobación y entrada en vigor.

La presente Política de Seguridad de la Información será aprobada por Acuerdo del Consejo de Gobierno y será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.