UNIVERSITAS Miguel Hernández

SECRETARIA GENERAL

NOTIFICACIÓ D'ACORD

Acord d'aprovació de la Política de seguretat de la informació de la Universitat Miguel Hernández.

La Universitat Miguel Hernández d'Elx té aprovada la seua Política de seguretat de les tecnologies de la informació i les comunicacions de la Universitat Miguel Hernández, pel Consell de Govern, reunit en la sessió de 28 de setembre de 2016. Aquesta política de seguretat mancava en el seu articulat de la Missió de la Universitat, sobre la base de la qual es pot recategoritzar el Sistema d'informació de la UMH a nivell bàsic i no nivell alt com teníem declarat el nostre sistema al Ministeri de la Presidència, en compliment de l'article 35 del RD 3/2010 pel qual es regula l'Esquema nacional de seguretat (ENS).

Després d'una auditoria encarregada per aquest vicerectorat a una consultora externa, es conclou que podem baixar el nostre sistema a nivell baix, evitant així dur a terme auditories d'obligat compliment bianuals per als sistemes catalogats com a mitjà o alt. Es proposa aquesta nova Política de Seguretat de la Informació, seguint les pautes que defineix la Guia CCN-STIC-805 per a les administracions públiques, igual que han fet ja altres universitats i adaptar-nos així a l'Informe executiu CCN-CERT IT 40/16 d'agost 2016 en què s'analitza l'estat ENS de 40 de les 50 universitats públiques espanyoles i es conclou que les universitats poden declarar els seus sistemes a nivell baix, complint amb l'ENS, i com ja han realitzat universitats d'Andalusia, Madrid i Catalunya.

NOTIFICACIÓN DE ACUERDO

Acuerdo de aprobación de la Política de Seguridad de la Información de la Universidad Miguel Hernández.

La Universidad Miguel Hernández de Elche tiene aprobada su Política de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad Miguel Hernández, por el Consejo de Gobierno, reunido en sesión de 28 de septiembre de 2016. Esta política de seguridad carecía en su articulado de la Misión de la Universidad, en base a la cual se puede recategorizar el Sistema de Información de la UMH a nivel básico y no nivel alto como teníamos declarado nuestro sistema al Ministerio de la Presidencia, en cumplimiento del artículo 35 del RD 3/2010 por el que se regula el Esquema Nacional de Seguridad (ENS).

Tras una auditoría encargada por este vicerrectorado a una consultora externa, se concluye que podemos bajar nuestro sistema a nivel bajo, evitando así realizar así auditorias de obligado cumplimiento bianuales para los sistemas catalogados como medio o alto. Se propone esta nueva Política de Seguridad de la Información, siguiendo las pautas que define la Guía CCN-STIC-805 para las administraciones públicas, al igual que han hecho ya otras universidades y adaptarnos así al Informe Ejecutivo CCN-CERT IT 40/16 de agosto 2016 donde se analiza el estado ENS de 40 de las 50 universidades públicas españolas y se concluye que las universidades pueden declarar sus sistemas a nivel bajo, cumpliendo con el ENS, y como ya han realizado universidades de Andalucía, Madrid y Cataluña.

Vista la proposta que formula el vicerector de Tecnologies de la Informació de la Universitat,

el Consell de Govern, reunit en la sessió de 27 de juny de 2018, ACORDA:

Aprovar la política de seguretat de la informació de la Universitat Miguel Hernández d'Elx, en els termes que es reflecteixen a continuació:

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE LA UMH

1. INTRODUCCIÓ

La Política de seguretat de la informació s'elabora en compliment de l'exigència del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema nacional de seguretat en l'àmbit de l'administració electrònica (d'ara en avant ENS), que en l'article 11 estableix l'obligació per a les administracions públiques de disposar d'una política de seguretat i indica els requisits mínims que ha de complir.

Així mateix, cal tindre presents les previsions de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques. En aquest sentit, destaca l'esmentada norma en la seua Exposició de Motius (apartat III) que "en l'entorn actual, la tramitació electrònica no pot ser encara una forma especial de gestió dels procediments sinó que ha de constituir l'actuació habitual de les administracions. Perquè una administració sense paper basada en un funcionament íntegrament electrònic no solament serveix millor als principis d'eficàcia i eficiència, en estalviar costos a ciutadans i empreses, sinó que també reforça les garanties dels interessats. En efecte, la constància de documents i actuacions en un arxiu electrònic facilita el compliment de les obligacions de transparència, perquè permet oferir informació puntual, àgil i actualitzada als interessats".

Vista la propuesta que formula el vicerrector de Tecnologías de la Información de la Universidad, **el Consejo de Gobierno, reunido en sesión de 27 de junio de 2018, ACUERDA:**

Aprobar la Política de Seguridad de la Información de la Universidad Miguel Hernández de Elche, en los términos reflejados a continuación:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UMH

1. INTRODUCCIÓN

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (en adelante ENS), que en su artículo 11 establece la obligación para las administraciones públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

Asimismo, hay que tener presentes las previsiones de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En este sentido, destaca la citada norma en su Exposición de Motivos (apartado III) que "en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las administraciones. Porque una administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados. En efecto, la constancia de documentos y actuaciones en un archivo electrónico facilita el cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados".

Aquesta política de seguretat segueix també les indicacions de la guia CCN-STIC-805 del Centre Criptològic Nacional, centre adscrit al Centre Nacional d'Intel·ligència.

La finalitat de l'Esquema nacional de seguretat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeta als ciutadans i a les administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans.

La Universitat Miguel Hernández d'Elx, d'ara en avant UMH, depén dels sistemes TI (Tecnologies d'Informació) per a aconseguir els seus objectius institucionals. En conseqüència, aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguen afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

Per això, l'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TI han d'estar protegits contra amenaces de ràpida evolució i amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per a defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis.

Esta política de seguridad sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La Universidad Miguel Hernández de Elche, en adelante UMH, depende de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos institucionales. En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

Por ello, 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.

Los sistemas TI deben estar protegidos contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de 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.

Això implica que l'organització i el seu personal ha d'aplicar les mesures mínimes de seguretat que exigeix l'Esquema nacional de seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

L'organització s'ha de cerciorar que la seguretat TI és una part integral de cada etapa del cicle de vida del sistema, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació.

Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TI.

L'organització ha d'estar preparada per a previndre, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'ENS.

1.1. PREVENCIÓ

L'organització ha d'evitar, o almenys previndre en la mesura que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per a això s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos.
Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats. Per a garantir el compliment de la política, l'organització ha de:

Autoritzar els sistemes abans d'entrar en operació.

Esto implica que la organización y su personal debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La organización debe cerciorarse de que la seguridad TI 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 TI.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

1.1. PREVENCIÓN

La organización 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 se deben implementar las medidas mínimas de seguridad determinadas por el ENS, 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, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización debe:

Autorizar los sistemas antes de entrar en operación.

Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.
Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtindre una avaluació independent.

1.2. DETECCIÓ

Atés que els serveis es poden degradar ràpidament a causa d'incidents, s'ha de monitorar l'operació de manera continuada per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que estableix l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i report que arriben als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagen preestablit com a normals.

1.3. RESPOSTA

L'organització ha de:
- Establir mecanismes per a respondre eficaçment als incidents de seguretat.
- Designar punt de contacte per a les comunicacions respecte a incidents detectats en àrees de l'entitat o en altres organismes relacionats amb la UMH.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els equips de resposta a emergències (CERT) reconeguts en l'àmbit nacional com Iris-CERT o CCN-CERT.

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.

1.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3. RESPUESTA

La organización debe:
- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la UMH.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los equipos de respuesta a emergencias (CERT) reconocidos a nivel nacional como Iris-CERT o CCN-CERT.

1.4. RECUPERACIÓ

Per a garantir la disponibilitat dels serveis crítics, l'organització ha de desenvolupar plans de continuïtat dels sistemes TI com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

2. MISSIÓ

Segons es reflecteix en els seus estatuts, actualment en vigor, la Universitat Miguel Hernández és una entitat de dret públic, dotada de personalitat jurídica i patrimoni propi, que gaudeix d'autonomia, d'acord amb el que estableix la Constitució i les lleis, per a l'exercici del servei públic d'educació superior mitjançant l'estudi, la investigació, la docència, la transferència de coneixement a la societat i l'extensió universitària. Igualment, l'article 2 dels esmentats estatuts disposa que l'objectiu de la Universitat és promoure la creació i la transmissió crítica del coneixement a tots els nivells, sempre amb l'excel·lència com a guia de les seues actuacions i amb l'únic límit de la seua pròpia capacitat. Per a aconseguir aquest fi, el mateix article determina una sèrie d'objectius específics com, per exemple, la vinculació amb el seu entorn per a millorar les condicions de vida dels ciutadans als quals serveix, col·laborant en el seu desenvolupament socioeconòmic i cultural i en la qualitat mediambiental.

De forma estretament relacionada amb el compliment d'aquesta missió, l'organització desitja manifestar la necessitat d'una infraestructura TI que prevalga i fomente les operatives obertes, enfocades a la funcionalitat, connectivitat i servei a l'usuari, com a funcions prioritàries per a la consecució dels objectius estratègics i institucionals.

1.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la organización debe desarrollar planes de continuidad de los sistemas TI como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. MISIÓN

Según se refleja en sus estatutos, actualmente en vigor, la Universidad Miguel Hernández es una entidad de derecho público, dotada de personalidad jurídica y patrimonio propio, que goza de autonomía, de acuerdo con lo establecido en la Constitución y las leyes, para el ejercicio del servicio público de educación superior mediante el estudio, la investigación, la docencia, la transferencia de conocimiento a la sociedad y la extensión universitaria. Igualmente, el artículo 2 de los citados estatutos dispone que el objetivo de la Universidad es promover la creación y la transmisión crítica del conocimiento a todos los niveles, siempre con la excelencia como guía de sus actuaciones y con el único límite de su propia capacidad. Para lograr este fin, el mismo artículo determina una serie de objetivos específicos como, por ejemplo, la vinculación con su entorno para mejorar las condiciones de vida de los ciudadanos a los que sirve, colaborando en su desarrollo socio-económico y cultural y en la calidad medioambiental.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifestar la necesidad de una infraestructura TI que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

3. ABAST

Degut a la missió de l'entitat, reflectida en el punt 2 del present document, l'organització desestima l'aplicació de la present política de seguretat sobretot el conjunt del sistema d'informació.

Sobre la base d'això, l'organització aplicarà la present política sobre el gruix dels sistemes TI que gestiona de manera centralitzada a través dels Serveis Informàtics de la UMH i específicament sobre tots aquells sistemes que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu.

De forma concreta la present política de seguretat és aplicable sobre els següents serveis i els sistemes TI que els conformen:

- Sistema institucional

· gestió acadèmica
· gestió econòmica
· gestió personal
· gestió de la investigació
· campus virtual

- Sistema d'administració electrònica

· Seu electrònica

Addicionalment i encara entenent-se que els següents serveis no es troben directament en l'abast marcat per l'ENS, a causa de la seua importància en la comunitat universitària, s'acorda estendre l'abast al següent servei de la UMH:

- Sistema web institucional

3. ALCANCE

Debido a la misión de la entidad, reflejada en el punto 2 del presente documento, la organización desestima la aplicación de la presente política de seguridad sobre todo el conjunto del sistema de información.

En base a ello, la organización aplicará la presente política sobre el grueso de los sistemas TI que gestiona de manera centralizada a través de los Servicios Informáticos de la UMH y específicamente sobre todos aquellos sistemas que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

De forma concreta la presente política de seguridad es aplicable sobre los siguientes servicios y los sistemas TI que los conforman:

- Sistema institucional

· Gestión académica
· Gestión económica
· Gestión personal
· Gestión de la investigación
· Campus Virtual

- Sistema de administración electrónica

· Sede electrónica

Adicionalmente y aún entendiéndose que los siguientes servicios no se encuentran directamente en el alcance marcado por el ENS, debido a su importancia en la comunidad universitaria, se acuerda extender el alcance al siguiente servicio de la UMH:

- Sistema web institucional

4. MARC NORMATIU

Són aplicable les lleis i normatives espanyoles amb relació a protecció de dades personals, propietat intel·lectual i ús d'eines telemàtiques. Per tot això, la UMH podrà ser requerida pels òrgans administratius pertinents a proporcionar els registres electrònics o qualsevol altra informació relativa a l'ús dels sistemes d'informació.

Aquesta política se situa dins del marc jurídic definit per les lleis i reials decrets següents:

- **Llei orgànica 6/2001**, de 21 de desembre, d'universitats i **Llei orgànica 4/2007**, de 12 d'abril, per la qual es modifica la Llei orgànica 6/2001, de 21 de desembre, d'universitats.
- **DECRET 208/2004**, de 8 d'octubre, del Consell de la Generalitat, pel qual s'aproven els Estatuts de la Universitat Miguel Hernández d'Elx i **DECRET 105/2012**, de 29 de juny, del Consell, pel qual s'aprova la modificació dels Estatuts de la Universitat Miguel Hernández d'Elx
- **Reial decret 3/2010**, de 8 de gener, pel qual es regula l'Esquema nacional de seguretat en l'àmbit de l'administració electrònica i **Reial decret 951/2015**, de 23 d'octubre, de modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema nacional de seguretat en l'àmbit de l'administració electrònica.
- **Llei orgànica 15/1999**, de 13 de desembre, de protecció de dades de caràcter personal i **Reial decret 1720/2007**, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

- **Directiva (UE) 2016/680** del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció,

4. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas en relación a protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, la UMH podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y **Ley Orgánica 4/2007**, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- DECRETO 208/2004, de 8 de octubre, del Consell de la Generalitat, por el que se aprueban los Estatutos de la Universidad Miguel Hernández de Elche y **DECRETO 105/2012**, de 29 de junio, del Consell, por el que se aprueba la modificación de los Estatutos de la Universidad Miguel Hernández de Elche
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica y **Real Decreto 951/2015**, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y **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.
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención,

investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la qual es deroga la Decisió Marc 2008/977/JAI del Consell
- **Reglament (UE) 2016/679** del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).

- **Llei 34/2002**, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

- **Llei 39/2015**, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- I altres disposicions concordants i de desenvolupament de les esmentades anteriorment.

5. ORGANITZACIÓ DE LA SEGURETAT

5.1. COMITÉ: FUNCIONS I RESPONSABILITATS

Les funcions que indica el RD 3/2010 al Comité de Gestió de l'ENS, les assumeix l'actual **Comissió Tècnica de Seguretat TI**, d'ara en avant Comissió de Seguretat.

La Comissió de Seguretat estarà format per:
- El/la vicerector/a de Tecnologies de la Informació o el/la vicerector/a competent en la matèria
- El/la secretari/ària general
- El/la director/a dels Serveis Informàtics
- El/la cap de secció dels Serveis Informàtics

La Comissió de Seguretat nomenarà un secretari/ària que tindrà com a funcions les pròpies del càrrec.

investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo
- **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 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Y demás disposiciones concordantes y de desarrollo de las mencionadas anteriormente.

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

Las funciones indicadas en el RD 3/2010 al Comité de Gestión del ENS, las asume la actual **Comisión Técnica de Seguridad TI**, en adelante Comisión de Seguridad.

La Comisión de Seguridad estará formado por:
- El/la vicerrector/a de Tecnologías de la Información o el/la vicerrector/a competente en la materia
- El/la secretario/a general
- El/la director/a de los Servicios Informáticos
- El/la jefe/a de sección de los Servicios Informáticos

La Comisión de Seguridad nombrará un secretario/a que tendrá como funciones las propias del cargo.

La Comissió de Seguretat tindrà informat al Consell de Direcció.
Les funcions de la Comissió de Seguretat en relació a l'ENS són:
- Divulgació de la política i normativa de seguretat de l'organització.
- Aprovació de la normativa de seguretat de l'organització.
- Revisió anual de la política de seguretat.
- Desenvolupament del procediment de designació de rols.
- Designació de rols i responsabilitats.
- Supervisió i aprovació de les tasques de seguiment de l'Esquema nacional de seguretat:

· Tasques d'adequació
· Anàlisi de riscos
· Auditoria biennal

5.2. ROLS: FUNCIONS I RESPONSABILITATS
Responsable dels serveis TI

El/la **vicerector/a de TI** tindrà el rol de responsable dels serveis TI de l'organització. Té les funcions següents:

- Establiment dels requisits dels serveis TI en matèria de seguretat.
- Treball en col·laboració amb el/la responsable de seguretat i el/la responsable de sistema en el manteniment dels sistemes catalogats segons l'annex I de l'Esquema nacional de seguretat.

Responsable de la informació
El/la **secretari/ària general** tindrà el rol de responsable de la informació de l'organització. Té les funcions següents:

La Comisión de Seguridad tendrá informado al Consejo de Dirección.
Las funciones de la Comisión de Seguridad en relación al ENS son:
- Divulgación de la política y normativa de seguridad de la organización.
- Aprobación de la normativa de seguridad de la Organización.
- Revisión anual de la política de seguridad.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
· Tareas de adecuación
· Análisis de riesgos
· Auditoría bienal

5.2. ROLES: FUNCIONES Y RESPONSABILIDADES
Responsable de los servicios TI

El/la **vicerrector/a de TI** tendrá el rol de responsable de los servicios TI de la organización. Teniendo por funciones las siguientes:

- Establecimiento de los requisitos de los servicios TI en materia de seguridad.
- Trabajo en colaboración con el/la responsable de seguridad y el/la responsable de sistema en el mantenimiento de los sistemas catalogados según el anexo I del Esquema Nacional de Seguridad.

Responsable de la información
El/la **secretario/a general** tendrá el rol de responsable de la información de la organización. Teniendo por funciones las siguientes:

- Establiment dels requisits de la informació en matèria de seguretat.
- Treball en col·laboració amb el responsable de seguretat i el de sistema en el manteniment dels sistemes catalogats segons l'annex I de l'Esquema nacional de seguretat.

Responsable de seguretat

El/la **director/a dels Serveis Informàtics** tindrà el rol de responsable de seguretat de l'organització. Tenint les funcions següents:

- Mantindre la seguretat de la informació manejada i dels serveis prestats pels sistemes TI en el seu àmbit de responsabilitat.
- Realitzar o promoure les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació dels Serveis Informàtics dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establides són adequades per a la protecció de la informació manejada i els serveis prestats.

- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat del sistema.
- Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria implementats en el sistema.
- Donar suport i supervisar la investigació dels incidents de seguretat des de la seua notificació fins a la seua resolució.
- Elaborar l'informe periòdic de seguretat per al propietari del sistema, incloent els incidents més rellevants del període.
- Aprovació dels procediments de seguretat elaborats pel responsable del sistema.
- Elaboració de la normativa de seguretat de l'entitat.

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y el de sistema en el mantenimiento de los sistemas catalogados según el anexo I del Esquema Nacional de Seguridad.

Responsable de seguridad

El/la **director/a de los Servicios Informáticos** tendrá el rol de responsable de seguridad de la organización. Teniendo por funciones las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TI en su ámbito de responsabilidad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación de los Servicios Informáticos dentro de su ámbito de responsabilidad.
- 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 en el sistema.
- 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.
- Aprobación de los procedimientos de seguridad elaborados por el responsable del sistema.

- Elaboració de la normativa de seguretat de l'entitat.

Responsable del Sistema TI
El/la **cap de secció dels Serveis Informàtics** tindrà el rol de responsable del sistema de l'organització. Té les funcions, dins de les seues àrees d'actuació, següents:

- Desenvolupar, operar i mantindre del Sistema durant tot el seu cicle de vida, de les seues especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i política de gestió del Sistema establint els criteris d'ús i els serveis disponibles en aquest.
- Definir la política de connexió o desconnexió d'equips i usuaris nous en el Sistema.
- Aprovar els canvis que afecten la seguretat de la manera d'operació del Sistema.
- Decidir les mesures de seguretat que aplicaran els subministradors de components del Sistema durant les etapes de desenvolupament, instal·lació i prova d'aquest.
- Implantar i controlar les mesures específiques de seguretat del Sistema i cerciorar-se que aquestes s'integren adequadament dins del marc general de seguretat.
- Determinar la configuració autoritzada de maquinari i programari a utilitzar en el Sistema.
- Aprovar tota modificació substancial de la configuració de qualsevol element del Sistema.

- Dur a terme el preceptiu procés d'anàlisi i gestió de riscos en el Sistema.
- Determinar la categoria del sistema segons el procediment que descriu l'annex I de l'ENS i determinar les mesures de seguretat que s'han d'aplicar segons descriu l'annex II de l'ENS.

- Elaborar i aprovar la documentació de seguretat del Sistema.

- Elaboración de la normativa de seguridad de la entidad.

Responsable del Sistema TI
El/la **jefe/a de sección de los Servicios Informáticos** tendrá el rol de responsable del sistema de la organización. Teniendo por funciones, dentro de sus áreas de actuación, las siguientes:
- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del 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 toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y 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.
- Elaborar y aprobar la documentación de seguridad del Sistema.

- Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del Sistema.

- Vetlar pel compliment de les obligacions de l'Administrador de Seguretat del Sistema (ASS).
- Investigar els incidents de seguretat que afecten el Sistema, i si escau, comunicació al responsable de Seguretat o a qui aquest determine.
- Establir plans de contingència i emergència, duent a terme freqüents exercicis perquè el personal s'hi familiaritze.

- A més, el responsable del Sistema pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que pogueren afectar la satisfacció dels requisits establits. Aquesta decisió ha de ser acordada amb els responsables de la informació afectada, del servei afectat i el responsable de seguretat, abans de ser executada.

- Elaboració dels procediments de seguretat necessaris per a l'operativa en el sistema.

5.3. POLÍTICA DE SEGURETAT

Serà missió de la Comissió de Seguretat la revisió anual d'aquesta Política de seguretat de la informació i la proposta de revisió o manteniment d'aquesta. La Política serà aprovada pel Consell de Govern i difosa perquè la coneguen totes les parts afectades.

6. DADES DE CARÀCTER PERSONAL

Tots els sistemes d'informació de la UMH s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal que recull l'esmentat document de seguretat.

- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación 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.
- Además, el responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

5.3. POLÍTICA DE SEGURIDAD

Será misión de la Comisión de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

6. DATOS DE CARÁCTER PERSONAL

Todos los sistemas de información de la UMH se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado documento de seguridad.

7. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada cada dos anys
- Quan canvie la informació manejada
- Quan canvien els serveis prestats
- Quan ocórrega un incident greu de seguretat
- Quan es reporten vulnerabilitats greus

Per a l'harmonització de les anàlisis de riscos, la Comissió de Seguretat establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

La Comissió de Seguretat dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

8. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT

Aquesta política es desenvoluparà per mitjà de normativa de seguretat que afronte aspectes específics. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible en el lloc web de la Seu de la Universitat.

7. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez cada dos años
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, la Comisión de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

La Comisión de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el sitio web de la Sede de la Universidad.

9. OBLIGACIONS DEL PERSONAL

Tots els membres de la UMH tenen l'obligació de conéixer i complir aquesta política de seguretat de la informació i la Normativa de seguretat desenvolupada a partir d'aquesta, i és responsabilitat de la Comissió de Seguretat disposar els mitjans necessaris perquè la informació arribe els afectats, tenint en compte sempre les disponibilitats pressupostàries de la UMH.

S'establirà un programa d'accions en conscienciació contínua per a atendre tots els membres de la UMH, en particular els de nova incorporació, tenint en compte sempre les disponibilitats pressupostàries de la UMH.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TI rebran formació per al maneig segur dels sistemes en la mesura en què la necessiten per a realitzar el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seua primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

10. TERCERES PARTS

Quan la UMH preste serveis a altres organismes o manege informació d'altres organismes, se'ls farà partícips d'aquesta Política de seguretat de la informació, s'establiran canals per a report i coordinació dels respectius Comités de Seguretat TI i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de la UMH tienen la obligación de conocer y cumplir esta política de seguridad de la información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad de la Comisión de Seguridad disponer los medios necesarios para que la información llegue a los afectados, teniendo en cuenta siempre las disponibilidades presupuestarias de la UMH.

Se establecerá un programa de acciones en concienciación continua para atender a todos los miembros de la UMH, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de la UMH.

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

10. TERCERAS PARTES

Cuando la UMH 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 TI y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Quan la UMH utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la Normativa de seguretat que concernisca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions que estableix aquesta normativa, i podrà desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de report i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que el que estableix aquesta política. Quan algun aspecte de la Política no puga ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del responsable de Seguretat que precise els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir avant.

11. ENTRADA EN VIGOR

La present política de seguretat de la Informació entrarà en vigor l'endemà de la seua publicació en el *Butlletí Oficial de la Universitat Miguel Hernández* (BOUMH), amb l'aprovació prèvia pel Consell de Govern, i fins que siga reemplaçada per una nova Política.

Queda derogada l'anterior Política de seguretat de les tecnologies de la informació i les comunicacions de la Universitat Miguel Hernández, que va ser aprovada pel Consell de Govern, reunit en la sessió de 28 de setembre de 2016.

Cuando la UMH utilice servicios de terceros o ceda información a terceros, se les hará partícipes 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.

11. ENTRADA EN VIGOR

La presente política de seguridad de la Información entrará en vigor al día siguiente de su publicación en el *Boletín Oficial de la Universidad Miguel Hernández* (BOUMH), previa aprobación por el Consejo de Gobierno, y hasta que sea reemplazada por una nueva Política.

Queda derogada la anterior Política de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad Miguel Hernández, que fue aprobada por el Consejo de Gobierno, reunido en sesión de 28 de septiembre de 2016.