UNIVERSIDAD DE EXTREMADURA

RESOLUCIÓN de 31 de mayo de 2023, del Rector, por la que se ejecuta el acuerdo adoptado por el Consejo de Gobierno por el que se aprueba la Normativa Reguladora de Política de Seguridad de la Información. (2023062209)

En cumplimiento con lo establecido en el artículo 93 de los Estatutos de la Universidad de Extremadura, aprobados por Decreto 65/2003, de 8 de mayo (DOE de 23 de mayo de 2003), y en virtud de lo previsto en el artículo 15.j) del Reglamento de funcionamiento del Consejo de Gobierno, se ejecuta el acuerdo adoptado por el Consejo de Gobierno en sesión de 25 de mayo de 2023, por el que se aprueba la Normativa Reguladora de Política de Seguridad de la Información de la Universidad de Extremadura. A tal efecto,

RESUELVO:

Ordenar la publicación en el Diario Oficial de Extremadura del Acuerdo del Consejo de Gobierno de la Universidad de Extremadura de 25 de mayo de 2023, por el que se aprueba la Normativa Reguladora de Política de Seguridad de la Información de la Universidad de Extremadura, que se recoge como anexo a la presente resolución.

Contra la presente resolución, que es definitiva, cabe interponer recurso contencioso-administrativo ante el Juzgado de lo Contencioso-administrativo competente, en el plazo de dos meses a contar desde el día siguiente al de la notificación, de conformidad con lo dispuesto en los artículos 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, y en concordancia con las previsiones de Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario, sin perjuicio de cualquier otro eventual recurso o reclamación que a su derecho conviniere.

Badajoz, 31 de mayo de 2023.

El Rector,

PEDRO M. FERNÁNDEZ SALGUERO

ANEXO

NORMATIVA REGULADORA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Aprobación y entrada en vigor.

Texto aprobado el día 25 de mayo de 2023 por el Consejo de Gobierno de la Universidad de Extremadura.

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

2. Introducción.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información.

Es por ello que el Real Decreto 3/2010, de 8 de enero, por el que se regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS), y modificado por el Real Decreto 951/2015, de 23 de octubre, ha sido sustituido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad para cumplir con las exigencias de mantenerse actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo. En su artículo 12, el ENS establece que "Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente".

Así pues, la Política de Seguridad de la Información de la Universidad de Extremadura (en adelante UEx) se elabora en cumplimiento de las siguientes exigencias legales:

— Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que en su Capítulo III establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

— Otras referencias legales y normativas incluidas en el apartado Marco normativo (ver sección 0).

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-881 del Centro Criptológico Nacional, que define las pautas para la adecuación al ENS para las universidades, de mayo de 2022 y está elaborada siguiendo su Anexo I Política de Seguridad de Universidades.

La UEx depende de los sistemas TIC (Tecnologías de Información y 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 se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

La UEx debe cerciorarse de que la seguridad de la información 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 UEx, el objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

2.1. Prevención.

La UEx debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las

medidas mínimas de seguridad determinadas por el ENS y la LOPDGDD así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la UEx deberá:

— Autorizar los sistemas antes de entrar en operación.

— Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

— Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

2.3. Respuesta.

La UEx 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 Servicios Universitarios 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 (Computer Emergency Response Team, CERT).

2.4. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, los Servicios Universitarios de la UEx debe desarrollar planes de contingencia de los sistemas TIC que garanticen la recuperación de los servicios más críticos.

3. Misión de la Universidad de Extremadura.

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

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

4. Principios básicos.

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

— Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

— Responsabilidad determinada: En los sistemas TIC se determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

— Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

— Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

— Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

— Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. 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 y, atendiendo a las recomendaciones del CCN-CERT, tendiendo a "Confianza Cero en seguridad" (Zero Trust).

5. Objetivos de la seguridad de la información.

La UEx define la presente Política de Seguridad de la Información, de carácter obligatorio para toda la comunidad universitaria y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve a la UEx para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad).

Bajo estas premisas los objetivos específicos de la Seguridad de la Información en la UEx son los siguientes:

— Garantizar la calidad y protección de la información, en las distintas dimensiones antes descritas.

— Lograr la plena concienciación de todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro 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 a las necesidades de nivel de servicio de sus usuarios.

— Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.

— Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

6. Alcance.

El alcance de esta Política incluye a todos los miembros de la comunidad universitaria y a los organismos o empresas colaboradoras. La política de seguridad es aplicable a todos los

sistemas de información de la UEx y a aquellos que den soporte a sus procesos y afecta a todos los activos de información sustentados en ellos, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

En este ámbito no se considera un "recurso TI de la Universidad" aquellos ordenadores personales financiados a título individual, no inventariados a nombre de la UEx, aunque pudieran ocasionalmente ser usados para labores propias de investigación. Por tanto, quedan fuera de este ámbito dichos elementos, así como las acciones sobre ellos o riesgos de seguridad de tales elementos. 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 normas e instrucciones de desarrollo.

La Política de Seguridad se aplica también a todas aquellas personas, instituciones, entidades o unidades y servicios, sean internos o externos, que hagan uso de los recursos de TI de la UEx, sea mediante conexión directa o indirecta con los mismos, conexión remota o a través de equipos ajenos a la misma, incluyendo expresamente sus servicios web. En adelante se considerará a todos ellos "usuarios".

Todos los usuarios tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue al personal afectado.

7. Marco normativo.

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

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

— Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

— Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

— Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

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

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

— Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

— Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

— Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

— Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

— Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

— Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

— Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

— Reglamento de actuación y funcionamiento del sector público por medios electrónicos (Real Decreto 203/2021, de 30 de marzo) que obliga a la actualización permanente del marco de ciberseguridad pública.

— También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la UEx, derivadas de las anteriores y dentro del ámbito de aplicación de la presente Política.

Puede consultarse más normativa de interés en la zona "Normativas" de la sección de la web de la UEx dedicada a la Secretaría General:

http://www.unex.es/organizacion/gobierno/sec_gral/normativas

8. Organización de la Seguridad de la Información.

8.1. Criterios utilizados para la organización de la Seguridad de la Información: roles y órganos.

La UEx, 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", establece los siguientes roles y órganos de la seguridad de la información:

Comité de Seguridad (COMSEG).

— Responsable de la Información.

— Responsable del Servicio.

— Responsable de la Seguridad de la Información (RSEG).

— Responsable del Sistema (RSIS).

— Oficina de seguridad y Centro de Operaciones de Ciberseguridad (COCS).

— Delegado de Protección de Datos.

8.2. Responsabilidades de los roles asociados al Esquema Nacional de Seguridad.

8.2.0. Comité de seguridad: Funciones y Responsabilidades.

El Comité de Seguridad de la Información es el órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información en la UEx. Este órgano colegiado estará formado por:

1. Presidencia: Rector o persona en quien delegue.

2. Miembros permanentes.

a) Responsable de la Información: Secretario general de la universidad o persona en quien delegue.

b) Responsable del Servicio: Gerente o persona en quien delegue.

c) Responsable de la Seguridad: A nombrar por el Rector, como cargo competente en materia de Seguridad de la Información en el ámbito del ENS, que actuará como secretario/a.

d) Responsable del Sistema. Director del Servicio de Informática y Comunicaciones (SICUE).

e) Asesor de Sistemas y Comunicaciones: Subdirector de Seguridad, Sistemas y Comunicaciones del SICUE.

f) Delegado de Protección de Datos.

3. Miembros no permanentes.

El Comité de Seguridad podrá convocar la presencia en sus reuniones de los asesores que considere oportunos para los temas a tratar, tanto internos como especialistas externos que, por razón de su experiencia o vinculación con los asuntos a tratar, sean necesaria su asistencia. Estos asesores participarán con voz, pero sin voto.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

De acuerdo con el ENS, el Comité de Seguridad tendrá las siguientes funciones:

Elaborar y revisar periódicamente la Política de Seguridad de la Información para que sea aprobada por el Consejo de Gobierno.

— Informar periódicamente del estado de la seguridad de la información a los Órganos de Gobierno de la UEx.

— Identificar, revisar y proponer objetivos estratégicos en materia de seguridad de la información.

— Proponer al Consejo de Dirección y al Consejo de Gobierno la aprobación de los reglamentos y normativas generales relacionadas con la aplicación del ENS.

— Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

— Monitorizar los principales riesgos residuales asumidos por la UEx y recomendar posibles actuaciones respecto de ellos.

— Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

— Proponer las iniciativas principales para mejorar la gestión de la seguridad de la información, incluyendo la divulgación de la política y normativas de seguridad.

— Coordinar la adopción de acciones y medidas encaminadas a la adaptación de la UEx al Esquema Nacional de Seguridad.

— Aprobar planes de mejora de la seguridad de la información de la UEx. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

— Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

— Asegurar la disponibilidad de los recursos necesarios para llevar a cabo los planes de acción relacionados con la seguridad de la información o priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

— Aprobación de los procedimientos de seguridad de la UEx cuando así lo solicite el Responsable de Seguridad.

— Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.

— Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la UEx en materia de seguridad

— Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:

  • Grado de cumplimiento del plan de adecuación.

  • Revisión de los resultados obtenidos en las diferentes actualizaciones del análisis de riesgos y los niveles de riesgo alcanzados.

  • Resultados de las auditorías bienales que se realicen y otros informes asociados a la idoneidad de los controles de seguridad implantados, identificando las causas origen de las excepciones que pudieran existir y proponiendo acciones de mejora.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- Elaborar y revisar periódicamente la Normativa de Uso de Medios electrónicos para todo el personal de la UEx para que sea aprobada por el Consejo de Gobierno.

- Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.

El Secretario/a del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su presidente.

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 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 se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

3. En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.

4. Las decisiones se adoptarán por consenso de los miembros permanentes.

8.2.1. Responsables de la Información y los Servicios.

El Responsable de la Información es el Secretario General de la universidad. El responsable de los Servicios es el gerente de la Universidad. Serán funciones de los Responsables de la Información y de los Servicios:

— Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.

— Dictaminar respecto a los derechos de acceso a la información y los servicios.

— Aceptar los niveles de riesgo residual que afectan a la información y los servicios.

— Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

8.2.2. Responsable de la Seguridad.

Serán funciones del Responsable de Seguridad:

Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.

— Promover la formación y concienciación en materia de seguridad de la información.

— Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.

— Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.

— Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.

— Gestionar las revisiones externas o internas del sistema.

— Gestionar los procesos de certificación.

— Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

— Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

8.2.3. Responsable del Sistema.

La figura del Responsable del Sistema recae en la figura del Director del Servicio de Informática y Comunicaciones.

De acuerdo a las propuestas del ENS, serán funciones del Responsable del Sistema:

Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.

— Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

— Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

— Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

— Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.

— Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

— Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

8.2.4. Delegado de Protección de Datos.

De acuerdo con RGPD (Sección 4) y LOPDGDD (Capítulo III), serán funciones, entre otras, del Delegado de Protección de Datos:

— Informar y asesorar a la UEx, 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 UEx, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

— Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.

— Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.

— El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

En el desempeño de sus tareas el Delegado de Protección de Datos tendrá acceso a todos los datos personales y procesos de tratamiento.

8.2.5. Oficina de seguridad.

Dentro de la estructura de gobernanza de la ciberseguridad propuesta en el ENS, en la Guía de Seguridad de las TIC CCN-STIC 881, se define Oficina de Seguridad, cuyas competencias estarán relacionadas con las áreas de adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad y otras funciones conexas o concordantes. Su composición será la siguiente:

— El Director de la Oficina de seguridad, nombrado por el Comité de Seguridad, 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, nombrado por el Comité de Seguridad, 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 serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad:

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. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.

c. Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

— Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al Comité de Seguridad 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 del Comité.

— Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

— Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.

— Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

— Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.

— Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.

— Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la Información y protección de datos.

Periodicidad de las reuniones y adopción de acuerdos:

1. El Director de la Oficina de Seguridad convocará las reuniones de trabajo de sus miembros y recabará los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad, para su aprobación, en su caso.

2. La Oficina podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en la Oficina de Seguridad serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad.

3. Se reunirá, al menos, una vez al mes y siempre antes de las celebraciones del Comité de Seguridad.

8.2.6. Centro de Operaciones de Ciberseguridad (COCS).

Se define el Centro de Operaciones de Ciberseguridad (COCS), bajo la responsabilidad y dirección del Comité de Seguridad. El 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.

Las funciones del COCS serán:

— 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 cumplimiento de las funciones asignadas este organismo es de importancia vital para el logro de los objetivos de seguridad de la UEx y su adecuación al ENS.

Sus funciones serán realizadas por personal del Servicio de Informática y Comunicaciones de la Universidad, mientras no exista disponibilidad presupuestaria para su creación.

8.3. Procedimientos de designación.

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los responsables identificados en esta política se realizará por el rector de la UEx.

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

8.4. Datos personales.

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

9. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la información, corresponderá su resolución, en última instancia, al Rector en su condición de máximo responsable de la institución.

El Rector estará asistido por el Comité de Seguridad de la Información y, cuando proceda, por el Delegado de Protección de Datos.

10. Obligaciones del personal.

Todos los miembros de la UEx tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, así como las normas y procedimientos que la desarrollen, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal que presta servicio en la Universidad tiene el deber de colaborar en la mejora de los principios y requisitos en materia de seguridad de la información y protección de datos personales, evitando y minorando los riesgos en la medida de sus respectivas responsabilidades.

Todos los órganos y unidades de la Universidad prestarán su colaboración en las actuaciones de implementación de la Política de Seguridad de la Información.

A todos los miembros de la comunidad universitaria se les informará adecuadamente sobre concienciación en materia de seguridad de la información y se desarrollarán actividades formativas para ello.

Se establecerá un programa de concienciación y formación continua para atender a todos los miembros de la Universidad, en particular a los de nueva incorporación, en materia de seguridad de la información.

11. Gestión de riesgos.

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

— Al menos una vez al año.

— Cuando cambien la información y/o los servicios manejados de manera significativa.

— Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes

sistemas, promoviendo inversiones de carácter horizontal. El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.

2. Análisis de riesgos.

3. El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional. En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

12. Notificación de incidentes.

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, la UEx, notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

13. Desarrollo normativo 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 al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a. Primer nivel normativo: constituido por la presente Política de Seguridad de la Información, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables a los organismos o unidades de la universidad a los que sea de aplicación dichos documentos.

b. Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores. (Política de uso aceptable, Política de seguridad de recursos humanos, Política

de seguridad física y del entorno, Política de gestión las comunicaciones y las operaciones, Política de protección frente a amenazas, Política de de control de acceso, etc).

c. Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al órgano superior de la UEx, Consejo de Gobierno, la aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de la universidad, siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas. Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de la UEx, 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 de la Universidad, en soporte papel, esta documentación será custodiada por el Servicio de Informática y Comunicaciones.

14. Terceras partes.

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

Cuando la UEx utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

15. Mejora continua.

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

a) Revisión de la Política de Seguridad de la Información.

b) Revisión de los servicios e información y su categorización.

c) Ejecución con periodicidad anual del análisis de riesgos.

d) Realización de auditorías internas o, cuando procedan, externas.

e) Revisión de las medidas de seguridad.

f) Revisión y actualización de las normas y procedimientos.

• • •