SECRETARIA GENERAL

Acuerdo de aprobación del documento de Política de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad Miguel Hernández.

Vista la propuesta que formula el Vicerrector de Infraestructuras de la Universidad, **el Consejo de Gobierno, reunido en sesión de 28 de septiembre de 2016, ACUERDA:**

Aprobar el documento relativo a la Política de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad Miguel Hernández, en los términos reflejados a continuación:

POLÍTICA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Índice

Introducción

El uso de medios informáticos y telemáticos en las diferentes actividades académicas que se llevan a cabo desde la Universidad, tanto docentes como de gestión o de mera comunicación, es un hecho incuestionable y totalmente imbricado en todas ellas.

Por otra parte, la normativa, tanto europea como nacional, reguladora de la implantación del uso de medios electrónicos exige que el establecimiento de servicios públicos en línea se realice dentro de un marco normativo propio que garantice un uso de los mismos con total seguridad y confianza para los usuarios y los funcionarios, a la vez que permita la necesaria interoperabilidad entre Administraciones, en un entorno también protegido.

El principal objetivo que se persigue con la seguridad de la información es poder garantizar la calidad de la información y la prestación continuada de los servicios, mediante la actuación preventiva y la

supervisión de la actividad diaria, reaccionando con agilidad ante los posibles incidentes que pudieran ocasionarse.

Por ello, la Universidad Miguel Hernández de Elche (en adelante UMH), reconoce como una obligación asegurar y proteger adecuadamente los sistemas de información, los datos, los equipos y las redes de comunicaciones. Esta obligación debe ser compartida por cada uno de los integrantes de la comunidad universitaria, en sus diferentes ámbitos de actuación y en sus diferentes niveles de uso y responsabilidad.

Los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y de los servicios. Para defenderse de estas amenazas y garantizar la prestación continua de los servicios, se requiere una estrategia que se adapte a los posibles cambios de las condiciones del entorno. La Política de Seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante TIC) afecta a todas las unidades organizativas de la UMH, las cuales deben conocer y poner en práctica todo aquello que en el desarrollo de la misma les sea de aplicación.

Para llevar a cabo este objetivo, es preciso la implicación de toda la comunidad universitaria, cada colectivo de una manera determinada según su actividad. A tal fin, Servicios Informáticos (SSII) de la Universidad es la unidad organizativa responsable de los Sistemas de Información de Gestión centralizada así como de los diferentes servicios TIC e infraestructuras tecnológicas de la institución.

La UMH, al ser un Centro de Educación Superior, está conectada al resto de la comunidad universitaria y a Internet mediante el acceso que le proporciona la institución Red.es a través de la firma de un Convenio de Adhesión. Esto conlleva el respeto y cumplimiento de las normas y condiciones de uso establecidas por esta organización. (http://www.rediris.es/).

La UMH asume el deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de sus servicios y, por tanto, los objetivos y principios establecidos en esta Política.

Por todo lo anterior, el presente documento recoge la Política de Seguridad TIC de la UMH y en él se establecen el conjunto de estrategias y medidas necesarias, tanto técnicas como organizativas, encaminadas a conseguir un nivel de protección adecuado y así asegurar el cumplimiento legal de garantizar la disponibilidad y la confidencialidad de la información.

Alcance

La Política de Seguridad TIC se aplica a todos los sistemas de Información de la UMH, a toda la comunidad universitaria y a todas las unidades organizativas que la conforman, así como a los terceros que por su actividad o su relación con la UMH se encuentren en el ámbito de aplicación de esta Política.

El objetivo de esta Política es garantizar la confidencialidad, integridad y disponibilidad de la información y de los servicios telemáticos ofrecidos, así como dar cumplimiento a todos los requisitos y condiciones establecidos en el marco legal aplicable.

Principios de protección

1. Principios básicos de Protección

La presente Política de Seguridad TIC se basa en unos principios básicos de protección que sustentarán todas las actuaciones que la UMH realice en materia de seguridad TIC. Estos principios son:

a. Prevención

La UMH implementará las medidas de seguridad y los controles adicionales basados en evaluación de amenazas y de riesgos establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en ámbito de la Administración Electrónica (en adelante ENS), para prevenir e intentar evitar que la información o los servicios se vean perjudicados por incidentes de seguridad.

b. Detección

La UMH implantará las medidas oportunas a través de la monitorización de los sistemas a fin de detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Además se establecerán los mecanismos de detección, análisis y reporte para casos en los que se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

c. Respuesta

La UMH contará con mecanismos para reaccionar y responder eficazmente frente a los incidentes de seguridad que puedan producirse y pondrá en marcha los protocolos necesarios para el intercambio de información relacionada con aquél.

d. Recuperación

Para garantizar la disponibilidad de los servicios esenciales, la UMH implementará medidas de recuperación que 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.

2. Gestión de los riesgos

Las decisiones en materia de seguridad deben basarse en el análisis y la gestión de los riesgos como proceso esencial de seguridad; proceso que deberá mantenerse permanentemente actualizado.

La evaluación de los riesgos identifica las amenazas y vulnerabilidades y debe ser suficientemente amplia para abarcar los principales factores internos y externos (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 del nivel de riesgo se realizará mediante el despliegue de las oportunas medidas de seguridad y la implantación de los controles necesarios. Con el objetivo de minimizar los posibles inconvenientes para los usuarios de los servicios TIC, la gestión de los riesgos siempre debe contemplar el equilibrio entre estos impactos en la institución y los posibles fallos de seguridad evaluados.

3. Concienciación, formación y capacitación en materia de seguridad TIC

Todo el personal de la UMH debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información ya que el uso de los servicios y el tratamiento de la información se realizan a todos los niveles. La UMH, a tal fin, establecerá las medidas formativas y de difusión oportunas para fomentar concienciación en materia de seguridad TIC de toda la comunidad universitaria.

La concienciación deberá ir dirigida a hacer posible que los usuarios TIC de la UMH puedan reconocer los problemas e incidentes en seguridad de la información y responder de acuerdo a las competencias de su puesto de trabajo.

En particular, la UMH llevará a cabo planes de formación y capacitación específicos en materia de seguridad TIC para cada uno de los perfiles profesionales del personal de la UMH.

4. Responsabilidad

El personal de la UMH es responsable de garantizar la seguridad de los sistemas de información de acuerdo a sus funciones o atribuciones desempeñadas. Esta responsabilidad se concreta en el cumplimiento del marco normativo legal en materia de Seguridad TIC y de la presente Política.

5. Diseño e implementación de la seguridad.

Los controles de seguridad TIC deben ser tenidos en cuenta en las fases iniciales de los proyectos técnicos o de diseño de los sistemas de información de forma que garanticen la seguridad por defecto. Aunque debe tenerse presente que ningún conjunto de controles pueden garantizar la seguridad TIC completa, los proyectos deben incorporar las medidas y controles necesarios a fin de minimizar y gestionar los riesgos, amenazas y vulnerabilidades identificadas.

Con el objetivo de respetar el principio de proporcionalidad, las medidas de seguridad a implantar para la protección de los sistemas y las garantías técnicas deben ajustarse al valor de la información.

6. Gestión de la seguridad y mejora continua

La gestión de la seguridad TIC debe ser sistemática, independiente y periódica, debiendo realizarse cuando se produzcan cambios significativos.

La gestión de la seguridad TIC implica el diseño de objetivos de control y seguimiento del estado de la seguridad TIC y la implantación de los controles necesarios, la gestión de incidencias, las medidas de seguridad, los procesos y los procedimientos oportunos para adoptar las acciones correctivas que correspondan.

En concreto, las auditorías planificadas deben comprobar el cumplimiento de los requisitos establecidos por ENS. Además se debe comprobar que las medidas de seguridad establecidas en la Política de Seguridad TIC son eficaces, proporcionando el nivel de seguridad deseado.

Marco legal

Las principales normas que configuran el marco jurídico en materia de seguridad de la Universidad Miguel Hernández se encuentran disponibles en la Sede Electrónica y, en concreto, las principales normas y reglamentos de aplicación en materia de Administración Electrónica. Toda la información puede ser consultada en la dirección https://sede.umh.es.

Marco normativo de seguridad TIC de la UMH

a. Estructura de la documentación y relación entre los diferentes tipos de documentos

El marco normativo en materia de seguridad de la UMH se encuentra estructurado en diferentes niveles, de forma que los objetivos planteados por el presente documento tengan un desarrollo reglamentario que permita definir y concretar aquellos aspectos aplicables a los sistemas de información y 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 ENS en el ámbito de la Administración Electrónica.

La UMH estructura su marco normativo en los siguientes documentos:

- La Política de Seguridad TIC establece los requisitos y los criterios de protección en el ámbito de la Universidad y servirá de guía para la creación de normas de seguridad. La Política de Seguridad TIC es acorde con lo establecido en el Documento de Seguridad que exige Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD).
- **Las normas de seguridad de la información** definen el ámbito de protección y los requisitos de seguridad necesarios. La Universidad contará con dos tipos de normativas de seguridad*:*
  a. De carácter general, aplicable a todo usuario final del ámbito universitario y
  b. De carácter técnico, aplicables al personal con perfil técnico.
  Estas normativas deben cumplir la medida org.2: normas de seguridad del R.D. 3/2010. En concreto, tendrá rango de norma de seguridad, el "*Documento de Seguridad de Ficheros Automatizados de Datos de Carácter Personal de la UMH*" al amparo de la presente Política.
- **Los procedimientos de seguridad** describen de forma concreta cómo debe actuar el usuario final de acuerdo a lo establecido en las normas y quienes son las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Estos procedimientos deben dar cumplimiento a la medida org.3: procedimientos de seguridad del R.D. 3/2010.
- **Las Instrucciones técnicas de seguridad** que se elaborarán para documentar, de forma explícita y detallada, las acciones técnicas a realizar o las tareas a considerar en la ejecución de un procedimiento.
- **Las Guías o recomendaciones específicas de uso** basadas en códigos de buenas prácticas y/o de uso indebido, que establecen comportamientos y códigos éticos que deben cumplir los destinados, tanto técnicos como usuarios finales.

b. Procedimiento de aprobación de la Política de Seguridad TIC y su desarrollo

- *Política de Seguridad* TIC es aprobada por el Consejo de Gobierno y publicada en el BOUMH. La revisión y modificación de la *Política de Seguridad* TIC seguirá el mismo procedimiento de aprobación y publicación.
- Las *normas de seguridad TIC* serán aprobadas por el Consejo de Gobierno, elevadas por la Comisión de Seguridad TIC, a propuesta de cualquier miembro de la comunidad universitaria responsable de cualquier actividad a las que hace referencia la norma. La Comisión de Seguridad TIC evaluará tanto la conveniencia como el contenido de las normas propuestas antes de elevarlas al Consejo de Gobierno, si procede, para su aprobación. La publicación se realizará en el sitio web correspondiente, contemplando los permisos de acceso que procedan. La revisión y modificación seguirá el mismo procedimiento de aprobación y publicación.
- Los *procedimientos de seguridad*, las *instrucciones técnicas de seguridad* así como las *guías y recomendaciones*, por su ágil ciclo de vida, serán aprobados por la Comisión de Seguridad TIC. La publicación se realizará por el Responsable de Seguridad en un espacio habilitado en el blog oficial de los Servicios Informáticos, contemplando los permisos de acceso que procedan.

Organización de la seguridad de la información

Tal como establece el ENS, es necesario dentro de la presente Política, establecer los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, el procedimiento para su designación y renovación, así como la estructura organizativa que permite a la UMH la gestión y coordinación de la seguridad TIC, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

En el conjunto de normativas que derivan del presente documento Política de Seguridad TIC se concretarán los roles y responsabilidades que correspondan y se identificarán los activos y los procesos de seguridad asociados con cada sistema específico, en función del tipo de materia en seguridad TIC o requisito legal, que cada una de las normativas esté regulando.

La Comisión de Seguridad TIC es el máximo órgano al que compete la Seguridad de la Información TIC en la UMH. En este sentido, identifica objetivos y estrategias relacionadas con la seguridad de la información y dirige y controla los procesos relacionados con la seguridad. El funcionamiento de esta Comisión se ajustará al funcionamiento de los órganos colegiados recogido en la Ley 40/15, de 1 de octubre de Régimen Jurídico del Sector Público.

Esta comisión estará compuesta por:

Presidente
Vocal jurídico
Vocal Técnico
Vocales Responsables de Servicios o Procesos de Gestión Administrativa Electrónica
Vocales Responsables de la Información
Responsable de Seguridad TIC
Secretario de la Comisión

La presidencia corresponde al Rector, quien podrá delegar esta función, y es el encargado del nombramiento del resto de miembros de la Comisión. A requerimiento de la Comisión podrán asistir a las reuniones, cuando así se decida, otros responsables designados por la Comisión encargados de la seguridad de sistemas concretos y con roles específicos. Estos roles se especifican en la presente Política en los siguientes epígrafes.

La Comisión de Seguridad TIC de la UMH asume todas las competencias, a nivel organizativo, para velar por el cumplimiento de las normativas incluidas en esta Política así como el marco legislativo que sea de aplicación en materia de seguridad de la información, en concreto, en la aplicación de la Ley de Protección de Datos de Carácter Personal y del Esquema Nacional de Seguridad.

Esta Comisión tendrá las siguientes funciones:

- Informar a los órganos de gobierno.
- Divulgación de la Política y normativas de seguridad TIC de la Universidad.
- Aprobación de los procedimientos de seguridad que desarrollen la presente Política.
- Revisión anual de la Política de Seguridad TIC.
- Desarrollo del procedimiento de designación de responsables a los diferentes roles previstos en la presente Política.
- Designación de responsables con diferentes roles y para diferentes activos a proteger.
- Supervisión y aprobación de las tareas de seguimiento del ENS: Adecuación, análisis de riesgos y auditoría bienal.
- Elaboración de informes periódicos (informe anual sobre los incidentes de seguridad registrados; informe anual sobre el estado de la seguridad de los sistemas de información afectados por el ENS y la LOPD y propuestas de mejora; informe anual sobre la evolución de los niveles de riesgo tras su revisión periódica y propuestas de mejora e informe anual de los procedimientos de seguridad aprobados).

a. Funciones y responsabilidades de los miembros de la Comisión de Seguridad TIC

i. Presidente de la Comisión de Seguridad

El presidente de la Comisión de Seguridad es el máximo representante de la universidad en materia de seguridad de la información y como tal tiene asignadas las siguientes funciones:

- Establecimiento de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información.
- Valorar el análisis de riesgos de las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) según el criterio de valoración establecido en el artículo 43 del ENS.
- Realizar el mantenimiento de los sistemas catalogados según el Anexo I del ENS, en colaboración con el resto de miembros de la Comisión.
- Velar por la inclusión de cláusulas de confidencialidad en los contratos con terceras partes y por su cumplimiento.
- Promover la formación y la concienciación del personal de la universidad involucrado en las labores de gestión de los sistemas de información que dan soporte a los procesos de administración electrónica de la universidad y a los ficheros de datos de carácter personal.
- Promover y supervisar la investigación de los incidentes de seguridad relacionados con los sistemas de información que dan soporte a los servicios de administración electrónica y a los ficheros de datos de carácter personal de la universidad desde su notificación hasta su resolución.
- Proponer la redacción de aquella normativa de seguridad de la universidad que considere necesario formalizar.
- Impulsar la realización del Plan de adecuación al ENS.

ii. Vocal Jurídico

El vocal jurídico tiene la función de asesoramiento a los diferentes miembros de la Comisión en materia jurídica dentro del marco regulatorio aplicable en cada momento, emitiendo para ello los informes que se estimen oportunos.

Asimismo tiene encomendada la función de participación en la propuesta y desarrollo de las normativas que como implementación de la presente Política se lleven a cabo con el fin de asegurar su adecuación al marco legal vigente.

iii. Vocal Técnico

El vocal técnico tiene la función principal de asesoramiento técnico a los diferentes miembros de la Comisión, teniendo en cuenta el estado tecnológico de los sistemas de la UMH y la evolución de la tecnología en cada momento, emitiendo para ello los informes que se estimen oportunos.

Igualmente, la participación en la propuesta y desarrollo de las normativas que como implementación de la presente Política se lleven a cabo con el fin de asegurar la adecuación de las decisiones y medidas que se propongan de tal forma que se garantice al máximo su factibilidad real en función de los recursos disponibles y el estado tecnológico de los sistemas de la UMH en cada momento.

iv. Vocales de Responsables de Servicios o Procesos de Gestión Administrativa Electrónica

Sus funciones son:

- Establecimiento de los requisitos de los servicios de tramitación electrónica en materia de seguridad que deban ser garantizados en el tratamiento de la información por parte de 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) según el criterio de valoración establecido en el artículo 43 del ENS.

- Realizar el mantenimiento de los sistemas catalogados según el Anexo I del ENS, en colaboración con el resto de miembros de la Comisión.
- Velar por la inclusión de cláusulas de confidencialidad en los contratos con terceras partes y por su cumplimiento.
- Promover la formación y la concienciación del personal de la universidad involucrado en las labores de gestión de los sistemas de información que dan soporte a los servicios de administración electrónica y a los ficheros de datos de carácter personal de los que son responsables.
- Apoyar y supervisar la investigación de los incidentes de seguridad relacionados con los sistemas de información que dan soporte a los servicios de administración electrónica y a los ficheros de datos de carácter personal de los que son responsables desde su notificación hasta su resolución.

v. Vocales de Responsables de la Información

Sus funciones son:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con la persona responsable de seguridad y la persona responsable de sistemas en el mantenimiento de los sistemas catalogados.
- Colaborar en la valoración de cada sistema de información de los que es responsable, además de en el análisis de riesgos de las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) según el criterio de valoración establecido en el artículo 43 del ENS.
- Colaborar en el mantenimiento de los sistemas catalogados según el Anexo I del ENS, en colaboración con el resto de miembros de la Comisión.
- Velar por la inclusión de cláusulas de confidencialidad en los contratos con terceras partes y por su cumplimiento.
- Promover la formación y la concienciación del personal de la universidad involucrado en las laboras de gestión de los sistemas de información a su cargo que dan soporte a los servicios de administración electrónica y a los ficheros de datos de carácter personal de los que son responsables.
- Apoyar y supervisar la investigación de los incidentes de seguridad relacionados con los sistemas de información que dan soporte a los servicios de administración electrónica y a los ficheros de datos de carácter personal de los que son responsables desde su notificación hasta su resolución.

vi. Responsable de Seguridad TIC

El Responsable de Seguridad TIC asume las funciones de la gestión, control y supervisión de los requisitos de seguridad de la información y de los servicios, únicamente en el ámbito de los Sistemas de Información de la Gestión Administrativa Universitaria, acorde con el cumplimiento de marco regulatorio aplicable, en concreto del ENS y de la LOPD. Además, es el referente organizativo en materia de Seguridad TIC de la UMH para los responsables técnicos de seguridad del resto de sistemas de información.

En las normativas correspondientes para cada sistema de información se asignará el responsable de seguridad concreto para cada activo. Dichas normativas deben incluir, como mínimo, la definición del conjunto de funciones del responsable de seguridad, la descripción de la provisión e implantación de los controles, las medidas de seguridad, la definición y documentación de los diferentes niveles de autorización que correspondan a cada uno de los activos a proteger dentro de su competencia.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios. La política de seguridad detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

En concreto este puesto tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en el ámbito del 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 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.
- Realizar o instar a la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados
- Monitorizar el estado de la seguridad de los sistemas proporcionado por las herramientas de gestión de eventos de seguridad u otros mecanismos de auditoría implementados en los sistemas por los diferentes responsables técnicos de los mismos
- Promover la formación y la concienciación del personal técnico de Servicios Informáticos involucrados en las laboras de gestión de los sistemas de información que dan soporte a los procesos de administración electrónica de la universidad y a los ficheros de datos de carácter personal
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución
- Proponer la redacción de aquella normativa de seguridad de la universidad que considere necesario formalizar
- Aprobar los procedimientos de seguridad elaborados por el responsable de los sistemas cuando en virtud del contenido definido no requieran revisión y aprobación de la Comisión de Seguridad
- Custodiar y organizar la documentación que da soporte y desarrolla la presente Política de Seguridad TIC de la UMH elaborada por los diferentes responsables involucrados

b. Roles y responsabilidades en materia de seguridad TIC

La Universidad es una organización compleja y desarrolla una actividad variada y heterogénea por lo que no es viable que una única persona asuma la responsabilidad completa de Seguridad TIC para toda la institución. De ahí que esta Política incluya diferentes responsables de seguridad de la información que serán nombrados por la Comisión para el desarrollo e implementación directa de las diferentes normativas y procedimientos para cada uno de los activos y/o actividades a proteger.

Los roles se estructuran funcionalmente en niveles, tal y como se contempla en el artículo 10 del ENS:

- Responsabilidades a nivel de datos o información
- Responsabilidades a nivel de operación o servicio de los sistemas de información, a través de los cuales se presenta o se hace uso de dicha información
- Responsabilidades a nivel técnico de los sistemas de información
- Responsabilidades de seguridad TIC

Estos responsables, una vez nombrados, deberán asistir a las reuniones de la Comisión cuando sean requeridos para ello, porque sea necesario para el seguimiento de cada una de actividades atribuidas a cada responsable en el ámbito de sus competencias.

1. Responsable de la Información en la UMH

Los Responsables de la Información tendrán las siguientes funciones:

- Establecer los requisitos de la información en materia de seguridad.
- Comunicar a la Comisión de Seguridad TIC cualquier actualización sobre la valoración del impacto definida o nuevas informaciones que requieran ser valoradas.
- Valorar el impacto que tendría un incidente que afectara a la seguridad de la información con perjuicio para integridad y confidencialidad, según establece el Anexo I del ENS.
- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Determinar los niveles de seguridad de la información en relación a la aplicación del Esquema Nacional de Seguridad y de la LOPD.

2. Responsable de los Servicios de Tramitación Telemática

Los Responsables de los Servicios de Tramitación Telemática tendrán las siguientes funciones:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los correspondientes a interoperabilidad, accesibilidad y disponibilidad.
- Comunicar al Comité de Seguridad cualquier actualización sobre los servicios telemáticos o nuevos servicios que requieran ser valorados.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos de los servicios de tramitación telemática con terceras partes y por su cumplimiento.
- Determinar los niveles de seguridad de los servicios en relación a la aplicación del Esquema Nacional de Seguridad y de la LOPD.

3. Responsable de Seguridad de la UMH

El Responsable de Seguridad de la UMH tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los Sistemas en su ámbito de responsabilidad.
- Realizar o promover 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 de los Servicios Informáticos, 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.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del Sistema.
- Monitorizar el estado de seguridad del Sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del Sistema, incluyendo los incidentes más relevantes del periodo.

- Proponer la normativa de seguridad de la universidad.
- Aprobar los procedimientos de seguridad elaborados por el Responsable del Sistema.

4. Responsable de los Sistemas de Información en la UMH

El Responsable del Sistema de Información tendrá, dentro de sus áreas de actuación, las siguientes funciones:

- Llevar a cabo el análisis y la gestión de riesgos en el Sistema.
- Determinar la categoría del Sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema 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 Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicar al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Elaborar planes de mejora de la seguridad del Sistema.
- Elaborar la documentación de seguridad del Sistema.
- Asegurarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Obligaciones del Personal de la UMH

Todos los miembros de la Universidad Miguel Hernández de Elche tienen la obligación de conocer y cumplir esta Política de Seguridad TIC de la UMH y las diferentes normativas de seguridad que le dan soporte, siendo responsabilidad de la Comisión de Seguridad TIC disponer de los medios necesarios para que la información llegue a los afectados.

Los miembros de la UMH atenderán a las sesiones informativas en materia de seguridad de la información cuando éstas sean convocadas por la Comisión. La UMH establecerá un programa de

formación continua para atender a todos los miembros de la UMH, en particular a los de nueva incorporación.

La Comisión se asegurará que las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo de forma específica. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Terceros Implicados

Cuando la Universidad Miguel Hernández preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad TIC, se establecerán canales para reporte y coordinación de las respectivas Comisiones de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la UMH utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad TIC y de las normativas de seguridad y procedimientos que ataña a dichos servicios o información. Los terceros quedarán sujetos a las obligaciones establecidas en dichas normativas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, en su caso. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que los terceros implicados estarán adecuadamente formados 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 los terceros, según lo establecido 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. Será necesaria la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Gestión de Riesgos

Las decisiones en materia de seguridad deben basarse en el análisis de riesgos y su gestión como proceso esencial de la seguridad. El análisis de riesgos deberá mantenerse actualizado regularmente y se aplica a todos los sistemas sujetos a esta Política, evaluando las amenazas y vulnerabilidades a los que están expuestos. El análisis debe ser lo suficientemente exhaustivo para abarcar los factores tanto internos como externos de tipo tecnológico, humano, político 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, los cuales serán valorados por la Comisión tras el informe preceptivo del responsable de seguridad. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que deberán, en cualquier caso, establecer un equilibro entre la naturaleza de los datos, los tratamientos y los servicios con los riesgos a los que estén expuestos y las medidas de seguridad adoptadas en cada caso. Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir los posibles daños procedentes de otros sistemas o causados por terceras personas.
Este análisis se repetirá al menos una vez al año o bien cuando cambie la información manejada; cambien los servicios prestados, ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, la Comisión de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados, como órgano competente y responsable de la Información. La Comisión de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Revisión de la Política de seguridad de la información.

Será misión de la Comisión de Seguridad TIC la revisión anual de esta Política de Seguridad TIC y su propuesta al Consejo de Gobierno para su aprobación.
Asimismo es misión de la Comisión de la Seguridad TIC la difusión de La Política de Seguridad TIC, una vez aprobada, para conocimiento de todas las partes afectadas.

Responsabilidades en caso de incumplimiento

La Comisión de Seguridad TIC podrá apreciar, si por parte del personal que tiene acceso a datos de la UMH o que realiza el tratamiento de los mismos 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 TIC de la UMH, se prevén medidas correctoras y preventivas 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 de la Administraciones Públicas o de la propia Universidad Miguel Hernández de Elche.

Entrada en vigor
La presente Política entrará en vigor en la fecha de entrada en vigor del Reglamento de Administración Electrónica de la UMH.