



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-075-2

Fecha de Edición: mayo de 2022

Personal de la CRUE y la empresa CIES han participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y las telecomunicaciones (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 311/2022 por el que se regula el Esquema Nacional, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

| | |
|--|-----------|
| 1. APROBACIÓN Y ENTRADA EN VIGOR..... | 5 |
| 2. INTRODUCCIÓN | 5 |
| 2.1 PREVENCIÓN | 5 |
| 2.2 DETECCIÓN..... | 6 |
| 2.3 RESPUESTA | 6 |
| 2.4 RECUPERACIÓN | 6 |
| 3. MISIÓN DE LA UNIVERSIDAD DE _____ | 6 |
| 4. PRINCIPIOS BÁSICOS..... | 7 |
| 5. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN..... | 8 |
| 6. ALCANCE..... | 9 |
| 7. MARCO NORMATIVO..... | 9 |
| 8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN..... | 11 |
| 8.1 CRITERIOS UTILIZADOS PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 11 |
| 8.2 ROLES Y ÓRGANOS DE LA SEGURIDAD DE LA INFORMACIÓN | 11 |
| 8.3 RESPONSABILIDADES DE LOS ROLES ASOCIADOS AL ESQUEMA NACIONAL DE SEGURIDAD | 13 |
| 8.3.1 RESPONSABLE DE LA INFORMACIÓN Y DE LOS SERVICIOS | 13 |
| 8.3.2 RESPONSABLE DE LA SEGURIDAD | 13 |
| 8.3.3 RESPONSABLE DEL SISTEMA..... | 14 |
| 8.4 DELEGADO DE PROTECCIÓN DE DATOS..... | 15 |
| 8.5 COMITÉ DE SEGURIDAD TIC (COMSEGTIC) | 16 |
| 8.6 OFICINA DE SEGURIDAD TIC..... | 17 |
| 8.7 CENTRO DE OPERACIONES DE CIBERSEGURIDAD (COCS)..... | 19 |
| 8.7.1 FUNCIONES..... | 19 |
| 8.8 FORO DE SEGURIDAD TIC DE LAS UNIVERSIDADES | 20 |
| 8.8 PROCEDIMIENTOS DE DESIGNACIÓN..... | 20 |
| 9. DATOS PERSONALES | 20 |
| 10. OBLIGACIONES DEL PERSONAL | 21 |
| 11. GESTIÓN DE RIESGOS..... | 21 |
| 12. NOTIFICACIÓN DE INCIDENTES | 22 |
| 13. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN | 22 |
| 14. TERCERAS PARTES | 23 |
| 15. MEJORA CONTINUA..... | 23 |
| 16. MODIFICACIONES | 24 |

1. Aprobación y entrada en vigor

Texto aprobado el día ___ de _____ de _____ por (Resolución / Acuerdo de Rectorado/ Junta de Gobierno /...) de la Universidad de _____.

Esta “Política de Seguridad de la Información”, en adelante Política, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. Introducción

La Universidad de _____, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la 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 los departamentos 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.

De este modo, todas las unidades administrativas de la universidad tienen 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.

Por tanto, para la Universidad de _____, 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 para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

2.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de _____, implementa 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, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Universidad de _____:

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

2.2 Detección

La Universidad de _____, establece 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 en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3 Respuesta

La Universidad de _____, 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.
- 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).

2.4 Recuperación

Para garantizar la disponibilidad de los servicios, la Universidad de _____, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

3. Misión de la Universidad de _____

La Universidad de _____, 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 _____, se persigue fomentar la relación electrónica todos los actores (docentes, estudiantes, investigadores, personal de administración y servicios, y otros) con la universidad.

4. 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, 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 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. 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.

5. Objetivos de la Seguridad de la Información

La Universidad de _____, 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 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.

6. Alcance

Esta Política se aplicará a los sistemas de información de la Universidad de _____, 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 de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue al personal afectado.

7. Marco normativo

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

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 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.
- 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 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.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- 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
- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto 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 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- 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.
- [...]

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

8. Organización de la Seguridad de la Información

8.1 Criterios utilizados para la organización de la Seguridad de la Información

La Universidad de _____, teniendo en cuenta lo establecido en el antedicho 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”, para organizar la seguridad de la información emprenderá las siguientes acciones:

- i. Designará roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.
- ii. 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 de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

8.2 Roles y Órganos de la Seguridad de la Información

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

- Responsables de los Servicios y Responsables de la Información: (Podrían ser los jefes y responsables de los diferentes órganos y unidades administrativas, o bien, aunar ambas figuras y que el Secretario General, como máxima autoridad administrativa, asumiera esas funciones).
- Responsable de Seguridad de la Información: **A designar**

El Responsable de la Seguridad corresponderá a un cargo o funcionario, de nivel ejecutivo, designado formalmente por el Rector o el Equipo de Dirección. 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: **Director o Jefe de Servicio del Área de TI**
- Comité de Seguridad TIC (COMSEGTIC):
 - Presidencia: Rector o delegado.
 - Vocales:
 - Miembros permanentes:
 - Secretario/a del COMSEGTIC: Secretario General o delegado
 - Responsable de Sistema (RSIS)
 - Responsable de Seguridad de la Información (RSEG)
 - Representantes de Información y Servicios de la universidad.
 - Asesores que se consideren oportunos para los temas en cuestión, pudiendo incluso acudir un representante del Centro Criptológico Nacional (CCN), con voz, pero sin voto.
 - El Delegado de Protección de datos.
 - Miembros no permanentes:
 - El Comité de Seguridad TIC podrá invocar la presencia en sus reuniones tanto de otros representantes de la universidad como de especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Los Representantes de la Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de seguridad TIC de la universidad. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de la misma.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así

como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

El Secretario/a del Comité realizará las convocatorias y levantará actas 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 pertinentes su Presidente.

8.3 Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

8.3.1 Responsable de la Información y de los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información 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 Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

8.3.2 Responsable de la Seguridad

Serán funciones del Responsable de Seguridad:

- 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 TIC.
- 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 no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

8.3.3 Responsable del Sistema

Serán funciones 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 Seguridad y/o Comité de Seguridad de la Información 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.
- Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:
 - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
 - 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.

- Aprobar los cambios en la configuración vigente del Sistema de Información.
- 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 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.

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.

8.4 Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a la Universidad de _____, 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 normativa de seguridad y de las políticas internas de la Universidad de _____, 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.
 - Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

8.5 Comité de Seguridad TIC (COMSEGTIC)

Serán funciones del Comité de Seguridad TIC:

Atribuciones del Comité de Seguridad TIC:

- 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 de Uso de Medios electrónicos para todo el personal.
- k) Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.

Periodicidad de las reuniones y adopción de acuerdos:

1. Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el Comité de Seguridad TIC se reunirá, al menos, una vez al trimestre.
2. Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados por la universidad, el Comité de Seguridad TIC 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.
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 los miembros permanentes.

8.6 Oficina de Seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la **Oficina de Seguridad TIC**¹, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad y otras funciones conexas o concordantes. Para su **composición** se propone:

- El **Director de la Oficina de seguridad TIC**, nombrado por el Comité de Seguridad TIC, que actuará como enlace con el mismo, que será el **Responsable de Seguridad (RSEG)**, o la persona en quien delegue.

¹ Se puede considerar también la posibilidad de englobar en una única Oficina de Seguridad las funciones de seguridad TIC, la de las personas, la de las infraestructuras, la de la documentación, etc.

- **Secretario de la Oficina de Seguridad TIC**, nombrado por el Comité de Seguridad TIC, a propuesta de los miembros de la Oficina de Seguridad.

Todos aquellos **administradores especialistas de seguridad (AES)** que el Responsable de Seguridad determine que sean necesarios.

Las **funciones de la Oficina de Seguridad TIC** serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad TIC:

- a) Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.
- b) Redacción y presentación de propuestas al Comité de Seguridad TIC. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
- c) Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
 - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al Comité de Seguridad TIC para su revisión y posterior aprobación del órgano superior².
 - Elaborar la normativa de Seguridad de la Información para su aprobación por el Responsable de Seguridad, con conocimiento del Comité.
 - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
 - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
 - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
 - Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
 - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
 - Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la Información y protección de datos.

² Rector o Junta de Gobierno

Periodicidad de las reuniones y adopción de acuerdos:

1. El Director de la Oficina de Seguridad TIC convocará las reuniones de trabajo de sus miembros y recabará los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad TIC, para su aprobación, en su caso.
2. La Oficina podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en la Oficina de Seguridad TIC serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad TIC.
3. Se reunirá, al menos, una vez al mes y siempre antes de las celebraciones del Comité de Seguridad TIC.

8.7 Centro de Operaciones de Ciberseguridad (COCS)

Bajo la responsabilidad y dirección del Director de la Oficina de Seguridad TIC de la universidad, o la persona que este designe con conocimiento del Comité de Seguridad TIC, el Centro de Operaciones de Ciberseguridad (COCS) presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

8.7.1 Funciones

El Centro de Operaciones de Ciberseguridad (COCS) llevará a cabo las siguientes funciones:

- Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operaciones de seguridad sobre los dispositivos de defensa.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad: Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/patcheo) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

El Área/Servicio TI deberá, por un lado, coordinarse con la Oficina de Seguridad TI en la definición y aplicación de las medidas de seguridad en los sistemas e infraestructuras que estén bajo su responsabilidad; y por el otro, colaborar con el Centro de Operaciones de Ciberseguridad (COCS) en las tareas de operativa diaria.

En el caso en el que una universidad, por su tamaño o falta de recursos, no disponga de un COCS, el Área/Servicio TI podrá asumir, en colaboración con la Oficina de Seguridad TIC, en todo o en parte, las funciones propias del mismo.

3.4. Foro de seguridad TIC de las Universidades

El Foro de seguridad TIC se constituye como un punto de encuentro de las universidades en el ámbito del Esquema Nacional de la Seguridad.

La Sectorial CRUE-TIC3, entre cuyas misiones está la de *“Estudiar las necesidades y aplicaciones de las TIC en la gestión, la docencia y la investigación, proponiendo actuaciones y proyectos conjuntos a las Universidades”*, dispone de un Grupo de Trabajo específico de Seguridad y Auditoría TI. En dicha Sectorial están representadas todas las universidades españolas, tanto públicas como privadas. Dicho Grupo de Trabajo constituye el marco ideal para ser el Foro de Seguridad TIC para universidades. Debido al carácter sectorial de mundo universitario, será de gran ayuda en el ámbito de la Gobernanza en ciberseguridad.

El funcionamiento del Foro se regirá según el Reglamento interno de la Sectorial CRUE-TIC. En el Foro de la Seguridad se plantearán, entre otras, las necesidades de seguridad de las universidades adheridas. Las propuestas planteadas por el Foro de Seguridad de las Universidades serán trasladadas a cada universidad por sus representantes para su análisis, debate y aprobación, si procede, por parte del Comité de Seguridad TIC.

Este Foro de Seguridad TIC podrá coordinarse con otros foros de carácter sectorial, local o regional.

8.8 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 el rector de la Universidad de _____,

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

9. Datos personales

La Universidad de _____, 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

³ <https://tic.crue.org/>

medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

La Universidad de _____, publicará en la Sede Electrónica su Política de Privacidad.

10. Obligaciones del personal

Todo el personal de la Universidad de _____, 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.

11. 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.

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 8 de 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.

12. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayoenero, La Universidad de _____, 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.

13. Desarrollo de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). 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.

El cuerpo normativo sobre seguridad 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 Política de Seguridad de la Información, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables a los organismos o unidades de la universidad a los que sea 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 de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al órgano superior de la Universidad de _____, **(Rectorado, Pleno, Junta de Gobierno, ...)** la aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de la Universidad, siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de la Universidad de _____, en materia de protección de datos.

La normativa de seguridad y, muy especialmente, la Política de seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos, será conocida y estará a disposición de todos los miembros de la universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet, en soporte papel, esta documentación será custodiada por el Servicio de Informática.

14. Terceras partes

Cuando la Universidad de _____, preste servicios a otros organismos o maneje información de otros organismos, se les hará participe 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 _____, utilice servicios de terceros o ceda información a terceros, se les hará participe 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 dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

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.

15. 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 de la Información.
- b) Revisión de los servicios e información y su categorización.
- c) Ejecución con periodicidad anual del análisis de riesgos.
- d) Realización de auditorías internas o, cuando procedan, externas.

- e) Revisión de las medidas de seguridad.
- f) Revisión y actualización de las normas y procedimientos.

16. Modificaciones

| Versión | Fecha | Modificaciones respecto a la versión anterior |
|---------|--------------------|---|
| 01 | __ de ____ de ____ | |

