FRANCISCO ANTONIO GONZÁLEZ DÍAZ, SECRETARIO GENERAL DE LA UNIVERSIDAD DE MURCIA

C E R T I F I C O:

Que el **Consejo de Gobierno de 16 de noviembre de 2018**, estando incluido en el orden del día, aprobó la **actualización del documento de Política de Seguridad de la Información,** en los términos que se indican en el anexo adjunto.

Lo que hago constar a los efectos oportunos.

VºBº
EL RECTOR
Fdo. José Luján Alcaraz

Firmado con certificado electrónico reconocido.
La información sobre el firmante, la fecha de firma y el código de verificación del documento se encuentra disponible en los márgenes izquierdo e inferior

(*) *A los efectos de lo establecido en el artículo 19.5, párrafo cuarto, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se advierte que el acta de la sesión citada en esta certificación se encuentra pendiente de aprobación.*

UNIVERSIDAD DE MURCIA

DOCUMENTO DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN

(Aprobado en Consejo de Gobierno de 2 de marzo de 2012, modificado en Consejo de Gobierno de 16 de noviembre de 2018)

1. Introducción

Las Tecnologías de la Información y las Comunicaciones (TIC) juegan un papel fundamental hoy día en la prestación de servicios en la administración pública y en el ámbito universitario y cada vez se hace más necesaria su adecuada gestión, y protección, ya que de ellas depende que la Universidad pueda desempeñar sus fines de forma efectiva. Además, con el inexorable contexto de transformación digital en el que nos encontramos, la información se convierte en uno de los activos más importantes de la Univesidad de Murcia, y como tal, debemos de protegerla con sistemas que garanticen seguridad de la misma, así como la continuidad en la prestación de los servicios universitarios.

Esta necesidad de seguridad y garantías en los sistemas de información, se convierte en esencial conforme se va avanzando en la implantación de las medidas establecidas por la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, que sentaron las bases para la creación de una administración electrónica 100% digital libre de papel.

La preocupación de la Universidad de Murcia por la seguridad de la información quedó de manifiesto con la aprobación por Consejo de Gobierno de 2 de marzo de 2012 de la Política de seguridad de la Información de la Universidad de Murcia, con el propósito de «sentar las bases de la fiabilidad con que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas».

La aprobación de dicha política reflejaba el compromiso de la Universidad de Murcia con el cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regulaba el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica establecía los principios básicos y requisitos mínimos que, de acuerdo con el interés general y con la naturaleza y complejidad de la materia regulada, permitían una protección adecuada de la información y los servicios telemáticos, y que por tanto exigía incluir el alcance y procedimiento para gestionar la seguridad electrónica de los sistemas que tratan información de las Administraciones públicas en el ámbito de la Ley 11/2007, de 22 de junio. En particular, este Real Decreto obligaba en su artículo 11 a que todas las administraciones públicas se dotasen de una Política de Seguridad aprobada por su órgano superior.

La actualización del Esquema Nacional de Seguridad con el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, y la aprobación del Reglamento General de Protección de Datos (RGPD 2016/679 de 27 de abril) de reciente entrada en vigor, añaden requisitos adicionales a la gestión interna de la seguridad de la información y la protección de datos que obligan a la actualización de nuestra política de seguridad, cuyo propósito es establecer de una forma clara y accesible a todos los miembros de la comunidad universitaria las bases de la gestión de la seguridad de la información en la Universidad de Murcia, así como las funciones, comisiones y procedimientos que se desarrollarán.

Mediante la aprobación de esta política todo el equipo de dirección de la Universidad y su Consejo de Gobierno ponen de manifiesto su compromiso con que la seguridad y el buen uso de sus sistemas de información sean uno de sus principales valores.

2. Objeto y ámbito de aplicación

El objeto de la presente Política de Seguridad de la Información es definir a todos los niveles los sistemas de Información de la Universidad de Murcia que dan soporte al ejercicio de los derechos y el cumplimiento de deberes a través de medios electrónicos en cumplimiento de lo dispuesto en la Ley 39/2015 y la Ley 40/2015. El R.D. 3/2010, modificado por R.D. 951/2015 se aplica a todos los recursos informáticos, los datos, las comunicaciones y los servicios electrónicos, y permite a la ciudadanía y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de medios electrónicos.

Los recursos informáticos de la Universidad de Murcia tienen como finalidad el apoyo a la docencia, a la investigación y a las tareas administrativas necesarias para el cumplimiento de sus fines. Son recursos TIC de la Universidad de Murcia todos los sistemas centrales y departamentales, estaciones de trabajo, ordenadores de puesto, impresoras y otros periféricos y dispositivos, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y almacenamiento que sean de su propiedad, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos. Así mismo, esta política también aplicará a toda la información que se genere como parte de la realización de las funciones de la Universidad, así como de los tratamientos de que esta pueda ser objeto, independientemente de que dicho tratamiento pueda ser manual, automático tanto si incluye como si no lo hace datos de carácter personal.

En este ámbito no se considera un “recurso TIC de la Universidad” aquellos ordenadores personales financiados a título individual, no inventariados a nombre de universidad de Murcia, 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. En estos casos, la Universidad se reserva el derecho de proporcionar acceso a la red desde este tipo de

recursos ajenos a la misma si no se proporcionan unos mínimos requisitos de seguridad o existen indicios o evidencias de un incidente potencial de seguridad que pueda comprometer o bien la seguridad de la información de los recursos TI de la Universidad o bien su buen nombre o imagen corporativa.

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 Universidad de Murcia, 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".

3. Misión y Objetivos

Tal cual se indica en nuestro portal de transparencia, la Universidad de Murcia es una institución pública de Educación Superior con un ámbito de acción internacional. Su finalidad es la de contribuir al desarrollo de la sociedad, actuando como agente dinamizador en cooperación con los demás agentes sociales. Sus actividades principales se centran en el desarrollo de la Investigación, la Formación, la Transferencia del conocimiento, y la Divulgación cultural, aplicando a todas ellas procesos de innovación y mejora continua, con el propósito de alcanzar un alto nivel de calidad de los resultados, visible mediante una clara política de transparencia.

Para llevar a cabo su misión en pleno siglo XXI, la Universidad es consciente de que ha emprender un verdadero proceso de transformación digital que, apoyándose en el uso de las TIC, le permita afrontar los grandes retos que supone la satisfacción de las necesidades que demanda nuestra sociedad digital en materia de formación, investigación y gestión.

Para poder afrontar este proceso de transformación, la Universidad de Murcia ha de dotarse de los medios necesarios para poder contar con una infraestructura TIC que garantice la continuidad y calidad de los servicios que presta, siendo fundamental el componente de la seguridad de la información como función prioritaria para la consecución de los objetivos estratégicos e institucionales. Para ello, se implantará un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la Norma UNE ISO/IEC 27001 integrado con el ENS, que permita fortalecer la seguridad de los servicios y de la información gestionada.

4. Marco Normativo

El Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad y su modificación por el Real Decreto 951/2015, de 23 de octubre, obliga a la Universidad de Murcia como organismo público a proteger los servicios que presta por medios electrónicos y que gestiona a través de su Sede Electrónica, siendo también de

aplicación la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.

Además, en materia de protección de datos, la Universidad de Murcia ha de cumplir la regulación legal estatal que regula la protección de los datos de carácter personal y lo dispuesto en el Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo al tratamiento y circulación de datos de las personas físicas.

Adicionalmente, el SGSI cumplirá el Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

Finalmente, también se respetarán las disposiciones de Ley 6/2001, de 21 de diciembre, de Universidades, modificada por la Ley Orgánica 4/2007, de 12 de abril, modificada por el Real Decreto Ley 14/2012, de 20 de abril, así como todas aquellas que se vayan incorporando como resultado de la aplicación de la presente política en el procedimiento referido al cumplimiento de la legislación vigente.

Las principales normas que configuran el marco general del régimen jurídico de la Universidad de Murcia se almacenarán en la Sede Electrónica, en el apartado “Normativa universitaria”. Allí estarán accesibles las principales normas y reglamentos de aplicación en la Universidad de Murcia. El apartado de normativa general recoge la legislación estatal y autonómica en materia universitaria; el de normativa de la Universidad de Murcia los reglamentos de organización y régimen interno.

Además la legislación y normativa interna de aplicación en el ámbito de la Administración electrónica de la Universidad de Murcia será recogida en la propia Sede electrónica de la UM en la sección “Sobre la Sede” que puede ser consultada en la dirección electrónica https://sede.um.es/

5. Principios de la seguridad de la información

En la toma de decisiones en materia de seguridad se deberán tener en cuenta los principios básicos enunciados en el Esquema Nacional de Seguridad. Por tanto, la presente Política de Seguridad de la Información, que establece el marco para el resto de los desarrollos normativos, estará también alineada con dichos principios:

a. La seguridad como un proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema que prestará la máxima atención a la concienciación de las personas que intervienen en el proceso. Toda la comunidad universitaria ha de 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. El conocimiento de los riesgos es la primera línea de defensa para la seguridad de los sistemas de información. Para mitigarlos, la Universidad mantendrá actualizado un marco normativo en materia de seguridad y ofrecerá la formación necesaria. El personal de la Universidad debe estar debidamente concienciado sobre esta materia para que pueda ser capaz de detectar posibles incidentes que pudieran perjudicar seriamente los sistemas de información.

Todo el personal de la Universidad es responsable de garantizar la seguridad de los sistemas de información con diferentes grados de participación según las funciones o atribuciones asignadas. Esta responsabilidad se concreta en el cumplimiento del marco normativo en materia de seguridad y protección de datos de carácter personal que la Universidad haya publicado y distribuido entre el personal. Se deberán articular los mecanismos necesarios para que el personal que acceda o trate información corporativa se comprometa a hacer un uso correcto de la misma, a acceder únicamente a la necesaria para desarrollar su trabajo y a reportar cualquier incidente o debilidad en este sentido por los medios que se determinen en las normas de seguridad.

b. Gestión de la seguridad basada en los riesgos

Las decisiones en materia de seguridad deben basarse en el análisis y gestión de riesgos como proceso esencial de seguridad, que deberá mantenerse permanentemente actualizado. La evaluación de riesgos identifica las amenazas y vulnerabilidades y debe ser suficientemente amplia para abarcar los principales factores internos y externos tales como factores tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones 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, los riesgos a los que estén expuestos y las medidas de seguridad. Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir la consideración de los posibles daños que pueden proceder de otros o ser causados por terceras personas.

c. Prevención, reacción y recuperación

La estrategia en materia de seguridad de la UM estará basada en la prevención, detección y corrección de amenazas, para conseguir que éstas no se materialicen o no

afecten gravemente a los datos que manejan los sistemas de información o los servicios que se prestan.

Las medidas de prevención deberán eliminar o, al menos, reducir la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, estrategias de disuasión y de reducción de la exposición a ciertas amenazas. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen en la mayor brevedad de tiempo que sea posible. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

d. Reevaluación periódica

Las medidas de seguridad se reevaluarán y se actualizarán de forma periódica para que su eficacia sea adecuada a la constante evolución tanto de los riesgos como de los sistemas de protección. Se realizarán evaluaciones y auditorías para comprobar que los requisitos establecidos por el ENS (tanto técnicos como normativos) se cumplen y que las medidas de seguridad son eficaces proporcionando el nivel de seguridad requerido.

e. Principio de legalidad

La seguridad de los sistemas de información deberá ser compatible con los valores esenciales de una sociedad democrática. Por tanto, las medidas de seguridad deberán ser aplicadas de manera coherente con la legislación garante de la intimidad de las personas, incluida la libertad de intercambiar pensamientos e ideas, el libre flujo de información y la protección adecuada de los datos de carácter personal. De la misma forma, la seguridad de los sistemas de información deberá preservar y proteger dichos valores respecto de los datos que sean custodiados por la Universidad con relación a los servicios que presta. Esta política y su desarrollo normativo, será coherente con el marco normativo del apartado 4.

f. Seguridad por defecto

Los sistemas de información deberán diseñarse y configurarse de forma que garanticen la seguridad por defecto. Un aspecto importante, pero no exclusivo, de este esfuerzo es el diseño y adopción de garantías adecuadas y soluciones para evitar o limitar el daño potencial de amenazas y vulnerabilidades identificadas.

La Seguridad debe ser un elemento fundamental de todos los servicios, sistemas y redes de la Universidad, así como una parte integral del diseño de los sistemas de información y su arquitectura. En los entornos de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

Tanto las garantías técnicas como las no técnicas y las medidas de seguridad a implantar serán proporcionales al valor de la información sobre los sistemas de información.

g. Gestión de incidencias

Se establecerán los mecanismos para llevar un control de las incidencias que se producen para que se pueda agilizar la reacción ante dicha incidencia con el objetivo de reducir los daños que ésta pueda producir, reaccionar de manera coordinada y obtener evidencias que permitan introducir los cambios necesarios para que la incidencia no se vuelva a producir; generando las correspondientes acciones preventivas, correctivas o de mejora que sean necesarias tras analizar los hechos.

6. Funciones y responsabilidades en seguridad de la información

Tal y como establece el ENS, la presente política ha de definir los roles o funciones de seguridad, especificando para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. La organización interna de la seguridad debe atender a la necesidad de regular tres grandes bloques de responsabilidad: la especificación de las necesidades o requisitos, la operación de los sistemas de información que se atiene a aquellos requisitos y la función de supervisión de acuerdo al principio básico del ENS de “la seguridad como función diferenciada”.

Para ello, se definen cinco roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información:

- Comisión de Seguridad de la Información
- Responsables de la Información.
- Responsable de los Servicios de Tramitación Electrónica.
- Responsable de los Sistemas de Información.
- Responsable de seguridad.

A continuación se describen cada uno de estos roles y sus responsabilidades.

A) Comisión de Seguridad de la Información

La Comisión de Seguridad de la Información es el órgano de gestión interna al que compete la Seguridad de la Información en la UM. El funcionamiento de esta Comisión se ajustará al funcionamiento de los órganos colegiados recogido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y otras normas que puedan resultarle de aplicación.

Esta Comisión estará compuesta por:

- El Delegado del Rector para la Universidad Digital, o Vicerrector con atribuciones en materia de gobernanza de las TIC, que actuará como presidente.
- El Secretario General.
- El Gerente.
- El Delegado de Protección de Datos.
- Dos Vicerrectores designados por el Rector.
- El jefe de Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA).
- El Responsable de Seguridad, que actuará como secretario del Comité.

La Comisión de Seguridad de la Información recabará información y auxilio de todas las áreas de la Universidad cuando así lo considere necesario y tiene las siguientes funciones y responsabilidades:

- Colaborar con el Comité de Estrategia del Gobierno TI en la elaboración de la estrategia de evolución de la Universidad de Murcia en lo que respecta a la seguridad de la información.
- Informar del estado de la seguridad de la información a los Órganos de Gobierno de la Universidad.
- Coordinar la adopción de acciones y medidas encaminadas a la adaptación de la Universidad de Murcia al Esquema Nacional de Seguridad.
- Proponer al Consejo de Dirección y al Consejo de Gobierno la aprobación de los reglamentos, política de seguridad y normativas generales y, en su caso, técnicas de seguridad de la UM relacionadas con la aplicación del ENS.
- Realizar una revisión anual del contenido de la Política de Seguridad proponiendo actualizaciones cuando sea necesario.
- Elaborar la normativa técnica de seguridad como desarrollo de la normativa general aprobada por Consejo de Gobierno.
- Aprobación de los procedimientos de seguridad de la UM.
- Proponer la designación de los responsables encargados de la aplicación y supervisión de las medidas de seguridad.
- Divulgación de la política y normativa de seguridad aprobada por la UM.
- Procurar que sean asignados los recursos necesarios para asegurar un adecuado nivel de seguridad en la UM priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Promover la realización de auditorías periódicas y promover la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI).
- Aprobar planes de mejora de la seguridad de la información.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
    - Informe del grado de cumplimiento del plan de adecuación.
    - 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.

- Nivel de desempeño de los procesos de gestión de incidencias.

- Seguimiento de las actividades desempeñadas por el Responsable de Seguridad de la Información así como la del resto de agentes que intervienen en la seguridad de la información.
- Resolver los conflictos de competencia que pudieran aparecer entre los diferentes responsables y/o las diferentes áreas de la Organización, elevando al Órgano competente aquellas cuestiones sobre las que no tenga suficiente autoridad para decidir.

B) Responsable de la Información

La figura del Responsable de la Información recaerá en el Secretario General de la Universidad de Murcia, que ostentará las funciones que la normativa vigente atribuye al responsable de los ficheros con datos de carácter personal, y promoverá la designación de un Delegado de Protección de Datos (DPD) según lo previsto en el Reglamento (UE) 679/2016. Tiene las siguientes funciones y responsabilidades:

- Establecimiento de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que es responsable.
- Valorar para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) establecidas por el ENS según el criterio de valoración establecido en su artículo 43.
- Trabajo en colaboración con el Responsable de Seguridad y el de Sistema en el mantenimiento actualizado del catálogo de los sistemas según el Anexo I del ENS.
- Velar por la inclusión y cumplimiento de cláusulas sobre seguridad en los contratos con terceras partes.

C) Responsable de los Servicios

El responsable de los servicios será el Delegado del Rector para la Universidad Digital, o vicerrector con competencia en materia de tecnologías de la información, que tendrá las siguientes funciones:

- Determinar los niveles de seguridad de los servicios, estableciendo sus requisitos en materia de seguridad. Dichos requisitos deberán ser garantizados en el tratamiento de la información que realicen los servicios de los que es responsable.
- Valorar para cada servicio contemplado en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) establecidas por el ENS según el criterio de valoración establecido en su artículo 43.
- Trabajo en colaboración con el Responsable de Seguridad y el de los Sistemas de Información en el mantenimiento de los sistemas catalogados según el Anexo I del ENS.
- Velar por la inclusión y cumplimiento de cláusulas sobre seguridad en los contratos con terceras partes.

D) Responsable de los Sistemas de Información

La figura del Responsable de los Sistemas de Información recaerá en el Jefe de Servicio de Infraestructuras TIC del Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA), que tendrá definidas las siguientes funciones y responsabilidades:

- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos de los sistemas de información bajo el alcance de aplicación del ENS, de forma regular y cuando haya cambios en la información manejada, en los servicios prestados o antes incidentes graves o reporte de vulnerabilidades graves.
- Desarrollar, operar y mantener los sistemas de información durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y los procedimientos de gestión de los sistemas estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Elaboración de los procedimientos de seguridad necesarios para la operativa de los sistemas, para que sean revisados por el Responsable de Seguridad y aprobados por la Comisión de Seguridad de la Información.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes de los sistemas durante las etapas de desarrollo, instalación y pruebas.
- Implantar y controlar las medidas específicas de seguridad de los sistemas y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación de los sistemas.
- Velar por el cumplimiento de las obligaciones de los Administradores de Seguridad del Sistema (ASS), cuyo rol se define en las recomendaciones del CCN-CERT.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión de los sistemas.
- Notificar e investigar los incidentes de seguridad que afecten a los sistemas de información, y en su caso, comunicarlo al Responsable de Seguridad y al Responsable de los servicios.
- Acordar la suspensión del manejo de cierta información o la prestación de cierto servicio si conoce deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos de protección establecidos.
- Elaboración de planes de continuidad del servicio que serán validados por el Responsable de Seguridad y aprobados y coordinados por la Comisión de Seguridad de la Información.
- Informar a Responsables de la información y de los Servicios de las incidencias funcionales relativas detectadas.

E) Responsable de Seguridad de la Información

La figura del Responsable de Seguridad de la Información recaerá en el Jefe de Sección Responsable de Seguridad del Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA), que será el responsable de velar por la seguridad de la información, de los servicios prestados por los sistemas de información y de dirigir el Sistema de Gestión de la Seguridad de la Información. Tendrá asignadas las siguientes funciones y responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en el ámbito de cumplimiento del ENS.
- Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos prestados por la Universidad según el criterio de valoración establecido por el artículo 43 del ENS.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS, en base a los niveles requeridos por el Responsable de la Información y el Responsable del Servicio Respectivamente.
- Elaboración y actualización de la Declaración de Aplicabilidad y las medidas adicionales de seguridad que se estimen oportunas.
- Realización y actualización del Análisis de Riesgos, en colaboración con el Responsable de los sistemas de información, e informar del resultado del análisis así como de los riesgos residuales al Responsable de la Información y al Responsable de los Servicios.
- Elaboración de la Configuración de Seguridad.
- Elaboración, en colaboración con el Responsable del los sistemas de información, de planes de mejora de la seguridad, para su aprobación en la Comisión de Seguridad de la Información.
- Realizar o instar la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Universidad en materia de seguridad.
- Promover la formación y concienciación del personal de la Universidad y en especial, del personal involucrado en las labores de gestión de los sistemas de información.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaboración de la normativa de seguridad que considere necesario formalizar, para su aprobación en Comisión de Seguridad de la Información.
- Revisión de los procedimientos de seguridad elaborados por el Responsable de los sistemas para su aprobación en la Comisión de Seguridad.
- Mantenimiento y gestión de toda la documentación, procedimientos y normas del Sistema de Gestión de la Seguridad de la Información.
- Elaborar como secretario de la Comisión los siguientes informes periódicos:

- Resumen consolidado de las actuaciones llevadas a cabo y en curso dentro del desarrollo del Plan de adecuación del ENS aprobado.
- Resumen consolidado de los incidentes de seguridad registrados desde la última reunión de la Comisión.
- Valoración y reporte a la Comisión de Seguridad de la Información del estado de la seguridad de los sistemas de información afectados por el ENS y la evolución de los niveles de riesgo a los que están expuestos.
- Resumen consolidado de los procedimientos de seguridad aprobados por el Responsable de Seguridad desde la última reunión de la Comisión.

F) Procedimiento de designación

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

7. Desarrollo normativo de esta política de seguridad

A) Estructuración de la documentación y relación entre los diferentes tipos de documentos

La Universidad de Murcia va a establecer un marco normativo en materia de seguridad estructurado por diferentes niveles de forma que los objetivos planteados por el presente documento tengan un desarrollo reglamentario que permita definir y concretar regulaciones y restricciones que sean aplicables sobre los sistemas de información o aplicables al personal que gestiona o utiliza dichos sistemas. Esta jerarquía de documentos debe ser conexa y coherente para dar cumplimiento a las medidas de seguridad establecidas por el R.D. 3/2010 modificado por el R.D. 951/2015 (ENS).

La Universidad de Murcia estructura su marco normativo en los siguientes tipos de documento:

- La presente *Política de Seguridad de la Información* que establece los requisitos y criterios de protección en el ámbito de la Universidad y servirá de guía para la creación de normas de seguridad. La política debe dar cumplimiento a la medida *org.1 Política de seguridad* del ENS.
- Las *normas de seguridad* definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política. La Universidad diferenciará entre *Normativa general*,

aplicable a todo el ámbito universitario y *Normativa técnica*, aplicable sobre el área de gestión y operación de las tecnologías de la información. Además, los contenidos elaborados deben también dar cumplimiento a la medida *org.2 Normas de seguridad* del ENS.

- Los *procedimientos de seguridad* en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos. Debe también dar cumplimiento a la medida *org.3 Procedimientos de seguridad* del ENS.

Esta jerarquía de tres niveles de documentación viene establecida como medidas de seguridad con carácter general que deben ser puestas en marcha para el cumplimiento del R.D. 3/2010 modificado por el R.D. 951/2015. Además, pueden considerarse dos tipos más de documentos:

- Basándose en los procedimientos de seguridad, y para entornos o sistemas de información concretos, podrán elaborarse *instrucciones técnicas de seguridad* que documenten de forma explícita y detallada las acciones técnicas a realizar en la ejecución del procedimiento o las tareas a considerar cuando se ejecute un procedimiento.
- También podrán existir como desarrollo de la propia política de seguridad o de cualesquiera de las normas existentes, las *normas de uso* que establecen las normas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información. Estos documentos destinados a usuario final resumirán y trasladarán los requisitos de seguridad a contemplar en la utilización o uso de determinadas tecnologías o servicios de manera concisa y fácilmente comprensible, así como lo que se considerará uso indebido y la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

B) Revisión, aprobación y difusión del marco normativo de seguridad

La documentación perteneciente al marco normativo en materia de seguridad debe estar controlada para garantizar su uso adecuado y correcto. Por ello, es necesario determinar en el presente apartado cómo se realizarán las siguientes tareas:

- Aprobar en forma los documentos previamente a su distribución;
- Revisar, actualizar y volver a aprobar los documentos, según vaya siendo necesario;
- Asegurar que los documentos están disponibles para todo aquel que los necesite;
- Asegurar que la distribución de documentos está controlada;
- Prevenir el uso no intencionado de documentos obsoletos.

La aprobación de los diferentes documentos del marco normativo se realizará por parte de los Órganos de Gobierno y Representación de la Universidad. A continuación se indica cada tipo de documento cual es el Órgano responsable de su aprobación.

- *Política de seguridad* será aprobada por el Consejo de Gobierno. Es responsabilidad de la Comisión de Seguridad de la Información la revisión anual del contenido de la Política de Seguridad y elevar una propuesta de actualización cuando sea necesario.
- *La Normativa general de seguridad* será bien aprobada por Consejo de gobierno o bien dictada por el Rector, el Secretario General o el Gerente.
- *La Normativa técnica de seguridad* será aprobada por el Rector a propuesta de la Comisión de Seguridad
- *Los Procedimientos de seguridad* serán aprobados por la Comisión de Seguridad de la Información.

La revisión y propuesta de nuevas versiones de cada documento podrá ser realizada por cualquiera de las áreas afectadas u Órganos de la Universidad y notificada al Responsable de Seguridad que canalizará las propuestas a través de la Comisión de Seguridad de la Información para que sean aprobadas por el Órgano adecuado según el criterio establecido en el párrafo anterior.

La distribución de documentación del marco normativo deberá atender también a criterios de seguridad según el contenido de dicha documentación. El marco normativo contendrá documentos de difusión pública y documentos de difusión limitada. En aquellas normativas y procedimientos técnicos de difusión limitada, la documentación será albergada en áreas de control de acceso restringido y será consultable por el personal técnico bajo el principio de mínimos privilegios. La información de difusión pública se albergará en la Sede electrónica de la UM que puede ser consultada en la dirección electrónica https://sede.um.es/.

Toda nueva versión de un documento aprobado dentro del marco normativo será comunicada según el alcance de uso del documento y el nivel de difusión requerido de forma que el personal pueda eliminar las versiones de los documentos obsoletos.

8. Responsabilidades en caso de Incumplimiento

La Comisión de Seguridad de la Información podrá apreciar si por parte del personal que tiene acceso a datos de la UM, o trata dichos datos en el ejercicio de sus actividades laborales, existe algún tipo de incumplimiento en las obligaciones generales establecidas en este documento. En el caso de incumplimiento de la Política de seguridad de la UM, se prevén medidas preventivas y correctoras encaminadas a salvaguardar y proteger las redes y sistemas de información. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Públicas o de la propia UM.

9. Terceras Partes

Cuando la Universidad de Murcia preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales de comunicación y colaboración entre los respectivos Órganos de Coordinación de la Seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la UM 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.

Glosario de términos

A continuación se describen el significado de los diferentes términos, pertenecientes al vocabulario de la seguridad de la información, que aparecen en el presente documento.

- ***activo:*** componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
- ***análisis de riesgos****:* utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
- ***auditoría de la seguridad***: revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.
- ***autenticidad****:* propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- ***categoría de un sistema***: es un nivel, dentro de la escala básica-media-alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. la categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.
- ***confidencialidad****:* propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- ***datos de carácter personal****:* cualquier información concerniente a personas físicas identificadas o identificables según establece la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- ***disponibilidad****:* propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- ***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 de los sistemas de información.
- ***integridad****:* propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- ***medidas de seguridad****:* conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

- ***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.
- ***responsable de la Información**:* persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
- ***responsable de la seguridad**:* el Responsable de Seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- ***responsable del Servicio**:* persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.
- ***responsable de los sistemas**:* persona que se encarga de la explotación de los sistemas de información.
- ***riesgo**:* estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- ***seguridad de la información**:* es la protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizada, con el fin de proporcionar confidencialidad, integridad y disponibilidad.
- ***seguridad de los sistemas de información:*** es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.
- ***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.
- ***trazabilidad**:* propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- ***vulnerabilidad**:* una debilidad que puede ser aprovechada por una amenaza.