I. DISPOSICIONES GENERALES

I.5. Secretario General

Política de Seguridad de la Información de la Universidad de Sevilla (Aprobada mediante Acuerdo del Consejo de Gobierno de 26 de febrero de 2014 y modificada por resoluciones rectorales de 16 de enero de 2017; 9 de febrero de 2019 y 26 de octubre de 2023 - Texto consolidado).

ÍNDICE

1. Introducción.

La Universidad de Sevilla depende de los sistemas TIC (Tecnologías de la Información y las Comunicaciones) 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 Sevilla, 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.

1.1. Prevención.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de Sevilla 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 Sevilla:

- 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.

1.2. Detección.

La Universidad de Sevilla 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.

1.3. Respuesta.

La Universidad de Sevilla 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).

1.4. Recuperación.

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

2. Misión de la Universidad de Sevilla.

La Universidad de Sevilla tiene una misión bien definida que se fundamenta en su Estatuto. En el título preliminar, Artículo 1 se encuentran los elementos definitorios de la misión de la Universidad:

La Universidad de Sevilla es una institución de Derecho público, dotada de personalidad jurídica, que desarrolla sus funciones, de acuerdo con la legislación vigente, en régimen de autonomía, y a la que corresponde la prestación del servicio público de educación superior, mediante el estudio, la docencia y la investigación, así como la generación, desarrollo y difusión del conocimiento al servicio de la sociedad y de la ciudadanía.

Para cumplir con su misión la Universidad de Sevilla 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 se persigue fomentar la relación electrónica todos los actores (docentes, estudiantes, investigadores, personal de administración y servicios, y otros) con la universidad.

3. Principios básicos.

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

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, 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.

4. Objetivos de la Seguridad de la Información.

La Universidad de Sevilla 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.

5. Alcance.

Esta Política se aplicará a los sistemas de información de la Universidad de Sevilla 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 de la Comisión de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

En este ámbito, no se consideran recursos TI de la Universidad aquellos ordenadores personales financiados a título individual no inventariados por la universidad, aunque pudieran ocasionalmente ser usados para labores propias de investigación. No obstante, en el caso de que se acceda a la red corporativa mediante dichos ordenadores personales, quedarán sujetos a las obligaciones establecidas en la presente política de seguridad de la información y normativas de desarrollo.

6. Marco normativo.

El marco normativo de seguridad que afecta al desarrollo de las actividades y competencias de la Universidad de Sevilla está constituido por normas jurídicas de ámbito europeo, estatal, autonómico y universitario orientadas a la administración electrónica, la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco se encuentran recogidas en un registro al efecto que se mantiene actualizado en https://www.us.es/laUS/secretaria-general/normativas y en https://osi.us.es/marco-legal-aplicable.

También forman parte del marco legal aplicable las restantes normas aplicables a la Administración Electrónica de la Universidad de Sevilla derivadas de las anteriores y publicadas en la sede electrónica comprendidas dentro del ámbito de aplicación de la Política de Seguridad de la información de la Universidad de Sevilla, así como otras normas que en la actualidad o en el futuro, de carácter general o interno, resulten de aplicación a la Universidad.

7. Organización de la seguridad.

7.1. Criterios utilizados para la organización.

La Universidad de Sevilla, 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, emprende las siguientes acciones:

i. Designa roles de seguridad: Responsable del Servicio, Responsable de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.

ii. Constituye 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 denomina "Comisión de Seguridad de la Información". Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2. Roles y Órganos de la Seguridad de la Información.

Para garantizar que todas las etapas del ciclo de vida de protección de la información sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, la US establece una estructura que permite promover la aplicación consistente de la presente política y acomodar efectivamente los frecuentes cambios tecnológicos y organizacionales.

Para ello, se definen los siguientes Comités y Roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información:

- Comisión de Seguridad de la Información.
- Responsable de la Información.
- Responsable del Servicio.
- Responsable de la Seguridad de la Información.
- Responsable del Sistema.

En la Universidad de Sevilla en el marco del ENS, el órgano de la Seguridad de la Información, será la Comisión de Seguridad de la Información compuesta por los miembros permanentes:

- El máximo responsable con competencias en materia de TI, como presidente de la misma.
- El Director de RRHH (como máximo responsable de los Recursos Humanos).
- El Secretario General (como Responsable de la Información).
- El Gerente (como Responsable del Servicio).
- El Director del Gabinete Jurídico (como máximo responsable de los Servicios Jurídicos de la US).
- El Responsable de la Seguridad de la Información (que actuará como Secretario).
- El Delegado de Protección de Datos de la US.
- El Director de Secretariado con competencias en materia TI (como Responsable del Sistema).

Miembros no permanentes: la Comisión de Seguridad de la Información 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 (Directores de Área o Jefes de Servicio) podrán ser convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de la misma.

El Secretario/a de la Comisión de Seguridad realizará las convocatorias y levantará actas de las reuniones de la Comisión de Seguridad. A las sesiones de la Comisión de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinente su Presidente.

7.3. Responsabilidades de los roles asociados al ENS.

7.3.1. Responsable de la Información y del Servicio.

Serán funciones del Responsable de la Información y del Servicio:

- 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 de la Información 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 Responsable de Seguridad de la Información dará traslado de dichos cambios a la Comisión de Seguridad de la Información en su próxima reunión.

7.3.2. Responsable de la Seguridad de la Información.

Serán funciones del Responsable de Seguridad de la información:

- 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 Comisión de Seguridad de la información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- 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 de la Comisión de Seguridad de la Información, y poner en conocimiento de ésta las modificaciones que se hayan realizado a lo largo del periodo en curso.

7.3.3. 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 Comisión de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso, en los planes de continuidad.
- 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.

7.4. Delegado de Protección de Datos.

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a la Universidad de Sevilla 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 Sevilla 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 Autoridad de Control correspondiente en materia 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:
  - º Recabar información para determinar las actividades de tratamiento.
  - º Analizar y comprobar la conformidad de las actividades de tratamiento.
  - º Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
  - º Recabar información para supervisar el registro de las operaciones de tratamiento.
  - º Asesorar en el principio de la protección de datos por diseño y por defecto.
  - º Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
  - º Priorizar actividades en base a los riesgos.
  - º Asesorar al Responsable de Tratamiento sobre áreas a someter a auditorías de cumplimiento normativo, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.
  - º 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, en colaboración con la Oficina de Seguridad de la Información.

7.5. Comisión de Seguridad de la Información.

Serán funciones de la Comisión de Seguridad de la Información:

- 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.
- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
- 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.
- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones de la Comisión, a las que su presidente, deberá dar cumplida respuesta.
- 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.
- Atender las inquietudes, en materia de Seguridad de la Información, de la Universidad y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
- 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.

- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
- Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
- 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:

- Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el avance del mismo y posibilitar su adecuado seguimiento, la Comisión de Seguridad de la Información se reunirá, al menos, una vez al trimestre.
- Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados por la universidad, la Comisión de Seguridad de la Información se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
- En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.
- Las decisiones se adoptarán por consenso de los miembros permanentes.

7.6. Oficina de Seguridad de la Información.

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la Oficina de Seguridad Información, 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 Información, nombrado por la Comisión de Seguridad de la Información, que actuará como enlace con la mismo, que será el Responsable de Seguridad de la Información (RSEG), o la persona en quien delegue.
- Secretario de la Oficina de Seguridad Información nombrado por la Comisión de Seguridad de la Información, a propuesta de los miembros de la Oficina de Seguridad.
- Todos aquellos administradores especialistas de seguridad (AES) que el Responsable de Seguridad de la Información determine que sean necesarios.

Las funciones de la Oficina de Seguridad Información serán, entre otras que les puedan ser encomendadas por la Comisión de Seguridad de la Información:

- 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.
- Redacción y presentación de propuestas a la Comisión de Seguridad de la información. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
- Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - º Elaborar y revisar regularmente la Política de Seguridad de la Información para su traslado a la Comisión de Seguridad de la Información para su revisión y posterior aprobación del órgano superior.

- Elaborar la normativa de Seguridad de la Información para su aprobación por el Responsable de Seguridad, con conocimiento de la Comisión de Seguridad.
- 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, en colaboración el Delegado de Protección de Datos.

Periodicidad de las reuniones y adopción de acuerdos:

- El Director de la Oficina de Seguridad Información convocará las reuniones de trabajo de sus miembros y recabará los acuerdos alcanzados, de los que dará cuenta a la Comisión de Seguridad de la Información, para su aprobación, en su caso.
- 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 de la Comisión de Seguridad de la Información.
- Se reunirá, al menos, una vez al mes y siempre antes de las celebraciones de la Comisión de Seguridad de la Información.

7.7. Centro de Operaciones de Ciberseguridad.

Bajo la responsabilidad y dirección del Director de la Oficina de Seguridad Información de la US, 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 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/parcheado) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

El Servicio de Informática y Comunicaciones deberá 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 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.

7.8. 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-TIC, 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 de la Comisión de Seguridad de la información.

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

7.9. Procedimiento de designación.

La creación de la Comisión de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por parte del Rector de la Universidad de Sevilla.

Los nombramientos se revisarán cada 4 años o cuando el puesto quede vacante.

El desempeño de cualquiera de las responsabilidades definidas en esta política de seguridad y en el ENS vendrá determinado por el acceso a los diferentes cargos o destinos, estatutarios o no, que han quedado vinculadas a ellas.

En el caso de que desapareciese o cambiara de denominación de alguno de los puestos vinculados a la aplicación del ENS, será competencia del Rector asignar el nuevo puesto al que quedará vinculada la figura.

8. Datos personales.

La Universidad de Sevilla solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan

obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

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

9. Obligaciones del personal.

Todo el personal de la Universidad de Sevilla 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.

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

Todo el personal de la US debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.

10. Gestión de los 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 de la Comisión de Seguridad de la Información.

La Comisión 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.
- Selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos, estar justificadas y ser validadas por la Comisión de Seguridad de la Información.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo, elaboradas por el Centro Criptológico Nacional.

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

11. Notificación de incidentes.

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la Universidad de Sevilla 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 del RD del ENS.

12. Desarrollo de la Política de Seguridad.

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 a la Comisión 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:

- 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.
- Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.
- 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 Consejo de Gobierno de la Universidad de Sevilla la aprobación de la Política de Seguridad de la Información, y siendo la Comisión de Seguridad de la Información el órgano responsable de su revisión, que se aprobará por resolución rectoral, y de la aprobación la Normativa Interna del Uso de los Medios Electrónicos de la Universidad y de los restantes documentos, y 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 Sevilla 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 o en soporte papel y será custodiada por el Servicio de Informática y Comunicaciones.

13. Terceras partes.

Cuando la Universidad de Sevilla 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 Sevilla 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 ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros 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.

14. Mejora continua.

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

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

Apéndice I. Lenguaje de género.

Las referencias a personas o colectivos figuran en la presente política en género masculino como género gramatical no marcado. Cuando proceda, será válida la cita de los preceptos correspondientes en género femenino.

Apéndice II. Glosario.

Análisis de riesgos.

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal.

Cualquier información concerniente a personas físicas identificadas o identificables.

ENS.

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

Gestión de incidentes.

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos.

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad.

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Información.

Caso concreto de un cierto tipo de información. Activo esencial de la universidad.

LOPD.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Política de seguridad.

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Principios básicos de seguridad.

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la Información.

Rol que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la Seguridad de la Información.

El Responsable de la Seguridad de la información determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del Servicio.

Rol que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema.

Persona que se encarga de la explotación del sistema de información.

RGPD.

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.

Servicio.

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de Información.

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

***