centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 881

Guía de Adecuación al ENS para Universidades

Mayo 2022

MINISTERIO DE DEFENSA

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

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.07.08 17:35:22 +02'00'

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 regulado por el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, 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. INTRODUCCIÓN

La evolución y revolución tecnológica que nos rodea es un proceso globalizado que afecta a todos los aspectos de la sociedad y especialmente aquellos en los que se ve implicada la información. El sector público no es ajeno a ello y ha generado una gran transformación de sus procesos, servicios y gestión de la información. Las universidades públicas son parte activa de esta transformación generando grandes sinergias en el conocimiento, el aprendizaje, la transmisión y promoción de la cultura e innovación y desarrollo en toda su actividad, tanto formativa como de investigación.

El sistema universitario se ha convertido en un marco de innovación tecnológica abierto y flexible que promociona y difunde el conocimiento a toda la sociedad con diferentes modalidades incluida la colaboración y cooperación con diferentes sujetos.

Pero esta evolución conlleva también una mayor facilidad para el tratamiento de gran cantidad de información lo que genera nuevas amenazas que no deben pasar inadvertidas y generar un efecto inmediato, esto es, la información debe ser debidamente protegida, con independencia de cómo se manifieste y se gestione. La acción universitaria se ha convertido en un factor dinamizador de la sociedad que genera confianza en la ciudadanía y como tal, debe ser protegida y controlada en su sistema de información, de manera que goce de una salud preventiva, correctiva y reactiva, que le permita disfrutar de seguridad y resiliencia.

Para dar respuesta a las necesidades del sector público y en particular, de las universidades Públicas, surge el marco común de seguridad de la información en las administraciones públicas y su sector público, tal y como lo señala el legislador en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[1]. Este marco común lo establece el Esquema Nacional de Seguridad (ENS)[2], constituyendo los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios.

En el actual régimen en el que interactúan las Administraciones Públicas y el Sector Público en general, tras la aprobación de la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, con la primacía de los procesos electrónicos y consagrándose la comunicación electrónica entre el sector público y la ciudadanía, es imprescindible garantizar el cumplimiento de los principios básicos y requisitos mínimos enmarcados en el ENS, para todo el sector público.

Esto implica necesariamente que las universidades públicas adopten los principios y requisitos que se desarrollan en el ENS, en sus procesos e interactuaciones con otras entidades del sector público y con la ciudadanía, debiendo desplegar todas aquellas

[1] Art. 156.2. Ley 40/2015: *"El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada."*

[2] Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad.

medidas de seguridad que permitan la materialización de los citados principios y requisitos.

No olvidemos la necesidad de generar la clara confianza que en la ciudadanía debe despertar relacionarse con la universidad mediante medios electrónicos, lo que implica necesariamente que la propia universidad debe mantener las obligaciones que se derivan y entre otras, la aplicación de los principios de seguridad en el uso de la información y de los servicios.

En el ámbito de las administraciones públicas, el derecho a comunicarse con ellas a través de medios electrónicos comporta una serie de obligaciones que requieren, entre otras cosas, incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

La universidad pública debe desarrollar su servicio de educación superior mediante investigación, docencia y estudio, con sistemas seguros con carácter holístico, con la seguridad implementada con carácter transversal sin excepciones, lo cual debe generar sistemas innovadores para la organización y gestión de las universidades, seguros.

Para poder dar cumplimiento a esto, debe considerarse el principio de proporcionalidad, en relación a las dimensiones de seguridad que afectan a los servicios e información de las universidades públicas y a la categoría correspondiente del sistema de información de cada una de ellas.

Debido al carácter sectorial del mundo universitario, y bajo el amparo del Nuevo Real Decreto, se hace necesario adaptar la adecuación al Esquema Nacional de Seguridad a la propia naturaleza y funciones de las universidades públicas, mediante la elaboración de un Perfil de Cumplimiento Específico para Universidades, que permita la implementación de las medidas del Anexo II de forma más eficaz y eficiente racionalizando los recursos requeridos sin menoscabo de la protección perseguida exigible.

Se ha tenido en cuenta la naturaleza de la universidad pública y el servicio público que debe desarrollar desplegado en las funciones reconocidas por la Ley Orgánica 6/2001 de 21 de diciembre, de Universidades.

2. OBJETIVO Y ALCANCE DE LA GUÍA

El objetivo de la presente Guía es proporcionar un modelo que facilite la Adecuación al ENS de los sistemas de las universidades públicas de forma ordenada y efectiva, que permita obtener la Certificación de Conformidad para sus sistemas según el Perfil de Cumplimiento Específico para Universidades que se ha desarrollado.

La presente Guía pretende abarcar la gestión de la ciberseguridad en las universidades públicas de manera integral, comenzando con el desarrollo de un modelo de gobernanza (desde la designación de roles de seguridad hasta la constitución de los órganos específicos que la gestionen, teniendo en cuenta las particularidades propias que se derivan de la naturaleza jurídica de las universidades públicas). Esta organización, junto con los compromisos de seguridad, se reflejará en la Política de Seguridad.

A continuación, habrá que elaborar un Plan de Adecuación de los sistemas de la universidad, mediante la identificación de los activos esenciales, su valoración, categorización, obtención de la declaración de aplicabilidad, análisis de riesgos…, del que resultará un Perfil de Cumplimiento Específico con las medidas que resulten de aplicación a sus sistemas para garantizar la seguridad de los mismos.

Como objetivo último, las universidades deberán superar el proceso de Certificación al ENS conforme al Perfil de Cumplimiento recomendado en esta guía, iniciando así el ciclo de gobernanza de la ciberseguridad, mediante la revisión y mejora continua de los procesos de seguridad desplegados en el sistema.

Para el desarrollo del Plan de Adecuación y la elaboración de la Política de Seguridad, el Centro Criptológico Nacional pone a disposición de las universidades sus herramientas de Gobernanza de la Ciberseguridad INES y AMPARO. Asimismo, en la Guía se proporciona un modelo desarrollado de Política de Seguridad y de Plan de Adecuación, en los Anexos I y II, respectivamente.

Se espera que cada universidad particularice las pautas de carácter general establecidas a lo largo de esta Guía, para adaptarlas a su ámbito, naturaleza, competencias y entorno singular.

3. MODELO DE GOBERNANZA

La gestión de la seguridad de los sistemas de información de las universidades - definición, implantación y mantenimiento - exige establecer una Organización interna de la Seguridad. Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

Cada universidad deberá establecer y aprobar su propio modelo de gobernanza de acuerdo con su estructura, dimensión y recursos disponibles, y deberá recogerlo en su Política de Seguridad de la Información.

Tras consensuar con la CRUE, y en base a la experiencia, se propone el siguiente Modelo de Gobernanza de la Seguridad en las universidades que facilita la toma de decisiones interna y articula la colaboración entre ellas. Está destinado a la gestión de los procesos relacionados con el Esquema Nacional de Seguridad y basado en bloques de responsabilidad. Habrá que adaptar este modelo a las posibilidades reales de decisión, gestión y operación de la seguridad de cada entidad.

Según el modelo, la gobernanza de la seguridad en la universidad se articula a través de un **Comité de Seguridad TIC**, se gestiona a través de una **Oficina de Seguridad TIC**, y se implementa mediante **Centros de Operaciones de Ciberseguridad** en colaboración con el Área o Servicio de TI. El COCS, realiza una vigilancia continua de los sistemas bajo su responsabilidad, junto a otros roles, y colabora con el Área o Servicio TI, para asegurar la correcta operación e implementación de la seguridad.

A modo de ejemplo se representa gráficamente la estructura básica del Comité de Seguridad TIC, la Oficina de Seguridad TIC y el Centro de Operaciones de Ciberseguridad de dos universidades, así como su relación con el Foro de Seguridad TIC.

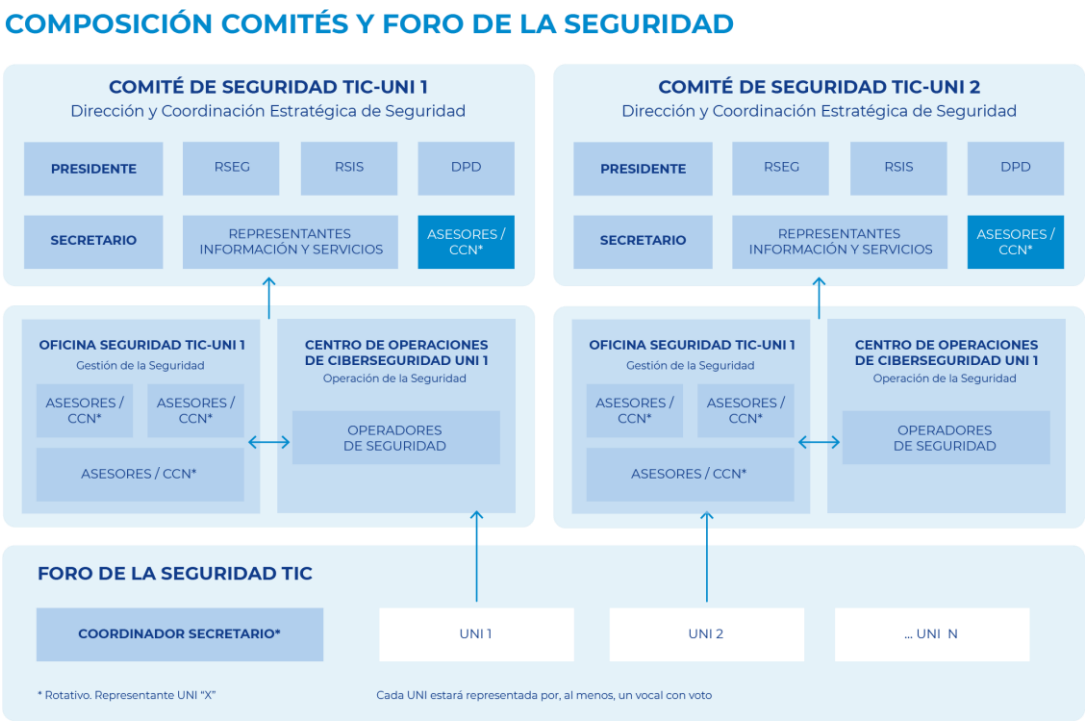

Figura 1: Composición Comité, Oficina, COCS y Foro de la Seguridad TIC

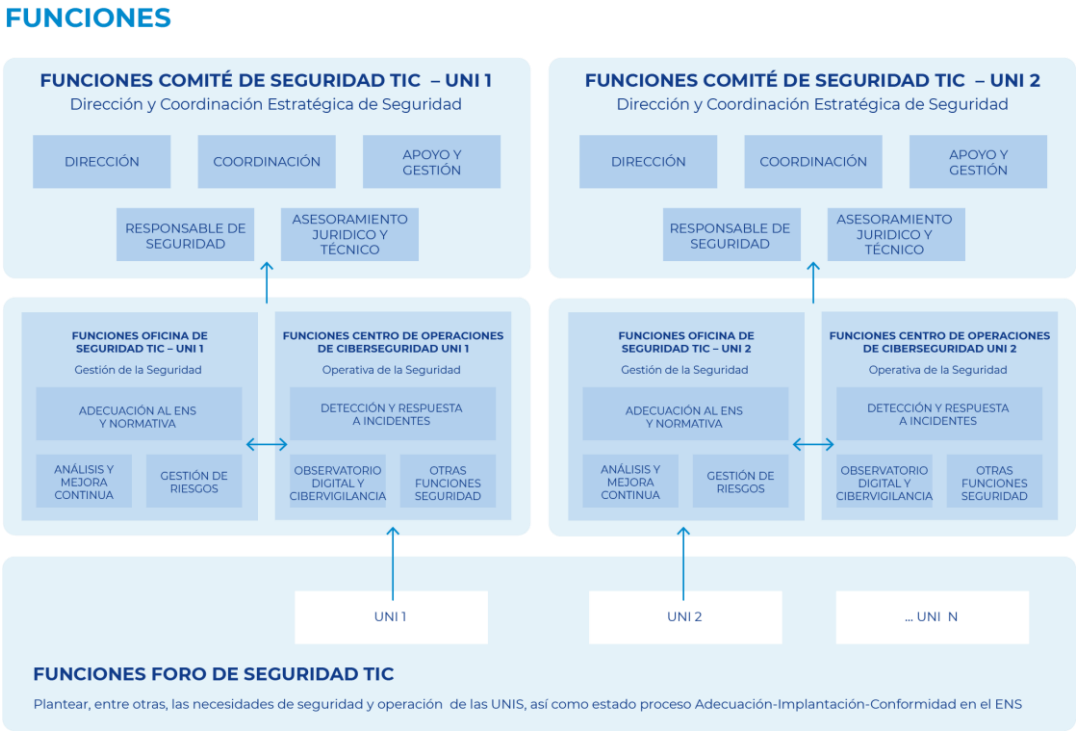

Figura 2: Funciones Comité, Oficina, COCS y Foro de la Seguridad TIC

Además, para facilitar la obtención de la Certificación de Conformidad a las universidades, y en función del tamaño de las mismas, se puede constituir un Órgano de Auditoría Técnica (OAT) destinado a realizar las Revisiones periódicas y Auditorías de Conformidad, siempre que se garantice la debida imparcialidad (inexistencia de conflicto de interés) entre el personal destinado a la Implantación del ENS del organismo auditado y el equipo auditor del órgano de auditoría técnica.

Conforme a lo descrito en las figuras anteriores, y teniendo en cuenta el OAT, se pueden resumir los procesos de gestión en la siguiente estructura de organización de la seguridad:

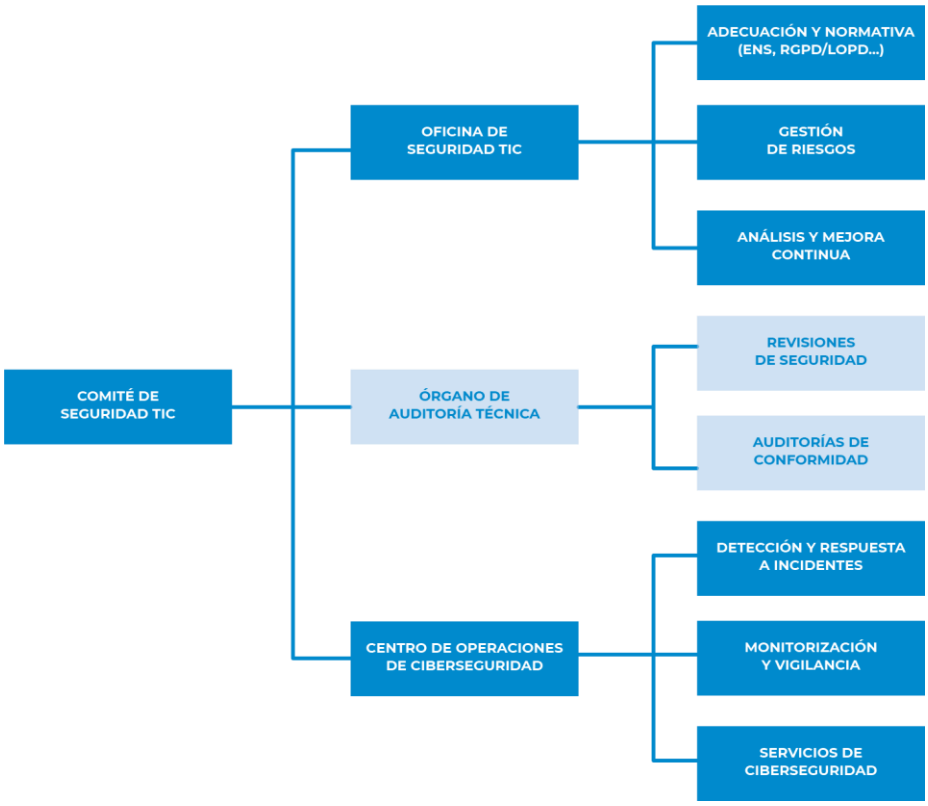

Figura 3: Organización de la Seguridad: Oficina, COC y OAT

Como puede observarse, lo Oficina y el OAT llevarán a cabo tareas de prevención proactiva, y en el COCS se realizará la vigilancia, detección y respuesta.
Si la organización no dispone de OAT, la estructura se simplificaría según la siguiente imagen:

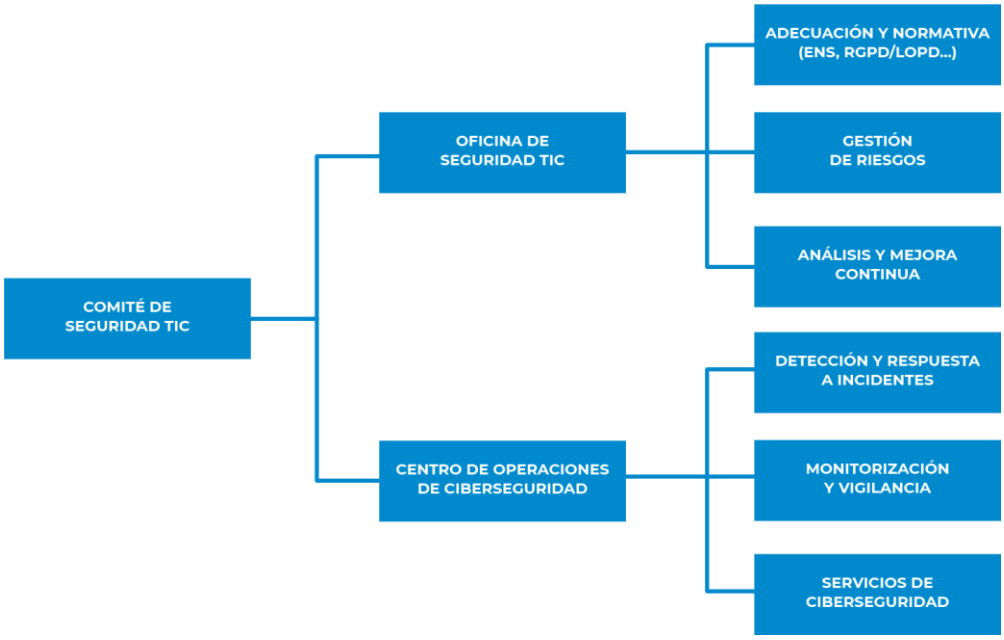

Figura 4: Organización de la seguridad – Oficina TIC y COC

3.1 Comité de Seguridad TIC

El Comité de Seguridad TIC se configura como un órgano colegiado que, de constituirse jurídicamente conforme a Derecho, estará regulado por lo dispuesto en la Sección 3ª del Capítulo II del Título Preliminar, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y por lo establecido en los presentes ToR (Terms of Reference). Para su **composición** se propone:

1. **Presidencia:** Rector o delegado.
2. **Miembros permanentes:**

   Serán miembros permanentes del Comité de Seguridad TIC, los siguientes:

   a) **El Secretario del COMSEGTIC** que será el Secretario General**,** o delegado.

   b) **El Responsable del Sistema (RSIS) de la universidad,** que será el Director o Jefe de Servicio del Área TI.

   c) **Responsable de Seguridad de la Información (RSEG)**[3] que será designado formalmente por el Rector de la Universidad o el equipo de dirección.

   d) Los **Representantes de Información y Servicios de la universidad** en función de los temas a tratar.

   Estos Representantes 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.

[3] Ver perfil del RSEG para Universidades en la Guía CCN-STIC-801 Responsabilidades y Funciones en el ENS.

e) Otros **Asesores** que se consideren oportunos o necesarios para los temas de la reunión en cuestión, pudiendo incluso acudir como asesor un representante del Centro Criptológico Nacional (CCN), con voz, pero sin voto.

f) El **Delegado de Protección de datos**, que participará con voz, pero sin voto.

3. **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.

Corresponden al **Comité de Seguridad TIC**, entre otras, las siguientes **funciones**:

a) Liderar, coordinar y velar por el correcto desarrollo del Proyecto de Adecuación al ENS, adoptando las medidas que correspondan, de acuerdo a los fines del Proyecto.

b) Alentar el proceso de Certificación de la Conformidad con el ENS para los servicios transversales prestados por la universidad.

c) Debatir en segunda instancia y decidir sobre la idoneidad de las propuestas realizadas por la Oficina de Seguridad TIC y trasladarlas al Órgano que las Aprobará formalmente (Rector o, por delegación, Junta Gobierno, Secretario General, Gerente, Vicerrector competencias TIC…).

d) Proponer para su análisis y, en su caso, redactar y publicar Normas, Criterios o Buenas Prácticas en materia de Seguridad y Adecuación al ENS y Certificación de la Conformidad con el ENS.

e) Asesorar al personal de la universidad de los procedimientos, herramientas y criterios en materia de Certificación de la Conformidad con el ENS y, en general, con su implantación, orientando su gestión al mejor servicio del sector público y la mayor y mejor colaboración con el sector privado, fabricantes y suministradores de productos o servicios.

f) Asesorar a las partes implicadas en la identificación de otros esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para los sectores público y privado.

g) Informar a las organizaciones públicas y privadas que corresponda sobre la implantación de la Certificación de Conformidad con el ENS en la universidad.

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.

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, por medio del Secretario a su iniciativa o por mayoría de sus miembros permanentes.
4. Las decisiones se adoptarán por consenso de los miembros permanentes.

3.2 Oficina de Seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad se podrá constituir una **Oficina de Seguridad TIC**[4], 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.
- **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:

[4] 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.

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 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 superior[5].
   - 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 del ENS que permitan verificar el cumplimiento de las obligaciones de las universidades en materia de seguridad de la Información y protección de datos.

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

[5] Rector o Junta de Gobierno

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.

3.3 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.

El COCS será único en la organización, aunque puedan existir varios emplazamientos físicos diferentes, todos los cuales operan bajo la dirección centralizada del Responsable de Seguridad.

Asimismo, en función de la naturaleza y dimensiones de la organización, el COCS puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el Responsable de Seguridad.

El **Centro de Operaciones de Ciberseguridad (COCS)** puede llevar 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.
- 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/parcheado) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

3.4 Área/Servicio TI de la Universidad

Bajo la responsabilidad del Director o Jefe de servicio, que ostenta el rol del Responsable del Sistema, las universidades disponen en su estructura organizativa de un Área o Servicio TI, que se compone de una plantilla de técnicos encargados de desarrollar, operar y mantener el sistema de información (redes de comunicaciones, aplicaciones, bases de datos, servidores, servicios e infraestructura TI en general) durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.

Tal y como se ha indicado al describir el funcionamiento del Modelo de Gobernanza, 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.

3.5 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-TIC6, 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 TIC 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.

[6] https://tic.crue.org/

3.6 Estructura y flujo de autorizaciones

ROL	FUNCIONES
COMITÉ DE SEGURIDAD TIC	Órgano colegiado que da respuesta a las necesidades de seguridad de la Universidad, desde el punto de vista estratégico, en relación con los sistemas de información utilizados para la prestación de servicios del alcance. **Presidente**: Rector o delegado **Vicepresidente**: Secretario general o delegado **Secretario**: Puede ser el Director de la Oficina y podría ser el Vicerrector de competencias TIC.
OFICINA DE SEGURIDAD TIC – CENTRO DE OPERACIONES DE CIBERSEGURIDAD	Como elemento de gestión y operativo, se constituirán la Oficina de Seguridad y el Centro de Operaciones de Ciberseguridad, cuyas competencias estarán relacionadas con la Normativa y análisis de riesgos, Seguridad en las interconexiones y conectividad, Vigilancia y determinación de superficie de exposición, Monitorización y gestión de incidentes, Observatorio digital y ciber vigilancia y otras funciones relacionadas con la seguridad.
FORO DE SEGURIDAD TIC	El Foro será un punto de encuentro de las Universidades que quieran adherirse a él. Podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas a trasladar a las Oficinas de Seguridad de cada Universidad y servirán análisis, debate y toma de decisiones en conjunto que serán aprobadas, si procede, por parte de cada Comité de Seguridad.

Figura 5: Modelo de Gobernanza - Estructura y funciones

Figura 6: Modelo de Gobernanza - Flujo de Autorizaciones

3.7 Modelo Extendido de Gobernanza

El modelo descrito admite variaciones en su desarrollo atendiendo a las características de la organización, tales como: la dimensión de esta, la asignación de funciones y responsabilidades, las dependencias organizativas y con terceros que existan, su grado de madurez y/o sus capacidades, por citar algunas de ellas. En consecuencia, hay más de un escenario de desarrollo del modelo. En todos ellos, la responsabilidad última de la seguridad siempre recae en el Comité de Seguridad TIC.

En una entidad de gran tamaño (medio-alto) y alto grado de madurez, se puede tomar la decisión de segregar las funciones de seguridad en dos (2) áreas: una que lideraría el cumplimiento y otra la operación, como se muestra en la figura siguiente.

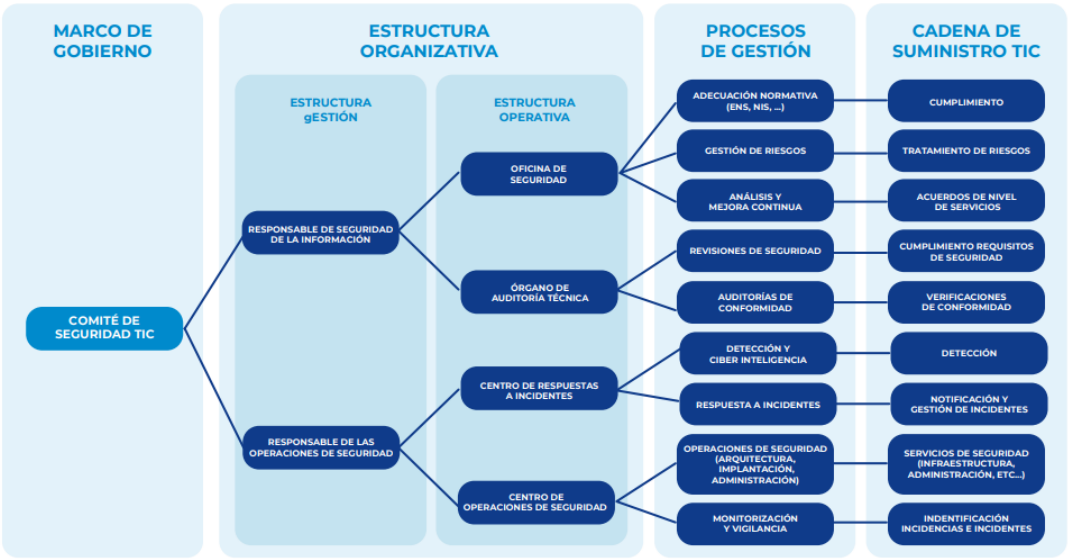

Figura 7.- Modelo extendido de referencia para la gobernanza de la ciberseguridad.

- La primera corresponde al Responsable de Seguridad de la información, que, en este supuesto, dirige:
  - La Oficina de Gobernanza y Cumplimiento Normativo de la Seguridad TIC, con el fin de poner en práctica las directrices del Comité de Seguridad TIC, la normativa de la entidad o la identificación y seguimiento de la mejora continua.
  - La supervisión técnica del cumplimiento, mediante la supervisión de la eficacia de las medidas a través del Órgano de Auditoría Técnica y la Gestión de los incidentes
- La segunda corresponde al Responsable de las Operaciones de Seguridad, que en este supuesto de desarrollo dirige:

- El Centro de Operaciones de Seguridad

Insistir una vez más que este desarrollo se muestra a modo ilustrativo y que cada entidad debe determinar su estructura organizativa, sus funciones, su marco normativo interno, sus procesos, sus actividades y cuantos elementos se hayan identificado en el modelo básico a modo de marco de referencia.

3.8 Política de seguridad del Organismo

La **Política de seguridad** se plasmará en un documento de alto nivel, mediante el cual la universidad definirá su compromiso respecto a la seguridad de los servicios (trámites electrónicos e información que estos gestionan) que proporcionan a la ciudadanía y otras entidades. En ella se describirán los mecanismos que se han implementado para garantizar la gestión continuada de la seguridad, así como los responsables y órganos que se han definido para velar por su cumplimiento. Para su redacción, entre otros se tendrá en cuenta la inclusión de los siguientes contenidos:

- La misión de la universidad.
- El marco legal y regulatorio en el que se desarrollan sus actividades.
- El Modelo de Gobernanza
  - La estructura del Comité de Seguridad TIC y demás órganos que se han constituido para organizar la seguridad y sus funciones.
  - Los roles de seguridad designados, sus funciones, el proceso de designación, así como de renovación, contando al menos con los siguientes:
    - El Responsable de la Información y el Responsable de los Servicios, para aquellos sistemas de información que no sean operados por terceros públicos o privados.
    - El Responsable de Seguridad que será diferente del Responsable del Sistema y no existirá dependencia jerárquica entre ambos.
- Los mecanismos que se han implementado para que los roles de seguridad actúen de forma coordinada y consensuada, así como los mecanismos implementados para la resolución de los conflictos que pudieran surgir entre estos (pudiendo ser el propio Comité de Seguridad TIC).
- El compromiso de la universidad con el cumplimiento de los requisitos mínimos de seguridad de acuerdo a los principios básicos establecidos por el ENS.
- La forma en la cual se va a desarrollar la Política de Seguridad, indicando que está se articulará, mediante el desarrollo de un sistema de gestión de la seguridad de la información documentado y con un proceso regular de aprobación. Así como la periodicidad de la revisión de la política.

- Referencia a la forma en la que la universidad da cumplimiento a la normativa de protección de datos.

En el anexo Política de Seguridad para universidades, se proporciona una definición sencilla de la Política de Seguridad.

4. PLAN DE ADECUACIÓN AL ENS

Para llevar a cabo el proceso de adecuación, será necesario elaborar un **Plan de Adecuación**, que es un documento que contendrá información sobre la identificación del Alcance del Sistema, la Categorización del Sistema, la Declaración de Aplicabilidad Provisional, el Análisis de Riesgos, la Declaración de Aplicabilidad Definitiva- Perfil de Cumplimiento específico validado.

Dado que el objetivo de esta Guía es proporcionar un Perfil de Cumplimiento Específico para Universidades, con un conjunto de medidas que, junto con sus criterios de aplicación, permitirán que estas se adecuen al ENS, únicamente será necesario realizar los siguientes pasos en el Plan de Adecuación:

- **Identificación del Alcance** de los sistemas a certificar**.**
- **Categorizar del Sistema.**
- **Declaración de Aplicabilidad Provisional- Aplicación del Perfil de Cumplimiento Específico.**
- **Análisis de riesgos.**
- **Declaración de aplicabilidad definitiva- Perfil de Cumplimiento Específico Validado.**

Una vez realizado el Plan de Adecuación, se pasará a la fase de Implantación de la Seguridad, mediante la definición del **plan de implantación que contendrá los documentos a elaborar y las medidas técnicas a implementar de forma priorizada.**

4.1 Alcance de los sistemas a certificar

La primera fase del Plan de Adecuación es identificar el **alcance** de los sistemas a certificar. Para ello, es necesario elaborar un catálogo de los servicios prestados (junto con la información que manejan) y el sistema en el que están alojados.

En el Anexo II de esta guía, se proporciona un modelo de catálogo de Servicios e Información, elaborado con la colaboración de los representantes de la CRUE, partiendo de Ley Orgánica 6/2001, de 21 de diciembre, de universidades, donde se recogen las funciones de las universidades.

4.2 Valoración y categorización

La **categoría de un sistema** es el resultado de la **valoración** de las dimensiones de seguridad de los servicios e información alojados en el mismo.

Conforme a las instrucciones del Anexo I del RD ENS y teniendo en cuenta los criterios recogidos en la "Guía CCN-STIC-803 Valoración de Sistemas en el ENS", se determinará el impacto que tendría un incidente de seguridad que afectaría a la información tratada o a los servicios prestados, en cada una de las cinco dimensiones de seguridad Confidencialidad [C], Integridad [I], Trazabilidad [T], Autenticidad [A] y Disponibilidad [D]). Este impacto se mide en tres niveles BAJO, MEDIO O ALTO determinado por los Responsables de Servicios y la Información, que podrán tener en cuenta la opinión del Responsable de Seguridad y/o del Responsable del Sistema.

4.3 Declaración de Aplicabilidad Provisional

En este punto se estaría en condiciones de acogerse al **Perfil de Cumplimiento Específico para Universidades,** siendo entonces de aplicación la Declaración de aplicabilidad asociada a este perfil en concreto. Su adopción deberá estar argumentada formalmente. Se elaborará en base a:

- Identificación de las medidas de seguridad y los refuerzos recogidos en el Perfil de Cumplimiento Específico para Universidades.
- Identificación de las medidas del Perfil de Cumplimiento Específico para Universidades que serán reemplazadas por otras compensatorias que ofrezcan igual o superior protección, justificando su implementación de acuerdo a lo establecido en la Guía "CCN-STIC 819 Medidas compensatorias" CCN-STIC.

La Declaración de Aplicabilidad Provisional, se plasmará en un documento. Para su realización, se puede utilizar el asistente del Plan de Adecuación INES. Además, en el anexo Plan de Adecuación al ENS para universidades, se proporciona un modelo para su elaboración.

4.4 Análisis de riesgos

El **análisis de riesgos** será acorde a lo establecido en el Anexo II del RD ENS. Para su realización se recomienda utilizar la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica -. MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA en http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html. Esta metodología permite estudiar los riesgos que soporta un sistema de información determinando, de este modo, las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Para realizar el análisis de riesgos se puede utilizar la herramienta de referencia PILAR, que implementa la metodología MAGERIT, en cualquiera de sus versiones (PILAR, PILAR Basic, µPILAR). Las Guías CCN-STIC-470 PILAR proporcionan manuales de uso en sus diferentes versiones.

En la realización del análisis de riesgos se reflejará el estado de cumplimiento de las medidas de seguridad, indicando el nivel de madurez de las medidas de la declaración de aplicabilidad.

El informe de riesgos se completará con la aceptación de los riesgos residuales del sistema, que serán aceptados formalmente por los Responsables de los Servicios y por los Responsables de la Información.

4.5 Declaración de Aplicabilidad Definitiva- Perfil de Cumplimiento Específico

El análisis de riesgos validará los criterios de aplicación de las medidas del Perfil de Cumplimiento Específico para Universidades, obteniéndose por tanto de la Declaración de Aplicabilidad Definitiva.

La Declaración de Aplicabilidad Definitiva-Perfil de Cumplimiento Específico se plasmará en un documento que será firmado por el Responsable de la Seguridad.

4.6 Elaboración del Plan de Implantación

Partiendo del Perfil de Cumplimiento Específico se elaborará el mapa normativo y la hoja de ruta con las tareas a realizar y su priorización.

5. IMPLANTANDO MEDIDAS

5.1 Marco organizativo [org]

La primera medida de este grupo es el desarrollo de la **política de seguridad**, que se habrá elaborado en el desarrollo del Marco de Gobernanza.

La **normativa de seguridad** recogerá las directrices respecto al uso correcto de los recursos (equipos, servicios e instalaciones), puestos a disposición del personal. En su redacción se contemplará la inclusión de los siguientes aspectos:

- Alcance: ¿a quién aplica la normativa de seguridad al personal propio, personal de terceros?
- Vigencia: fecha de entrada en vigor.
- Aprobación y revisión: órganos a los que corresponde su aprobación y/o revisión y periodicidad de la misma.
- Regulación del uso correcto de todos los recursos TIC, correo, Internet, soportes de información, impresoras, carpetas de red, etc.
- Qué se considera uso indebido: se debe indicar claramente lo que está permitido y lo que no, en el uso de los recursos TIC.
- Régimen disciplinario: consecuencias en caso de incumplimiento.

Esta norma será aprobada por el órgano superior correspondiente, siendo un aspecto relevante a tener en cuenta la forma en la cual se le va a dar difusión entre el personal, prestando especial atención a que estos la comprendan. El cumplimiento de este control está relacionado también con los siguientes:

- **Deberes y obligaciones,** mediante la normativa se da traslado al personal de sus funciones y obligaciones en materia de seguridad.
- **Concienciación**, una de las materias a tener en cuenta para las actividades de concienciación es trasladar a los usuarios la normativa de seguridad. Por tanto, una de las acciones de concienciación será instruir en su contenido. Estas acciones se pueden completar con la realización de un pequeño cuestionario tras las acciones de concienciación.
- **Mecanismo de autenticación (usuarios de la organización)**, esta medida requiere que el sistema informe al usuario de sus obligaciones inmediatamente después de obtener el acceso. Por tanto, en ese mensaje se puede recordar la existencia de una normativa de seguridad y dónde se puede consultar.

La "Guía CCN-STIC-821 Normas de Seguridad en el ENS y sus apéndices", pueden servir de base para el desarrollo de la normativa de seguridad.

Para la elaboración de los **procedimientos de seguridad,** se tendrá en cuenta que estos describan las tareas habituales que se realizan sobre el sistema, indicando quiénes son los responsables de su ejecución. Estos documentos podrían contener al menos los siguientes apartados:

- Objetivo: qué tareas va a describir el documento.
- Alcance: a qué sistemas y/o personal afecta.
- Desarrollo: descripción de las tareas a realizar.
- Responsabilidades: indicación de quién va a realizar cada tarea. Esto se puede reflejar en este apartado o bien puede ir indicándose en el apartado "desarrollo".
- Comunicación de deficiencias del procedimiento: correo, persona, aplicación donde se deben comunicar las inconsistencias y/o errores que presente el documento, al objeto de que los responsables del mismo procedan a su corrección.
- Otros:
    - Referencias: documentos (guías, informes, etc.) que se han tomado como referencia para la elaboración del procedimiento.
    - Definiciones: que se consideran necesarias para entender el procedimiento.
    - Registros relacionados: evidencias de cumplimiento de lo indicado en el procedimiento.

- Otros: cualquier otro apartado que se considere que proporciona información complementaria al procedimiento.

Igualmente se desarrollarán procedimientos específicos donde se describa cómo se ha de tratar la información (control de acceso, almacenamiento, copias de seguridad, etiquetado de soportes, transmisión telemática, etc.) teniendo en cuenta su nivel de seguridad.

La "Guía CCN-STIC-822 Procedimientos de Seguridad en el ENS" y sus anexos, pueden servir de base para el desarrollo de los procedimientos.

En la definición del **proceso de autorización** se contemplará que la entrada y/o utilización de los diferentes elementos que forman parte del sistema (instalaciones, equipos y/o aplicaciones, establecimiento de enlaces y/o la utilización de medios de comunicación, soportes de información y/o equipos móviles o bien el uso de servicios de terceros), se realiza tras contar con la correspondiente autorización, mediante la definición y documentación de quién o quiénes tienen la capacidad de autorizar el uso o la utilización de cada uno de los mencionados recursos. Implementar este proceso en una herramienta de Help Desk o similar facilita el registro de las evidencias de su realización.

5.2 Marco operacional [op]

El marco operacional se estructura en varios grupos de medidas, las cuales se analizan a continuación.

5.2.1 Planificación [op.pl]

Para el **análisis de riesgos**, que ya se habrá realizado para la elaboración del Plan de Adecuación, se tendrá en cuenta qué deberá ser un *análisis de riesgos semiformal* qué se debe actualizar al menos, anualmente o bien cuando haya cambios relevantes en el sistema.

La definición de la **arquitectura de seguridad** se estructura en dos bloques, por un lado, hay que detallar de forma precisa las instalaciones, equipos, redes, puntos de acceso al sistema, líneas de defensa, etc., esta información se puede reflejar en esquemas de red físicos y lógicos. Por otro lado, hay que disponer de un *sistema de gestión* que recopile toda la documentación que da soporte al cumplimiento del ENS. La organización, estructura, ubicación de esta documentación es conveniente reflejarla en un procedimiento que contenga al menos los siguientes apartados:

- Tipo de documentos: políticas, normativas, procedimientos, instrucciones técnicas, registros, indicadores.
- Organización de la documentación: distribución de la documentación (estructura de carpetas).
- Identificación de la documentación: nomenclatura de los documentos.

- Estructura de la documentación: portada, encabezado, primera página del documento, desarrollo del documento (contenido). Esto deberá estar alineado con lo indicado en Procedimientos de seguridad [org.3].
- Responsables de elaboración, revisión y aprobación de la documentación: teniendo en cuenta las obligaciones establecidas por el Real Decreto ENS.
- Ubicación y difusión de la documentación: lugar donde se almacenará la documentación y como se dará a conocer a las partes afectadas.
- Documentos vigentes y obsoletos: cómo se identificarán los documentos vigentes, donde se almacenarán los obsoletos.
- Registros: donde se almacenarán los registros: ofimática, aplicaciones, etc.

Figura 8: Tipo de documentos

Antes de la **adquisición de nuevos componentes** con carácter previo, se realizará un estudio donde se reflejará que se han tenido en cuenta los resultados del **análisis de riesgos**, y que es acorde a la **arquitectura de seguridad**. También incluirá las necesidades técnicas, de formación y de financiación.

Antes de la puesta en explotación de un nuevo elemento se llevará a cabo un estudio de **dimensionamiento/gestión de capacidades** del sistema para identificar las

necesidades relativas al procesamiento, almacenamiento de información, comunicación, personal, instalaciones y medios auxiliares, dejando constancia de su realización. Siendo necesario realizar una *mejora continua de la gestión de la capacidad*, de tal forma que se mantenga actualizada durante todo el ciclo de vida del sistema, utilizando herramientas y recursos de monitorización de la capacidad.

En la adquisición de productos o servicios de seguridad suministrados por terceros, que vayan a ser utilizados en el sistema de información objeto de la certificación, se emplearán **componentes certificados** del Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN. En caso de que el catálogo no disponga de productos o servicios con las funcionalidades requeridas, se atenderá a lo dispuesto en el artículo 19 del RD.

5.2.2 Control de acceso [op.acc]

La **identificación** de usuarios, entidades o procesos en el sistema se implementará asegurando un identificador singular (cuentas individualizadas) de tal forma que se pueda conocer a quién pertenece, y con qué privilegios se accede y qué acciones realiza. La *identificación avanzada* de los usuarios permitirá al sistema determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos y se mantendrá una lista actualizada de usuarios autorizados para acceder a los diferentes recursos.

Cuando los usuarios dejen la entidad, hayan sido cesados en su función o se les hayan revocado los permisos, se inhabilitarán sus cuentas, manteniendo los registros de actividad asociados durante el periodo de retención que previamente se haya establecido.

Los **requisitos de acceso** a la información se recogerán en una política o normativa que identifique quiénes tienen capacidad de otorgar los accesos a los recursos y la forma de solicitarlos. El **proceso de gestión de derechos de acceso** se realizará en base al cumplimiento principios tales como, “todo acceso está prohibido, salvo autorización expresa”, “mínimo privilegio”, “necesidad de conocer y responsabilidad de compartir” y “capacidad de autorizar”. Los permisos de acceso se revisarán periódicamente y el acceso remoto debe ser previamente autorizado, contando con una normativa específica de uso.

En la definición de la política acceso de los usuarios, se tendrá en cuenta que se debe establecer una **segregación de funciones y tareas**, asegurando la concurrencia de dos o más personas, para aquellas tareas consideradas como críticas y separando, siempre que sea posible, funciones incompatibles, de tal forma que no recaigan en la misma persona tareas de desarrollo y operación y que las personas que autorizan el acceso y las que controlan el uso sean distintas. Si la falta de personal imposibilita la aplicación de esta segregación, la medida podría ser reemplazada por una medida compensatoria, como por ejemplo la activación de registros de actividad de las actuaciones de estos usuarios sobre el sistema de información, registro que solo podrá ser accesible por personal autorizado. Como apoyo a estas actividades pueden emplearse las Guías “CCN-STIC 819 Medidas compensatorias” y “CCN-STIC 831 Registro de la actividad de los usuarios”.

Los **mecanismos de autenticación (usuarios externos[7])** se adecuarán al nivel de seguridad del sistema, pudiendo usarse los siguientes factores de autenticación: *contraseñas*, *contraseña de usuario + contraseña de un solo uso (OTP), Certificados o bien certificados en dispositivo físico*. Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

Antes de proporcionar las credenciales (factores de autenticación) a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre y estarán bajo el control exclusivo del usuario, reconociendo que las ha recibido y que acepta las condiciones que implica su tenencia antes de que se haya activado el mecanismo de autenticación. Se cambiarán con la periodicidad marcada por la política de la universidad y se retirarán e inhabilitarán cuando se termine la relación con el sistema o cuando se detecte que su pérdida o control por parte del usuario. Se establecerá una limitación de intento de accesos que requerirá una intervención específica para reactivar la cuenta. La información suministrada en el acceso será la mínima imprescindible. Una vez otorgado el acceso se informará al usuario de sus obligaciones. Se habilitará el *registro* de los accesos con éxito y fallidos, y se informará al usuario del último acceso realizado con su identidad.

En función de los mecanismos de autenticación usados se tendrá en cuenta lo siguiente:

- *Contraseñas o contraseñas + OTP,* estas dispondrán de una complejidad mínima y no serán fácilmente adivinables. Para su creación se puede tomar como referencia el APÉNDICE V: NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS NP40 de la Guía CCN-STIC 821 Normas de Seguridad en el ENS.
- *Certificados*, las credenciales se obtendrán tras un proceso de registro previo bien sea presencial, telemático, o bien usando certificado electrónico. El uso del certificado estará protegido por un segundo factor (PIN o biométrico).
- *Certificados en dispositivo físico* (tarjeta o similar), las credenciales se obtendrán tras un proceso de registro previo bien sea presencial, telemático, o bien usando certificado electrónico, se usarán al algoritmos, parámetros y dispositivos autorizados por el CCN y su uso estará protegido por un segundo factor (PIN o biométrico).

[7] Según el RD 311/2022 - Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.
Atendiendo a esta definición, en el ámbito del ENS, los estudiantes no se consideran “usuarios de la organización” y deberán tratarse como "usuarios externos".

En cuanto a los **mecanismos de autenticación (usuarios de la organización[8])** del personal propio o contratado estable o circunstancial, que pueda tener acceso a la información contenida en el sistema, se podrá usar los siguientes factores de autenticación: *contraseñas* (cuando el acceso se realiza desde zonas controladas[9], en su defecto será necesario *doble factor para acceso desde o a través de zonas no controladas*), *contraseña + otro factor de autenticación (OTP), Certificados o bien certificados en dispositivo físico.*

Las credenciales estarán bajo el control exclusivo del usuario, reconociendo que las ha recibido y que acepta las condiciones que implica su tenencia antes de que se haya activado el mecanismo de autenticación. Se cambiarán con la periodicidad marcada por la política de la universidad y se retirarán e inhabilitarán cuando se termine la relación con el sistema o cuando se detecte que su pérdida o control por parte del usuario. Se establecerá una limitación de intento de accesos que requerirá una intervención específica para reactivar la cuenta. La información suministrada en el acceso será la mínima imprescindible. Una vez otorgado el acceso se informará al usuario de sus obligaciones. Se habilitará el *registro* de los accesos con éxito y fallidos, y se informará al usuario del último acceso realizado con su identidad.

En cuanto al *acceso remoto (todos los niveles)* será de aplicación la ITS de interconexión de sistemas de información, deberá ser autorizado previamente, el tráfico deberá estar cifrado, se inhabilitará cuando su uso no sea constante y se activarán los registros de auditoría de las conexiones.

5.2.3 Explotación [op.exp]

El **inventario de activos** detallará todos los elementos del sistema indicando su naturaleza e identificando a su responsable. Las herramientas de detección automática de los elementos que se encuentran conectados a la red permitirán mantener actualizado el inventario.

Se definirá y documentará la **configuración de seguridad** (bastionado) mínima de los principales componentes del sistema: equipamiento (seguridad perimetral, electrónica de red, servidores (físicos y virtuales), bases de datos, equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, escáneres, proyectores, etc.), de tal forma que se asegure que antes de que estos elementos entren en operación se les haya aplicado dicha configuración. Para su elaboración es posible apoyarse en los recursos proporcionados por el CCN-CERT: Guías CCN-STIC, Clara, Rocío, etc.

Para la **gestión de la configuración de seguridad** de los componentes del sistema, se tendrá en cuenta que solo puede ser editada por personal autorizado y se realizará en base a los principios de “funcionalidad mínima” y “mínimo privilegio”, adaptándola a las

[8] Según el RD 311/2022 - Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.

[9] Según el RD 311/2022 - Zona controlada: aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

nuevas necesidades y reaccionando a la aparición de vulnerabilidades e incidentes de seguridad. Para el *mantenimiento regular de la configuración* hardware/software de los servidores, elementos de red y estaciones de trabajo existirán configuraciones autorizadas y mantenidas regularmente, verificando periódicamente la configuración del sistema y se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

El personal autorizado para realizar el **mantenimiento** (físico y lógico) y las **actualizaciones de seguridad** del sistema atenderá principalmente a las especificaciones del fabricante y analizará, priorizará y determinará cuándo se deben aplicar las actualizaciones de seguridad o la corrección de defectos. Las *pruebas* se realizarán *preproducción*, en un entorno aislado, que no se encuentre en producción.

Para mantener un control continuo sobre los cambios en el sistema será necesario implantar un proceso de **gestión de cambios**, que permita su registro y seguimiento, que tenga en cuenta que deben ser planificados para reducir el impacto sobre los servicios, que deben contar con la autorización pertinente, que deben contemplar la realización de las pruebas necesarias antes de que se pongan en producción y que debe tener en cuenta la actualización de la documentación de configuración afectada (esquemas de red, bastionados, inventario, etc.).

Todos los equipos (puestos de usuario, servidores, elementos perimetrales), dispondrán de mecanismos de **protección** (y reacción) **frente a código dañino** que se mantendrán siguiendo las recomendaciones del fabricante. Las bases de datos de detección frente a código dañino se mantendrán actualizadas permanentemente y en los puestos de usuario se implementará una protección en tiempo real. Los ficheros procedentes de fuentes externas se analizarán con carácter previo a su uso y se emplearán herramientas que dispongan de *capacidad de respuesta en caso de incidente* de seguridad (EDR -Endpoint Detection and Response).

Se desarrollará un proceso integral para la **gestión de incidentes y registro de la gestión de incidentes de seguridad,** que contemple también las obligaciones impuestas por la normativa de protección de datos. Este proceso incluirá medidas de *detección y respuesta frente a los incidentes*. Para su elaboración se tendrán en cuenta la **"Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad[10]"** y la Guía CCN-STIC 817 Esquema Nacional de Seguridad - Gestión de Ciberincidentes y cuando el incidente afecte a datos de carácter personal lo establecido en el **artículo 33 "Notificación de una violación de la seguridad de los datos personales a la autoridad de control"** del REGLAMENTO (UE)[11]. La utilización de la herramienta LUCIA, como

[10] La Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad aprobada por Resolución de la Secretaría de Estado de Función Pública de de 13 de abril de 2018, establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

[11] 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).

ventanilla única para la *notificación* de incidentes, facilitará notablemente la gestión de los incidentes de seguridad.

Se mantendrá un **registro de la actividad** de los usuarios, mediante el establecimiento de un registro de auditoría que contendrá al menos los siguientes campos: el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito). Se activarán los registros de actividad de los servidores y se definirá un proceso periódico de *revisión de los registros* en busca de patrones anormales. Se documentarán los eventos de seguridad a auditar incluido el tiempo de *retención de* los *registros* y se contará con una referencia de tiempo (timestamp), para la *sincronización del reloj del sistema*. Se establecerá un *control de acceso* a estos registros de auditoría (incluidas las copias) siendo accesible solo a personal autorizado. Como apoyo para el establecimiento de este registro puede utilizarse la Guía "CCN-STIC 831 Registro de actividad de los usuarios".

Se implantarán mecanismos que garanticen la **protección de claves criptográficas** durante todo su ciclo de vida: generación, transporte, custodia, retirada y destrucción, garantizando que los medios de generación están aislados de los de explotación. Se utilizarán *algoritmos* y parámetros *autorizados* por el CCN.

5.2.4 Recursos externos [op.ext]

Con carácter previo a la utilización de recursos externos, ya sean servicios, productos, instalaciones o personal, se definirán los requisitos de seguridad (que se incorporarán en los pliegos y/o peticiones de ofertas) a tener en cuenta en la **contratación y** en la definición de los **acuerdos de nivel de servicio**, con el establecimiento de lo que se considera como "servicio mínimo admisible", la identificación de las responsabilidades de los prestadores y las consecuencias de los incumplimientos.

En la contratación de servicios se solicitará la conformidad con el ENS, en la categoría alcanzada por los sistemas afectados, de acuerdo con lo establecido en la Disposición adicional tercera. Conformidad con el Esquema Nacional de Seguridad de los servicios prestados por terceros pertenecientes al sector privado del Real Decreto ENS y la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad[12], donde se describe la obligación de exigir a los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, la conformidad con el Esquema Nacional de Seguridad.

Para medir el cumplimiento de las obligaciones de servicio se definirá un proceso rutinario de **gestión diaria,** para medir los niveles acordados, que defina también los procedimientos de coordinación necesarios para las tareas de mantenimiento, así como la reacción frente a incidentes y desastres.

En la **interconexión de sistemas**, para el intercambio de información y prestación de servicios, se contará siempre con autorización previa, que irá acompañada de

[12] Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad aprobada por la Secretaría de Estado de Administraciones Públicas de 13 de octubre de 2016.

documentación detallada sobre la interfaz, los requisitos de seguridad y protección de datos, así como la naturaleza de la información cambiada, etc.

5.2.5 Servicios en la nube [op.nub]

Para la **protección de los servicios en la nube** (SaaS[13], PaaS[14], IaaS[15]) suministrados por terceros, estos deben cumplir con las medidas desarrolladas en las Guías CCN-STIC que sean de aplicación, como por ejemplo la Guía CCN-STIC-823 Utilización de servicios en la nube, que incluirá como mínimo los siguientes requisitos: auditoría de pruebas de penetración, transparencia, cifrado y gestión de claves y jurisdicción de los datos. Los *servicios* en la nube deberán estar *certificados* disponiendo de una certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información. Para los servicios de seguridad en la nube además deberán cumplir con los requisitos establecidos en componentes certificados.

5.2.6 Continuidad del servicio [op.cont]

Será necesario determinar los requisitos de disponibilidad de cada servicio, y los elementos críticos para su prestación, mediante la realización de un **análisis de impacto.**

5.2.7 Monitorización del sistema [op.mon]

El sistema contará con herramientas de **detección** o prevención **de intrusión** que dispongan de *detección basada en reglas***.**

Para la recopilación de los datos necesarios para dar respuesta a la encuesta INES (Informe Nacional sobre el Estado de la Seguridad), será necesario definir un **sistema de métricas,** junto con los indicadores asociados, que permita conocer el nivel de madurez de las medidas de seguridad que son de aplicación al sistema, así como la información necesaria para cumplimentar la encuesta, conforme a lo establecido en la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

Será necesario también definir los indicadores y la métrica necesaria para conocer la *efectividad del sistema de gestión de incidentes* de acuerdo a lo establecido en la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y las Guías "CCN-STIC-824 Información del Estado de Seguridad" y "CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes". Así como los necesarios para evaluar la *eficiencia del sistema de gestión de la seguridad*, en relación con los recursos consumidos, en términos de horas y presupuesto.

Para la **vigilancia** del sistema se contará con un sistema automático de recolección de eventos de seguridad, que permita su *correlación*.

[13] SaaS (Software as a Service)- Software como servicio.
[14] PaaS (Platform as a Service)- Plataforma como servicio.
[15] IaaS (Infrastructure as a Service)- Infraestructura como servicio.

5.3 Medidas de protección [mp]

5.3.1 Protección de las instalaciones e infraestructuras [mp.if]

El equipamiento del Centro de Proceso de Datos (CPD) estará protegido mediante su disposición, en la medida de lo posible, en **áreas separadas y con control de acceso**, que permitan la **identificación de las personas** que acceden a las mismas, mediante su registro de entrada y salida. Estos accesos se revisarán a intervalos regulares.

Para el **acondicionamiento de los locales** donde se ubiquen los sistemas de información y sus componentes esenciales, se tendrá en cuenta que estos dispongan de unas condiciones adecuadas de temperatura y humedad, que el cableado se encuentra protegido y que se han implementado las protecciones necesarias, fruto del análisis de riesgos. Se evidenciarán los mantenimientos y revisiones realizadas.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de la **energía eléctrica** necesaria mediante el establecimiento de las suficientes tomas eléctricas y se dotarán del *suministro eléctrico de emergencia* necesario garantizando que, aun fallando el suministro general, se disponga del tiempo suficiente para la terminación ordenada de todos los procesos. Se evidenciarán los mantenimientos y las revisiones realizadas.

La **protección frente a incendios** de los locales donde se ubiquen los sistemas de información y sus componentes esenciales será acorde, como mínimo, a la normativa industrial de aplicación. Se evidenciarán los mantenimientos y revisiones realizadas. Se contará también con **medidas de protección frente a inundaciones**.

Se mantendrá un **registro de entrada y salida de equipamiento** esencial que contemplará la identificación de la persona que autoriza el movimiento.

5.3.2 Gestión del personal [mp.per]

Las responsabilidades en materia de seguridad estarán definidas en la **caracterización del puesto de trabajo,** especialmente las relativas a la confidencialidad. Estas se definirán en base a los riesgos y se tendrán en cuenta para la selección de personal.

Se informará al personal de los **deberes y obligaciones** de su puesto de trabajo, así como las medidas disciplinarias en caso de incumplimiento. Para personal de terceros, estos requisitos se establecerán en los contratos de prestación de servicios.

Se deben realizar acciones de **concienciación** sobre las responsabilidades del personal respecto a la seguridad del sistema, especialmente aquellas relacionadas con la normativa de seguridad, las técnicas de ingeniería social más habituales, la identificación de incidentes de seguridad y la forma de comunicarlos. Se recomienda realizar una planificación por ciclo anual, que identifique las actividades a realizar por el personal por periodos (semestre o cuatrimestre o trimestre…), la frecuencia de distribución de píldoras de concienciación, buenas prácticas, etc.

También se realizarán acciones de **formación** en materia de seguridad de la información, necesarias para el desempeño de las funciones del personal, especialmente relativas a la configuración de sistemas, detección y reacción frente a incidentes y gestión de la información en cualquier tipo de soporte. Se recomienda realizar un Plan de formación, por ciclo anual, que especifique tanto las acciones destinadas al personal de nueva incorporación como aquellas dirigidas a la formación continua; deberá incluir la evaluación de la eficacia de las acciones formativas realizadas.

El Centro Criptológico nacional, a través de la plataforma ÁNGELES, proporciona recursos para formación, capacitación, sensibilización y concienciación en ciberseguridad, mediante ciberconsejos, cursos, informes de buenas prácticas, vídeos, emisiones online, etc.

5.3.3 Protección de los equipos [mp.eq]

Para garantizar la seguridad de la información será necesario que el **puesto de trabajo** permanezca **despejado**, sin más material encima de la mesa que el necesario en cada momento. Será necesario, siempre que se factible, el *almacenamiento del material, una* vez usado, en lugar cerrado. Esta necesidad se trasladará a los usuarios en la normativa de seguridad general.

Los equipos incluirán en su configuración la activación del **bloqueo de puesto de trabajo** para que, transcurrido un tiempo de inactividad, sea requerida una nueva autenticación. Resulta conveniente concienciar a los usuarios en el seguimiento de "Buenas Prácticas" en el uso de los equipos, tales como el bloqueo de forma proactiva de su equipo de trabajo. Todo lo anterior se podrá trasladar al personal mediante su inclusión en la normativa de seguridad general.

Para la **protección de los equipos portátiles** (ordenadores portátiles, tabletas, etc.), que sean susceptibles de salir de las instalaciones de la entidad se mantendrá un inventario actualizado, que registrará también la persona responsable de su custodia. Se establecerán canales de comunicación de pérdida, robo o incidentes de seguridad y en la medida de lo posible estos no contendrán claves de acceso remoto a la universidad, procurándose que cuando se conecten a Internet y otras redes que no sean de confianza, los servicios a los que se acceda sean los mínimos imprescindibles. Se elaborará una normativa específica respecto a su uso y las medidas de seguridad a adoptar, que se podrá incluir en la normativa de seguridad general.

Para **otros dispositivos conectados a la red** (impresoras, escáneres, proyectores, BYOD[16], etc.) se aplicará una configuración de seguridad específica que garantice el control del flujo de la información. En caso de que dispongan de almacenamiento de información, ya sea temporal o permanente, deberán contar con funcionalidades que permitan eliminar de forma segura la información.

[16] BYOD- *Bring Your Own Device*

5.3.4 Protección de las comunicaciones [mp.com]

Se dispondrá un sistema de protección perimetral que establezca un **perímetro seguro** que separe la red interna del exterior. Los flujos de información deberán contar con la autorización correspondiente. La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Para la **protección de la confidencialidad** cuando la comunicación discurra por redes fuera del propio dominio de seguridad, se emplearán redes privadas virtuales (VPN) cifradas y *algoritmos y parámetros autorizados* por el CCN.

Para la **protección de la integridad y de la autenticidad** en las comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información y se prevendrán ataques activos (alteraciones de información, inyección de información espuria o secuestros de sesión) garantizando que si son detectados se activarán los procedimientos de gestión del incidente. En cuanto a los mecanismos de identificación y autenticación se atenderá a los previstos en el ordenamiento jurídico en normativa de aplicación. Se emplearán *redes privadas virtuales* (VPN) cifradas y *algoritmos y parámetros autorizados* por el CCN.

Para el control de acceso a la información y la mitigación de los efectos de propagación de los incidentes de seguridad será necesario llevar a cabo una **separación de flujos de información en la red** de tal forma que cada equipo solamente tenga acceso a la información que necesita y en caso de utilizar comunicaciones inalámbricas, estas se dispondrán en un segmento separado. Se podrá implementar cualquiera de las siguientes opciones:

- *Segmentación lógica básica*: empleando redes de área locales virtuales (Virtual Local Area Network VLAN) segregando las siguientes subredes: usuarios, servicios y administración.
- *Segmentación lógica avanzada:* empleando redes privadas virtuales (Virtual Private Network VPN).
- *Segmentación física*: empleando medios físicos separados.

5.3.5 Protección de los soportes de información [mp.si]

El **marcado de soportes** de información (papel impreso, documentos electrónicos, contenidos multimedia - vídeos, cursos, presentaciones, etc.) y las medidas de seguridad a aplicar sobre los mismos, se establecerán conforme a la calificación de información que contienen, siendo necesario que estos lleven las marcas o metadatos correspondientes al nivel de seguridad de la información de mayor calificación.

Para proteger la información en dispositivos removibles (CD, DVD, discos extraíbles, pendrives, memorias USB, u otros de naturaleza análoga), cuando salgan de las áreas controladas, se aplicará **criptografía,** garantizando de este modo la confidencialidad e

integridad de la información contenida en los mismos. Siendo necesario el uso de algoritmos y parámetros autorizados por el CCN. Las *copias de seguridad* se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

La **custodia** de este tipo de dispositivos se garantizará mediante la implementación de medidas de control de acceso físico y/o lógico, respetándose las indicaciones respecto a temperatura, humedad y otros agentes medioambientales, establecidas por los fabricantes.

Se implementará un registro de entrada y salida de soportes que identifique al transportista que realiza el **transporte**, con indicación de las personas que lo reciben y entregan y un procedimiento para cotejar salidas con llegadas. Si la información contenida en el soporte está clasificada con un nivel que aconseje su cifrado, se aplicará esta medida para proteger la información durante el transporte.

Se implementarán y documentarán los métodos de **borrado y destrucción** a aplicar en función del dispositivo, garantizando que los soportes que vayan a ser reutilizados o liberados a otra organización sean objeto de un borrado seguro, empleando productos certificados, y cuando este no sea posible, no sea utilizado en ningún otro sistema. Se utilizarán *productos* o servicios *certificados*.

5.3.6 Protección de las aplicaciones informáticas [mp.sw]

En el caso de que se desarrolle software se deberá aplicar y documentar una metodología de **desarrollo de aplicaciones** que garantice que estas se llevan a cabo en un sistema independiente, separado del de producción. Se seguirá una *metodología de desarrollo seguro* que tenga en cuenta los principios de *mínimo privilegio* y *seguridad desde el diseño*, regulando el uso de los *datos* reales *de* las *pruebas*.

Antes de pasar a producción las aplicaciones se diseñará un plan de **aceptación y puesta en servicio** que contemple su correcto funcionamiento y que verifique que se cumplen los criterios de seguridad que se hayan establecido y que no se ha comprometido la seguridad de otros componentes del servicio. Para aplicaciones que gestionen servicios corporativos las *pruebas* se realizará en un entorno aislado (pre-producción).

5.3.7 Protección de la información [mp.info]

Cuando el sistema trate **datos de carácter personal**, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y en l Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el ENS. El Responsable de Seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, que con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos

24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Se implementará y documentará un proceso de **calificación de la información**, que tenga en cuenta que esta se realizará según lo establecido legalmente sobre la naturaleza de la misma, se utilizará "USO OFICIAL" para información con algún tipo de restricción ya sea en su manejo, sensibilidad y confidencialidad.

En cuanto a la **firma electrónica,** se emplearán los tipos previstos en el ordenamiento jurídico. Se emplearán sistemas de firma electrónica avanzada basados en *certificados cualificados*, empleando *algoritmos y parámetros autorizados* por el CCN o por un esquema nacional o europeo. Se garantizará la *verificación y validación de la firma* electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período, de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin, se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Los **sellos de tiempo** se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro, empleándose "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) nº 910/2014 y normativa de desarrollo. Los datos necesarios para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad. Los sellos de tiempo se renovarán regularmente hasta que no sea necesario para el procedimiento administrativo al que da soporte.

Cuando los documentos vayan a ser difundidos ampliamente ya sea directamente o a través de su publicación en sitios web o sedes electrónicas, se definirá y documentará un proceso de **limpieza de documentos**, de tal forma que se garantice que con carácter previo a su difusión se ha eliminado toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores.

Se implementarán políticas de **copias de seguridad** que garanticen la recuperación de la información ante un incidente de seguridad, definiéndose su periodicidad y plazos de retención. Se realizarán y planificarán *pruebas* periódicas de *recuperación*.

5.3.8 Protección de servicios [mp.s]

Para garantizar la **protección del correo electrónico**, se implementarán medidas que lo protejan de las amenazas propias de este medio, protegiendo la información tanto en el cuerpo de los mensajes como en los anexos. Se dispondrán de mecanismos de protección frente al spam, programas dañinos y código móvil. La normativa de seguridad regulará el uso del correo electrónico, definiendo lo que se considera un uso no autorizado del mismo. Se contemplarán actividades de concienciación y formación sobre el uso seguro del correo electrónico.

Se implementarán medidas que garanticen la **protección de servicios y aplicaciones web** frente a la materialización de amenazas propias, que impidan el acceso a la

información por vías alternativa obviando la autenticación, frente a los intentos de escalado de privilegios, y frente a los ataques de cross site scripting. Además, sobre las aplicaciones web se realizarán de forma periódica *auditorías de seguridad* de "caja negra" en las fases de desarrollo y antes de la fase de producción o bien *auditorías de seguridad avanzada* de "caja blanca" durante su fase de desarrollo, empleando metodologías definidas y herramientas automáticas de detección de vulnerabilidades. Los resultados de la auditoría serán analizados resolviéndose las vulnerabilidades detectadas.

Para la **protección de la navegación web** de los usuarios internos de las amenazas propias de este medio se implementarán medidas tales como el establecimiento de una normativa de uso (que se puede incluir en la normativa de seguridad), se realizarán acciones de concienciación sobre los riesgos de este medio, se formará al personal con responsabilidad en la administración del sistema sobre la monitorización de la navegación y respuesta a incidentes, etc.

Como medida de **protección frente a la denegación de servicio**, el sistema se planificará y dotará de la capacidad suficiente para asumir la carga prevista con holgura y se desplegarán tecnologías para prevenir los ataques conocidos.

6. HERRAMIENTAS PARA LA GOBERNANZA DE LA CIBERSEGURIDAD

Para la gobernanza de la ciberseguridad, en consonancia con lo establecido en el artículo 10 Vigilancia continua y reevaluación periódica del RD ENS, *"Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.",* desde el Centro Criptológico Nacional, se proporcionan las herramientas de gobernanza INES y AMPARO que garantizan la gestión de la ciberseguridad.

TAREAS	DESCRIPCIÓN	HERRAMIENTA
Elaboración del Plan de Adecuación y actualización	Alcance del Sistema, Categorización del Sistema, Declaración de Aplicabilidad Provisional, Análisis de Riesgos, Declaración de Aplicabilidad Definitiva- Perfil de Cumplimiento específico validado	INES
Elaboración del plan de implantación, seguimiento periódico y ajustes del plan	Elaboración de hoja de ruta detallada para la implantación de las medidas de seguridad.	INES-AMPARO
Revisión de la Información y los Servicios, su valoración y proceso de categorización del sistema	Los Responsables de la Información y los Responsables de los Servicios comunicarán al Responsable de Seguridad la aparición de nuevos activos de Servicios o Información, o cambios que pudieran afectar a la valoración de los mismos. Esto derivará en la revisión de la categorización del sistema.	INES

TAREAS	DESCRIPCIÓN	HERRAMIENTA
Elaboración y Revisión de la Política de seguridad	El comité de seguridad, con la periodicidad que se haya indicado en la propia política (normalmente con carácter anual), revisará la Política de Seguridad prestando especial atención a la aparición, durante ese periodo, de nuevas normas, legislación, instrucciones técnicas, que introduzcan cambios en las obligaciones en materia de seguridad.	INES
Elaboración del Plan de Concienciación y Plan de Formación anual	Con carácter anual se diseñarán las acciones de concienciación, para todo el personal, y las de formación, para el personal con responsabilidad en la operación sobre el sistema.	INES-AMPARO
Elaboración y Revisión de la Normativa de seguridad	El comité de seguridad revisará, al menos con carácter anual, la normativa de seguridad, con objeto de identificar si se encuentran regulados todos los recursos TIC puestos a disposición de los usuarios, si las normas son eficaces y si se han derivado medidas disciplinarias.	INES-AMPARO
Actualización del análisis de riesgos	Con carácter anual, se revisará el análisis de riesgos y se aprobarán formalmente los riesgos residuales por parte de los Responsables de la Información y los Responsables de los Servicios. Los cambios relevantes sobre el sistema (cortafuegos, cabinas, servidores, etc.) que introduzcan componentes con nuevas tecnologías, requerirán también de una actualización del análisis de riesgos.	PILAR
Revisión de la Declaración de aplicabilidad o del Perfil de Cumplimiento Específico	El Responsable de seguridad revisará los cambios derivados de la actualización de la categorización del sistema, del análisis de riesgos, o bien del Perfil de Cumplimiento Específico, y procederá revisar la declaración de aplicabilidad	INES
Realización de auditorías y chequeos internos	Es conveniente establecer chequeos periódicos de cumplimiento de: • **Revisar las medidas de seguridad:** verificar si las medidas de seguridad están correctamente implantadas y si son eficaces. • **Revisar los procedimientos:** verificar si los procedimientos reflejan correctamente las tareas existentes y la forma de llevarlas a cabo. • **Revisión del plan de implantación:** el comité de seguridad revisará si se están cumpliendo los hitos marcados, reprogramándolos en caso de que sea necesario y añadiendo aquellos que hayan surgido de la realización de las auditorías internas. • **Informe de estado de cumplimiento.**	AMPARO
Revisión del Estado de la Seguridad. INES	Asegurar, mediante la designación de responsables, que la encuesta se cumplimenta anualmente.	INES
Auditorías de conformidad con el ENS	Con carácter bienal se procederá a realizar auditorías de conformidad con el ENS.	AMPARO

7. ANEXOS

La Guía se complementa con los siguientes documentos:

7.1 Política de Seguridad para Universidades

7.2 Plan de Adecuación al ENS Universidades

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL