COGO2022/04.109

UNIVERSITAS Miguel Hernández

SECRETARIA GENERAL

NOTIFICACIÓ D'ACORD

Acord d'aprovació de la Normativa de seguretat en servidors de la Universitat Miguel Hernández

La conscienciació, el sentit comú i les bones pràctiques són les millors defenses per a previndre i detectar contratemps en la utilització de sistemes de les tecnologies de la informació i la comunicació (TIC).

Es pot dir que no hi ha un sistema que garantisca al 100 % la seguretat del servei que presta i la informació que maneja a causa, en gran mesura, de les vulnerabilitats que presenten les tecnologies i, el que és més important, la impossibilitat de disposar dels suficients recursos per a fer-hi front. Per tant, sempre cal acceptar un risc; el conegut com a risc residual, assumint un compromís entre el nivell de seguretat, els recursos disponibles i la funcionalitat desitjada.

La present normativa té per objecte regular les condicions d'ús dels servidors connectats a la xarxa de la UMH intentant garantir el nivell de seguretat requerit en tots els recursos connectats a la xarxa UMH i minimitzant el risc residual en el servei. En concret es pretén definir un marc institucional de seguretat dels servidors connectats a la xarxa de la UMH, la supervisió del compliment de les obligacions de seguretat dels administradors de servidors i la gestió dels incidents de seguretat que s'hi produïsquen.

I vista la proposta que formula el vicerector de Tecnologies de la Informació d'aquesta universitat, **el Consell de Govern, reunit en la sessió extraordinària de 12 d'abril de 2022, ACORDA per unanimitat:**

Aprovar la Normativa de seguretat en servidors de la Universitat Miguel Hernández d'Elx, en els termes reflectits a continuació:

NOTIFICACIÓN DE ACUERDO

Acuerdo de aprobación de la Normativa de Seguridad en Servidores de la Universidad Miguel Hernández

La concienciación, el sentido común y las buenas prácticas son las mejores defensas para prevenir y detectar contratiempos en la utilización de sistemas de las Tecnologías de la Información y la Comunicación (TIC).

Se puede decir que no existe un Sistema que garantice al 100 % la seguridad del servicio que presta y la información que maneja debido, en gran medida, a las vulnerabilidades que presentan las tecnologías y lo que es más importante, la imposibilidad de disponer de los suficientes recursos para hacerlas frente. Por tanto, siempre hay que aceptar un riesgo; el conocido como riesgo residual, asumiendo un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada.

La presente normativa tiene por objeto regular las condiciones de uso de los servidores conectados a la red de la UMH intentando garantizar el nivel de seguridad requerido en todos los recursos conectados a la red UMH y minimizando el riesgo residual en el servicio. En concreto se pretende definir un marco institucional de seguridad de los servidores conectados a la red de la UMH, la supervisión del cumplimiento de las obligaciones de seguridad de los administradores de servidores y la gestión de los incidentes de seguridad que se produzcan en los mismos.

Y vista la propuesta que formula el vicerrector de Tecnologías de la Información de esta universidad, **el Consejo de Gobierno, reunido en sesión extraordinaria de 12 de abril de 2022, ACUERDA por unanimidad:**

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

UNIVERSITAS Miguel Hernández

SECRETARIA GENERAL

NORMATIVA DE SEGURETAT EN SERVIDORS DE LA UNIVERSITAT MIGUEL HERNÁNDEZ

PREÀMBUL

La conscienciació, el sentit comú i les bones pràctiques són les millors defenses per a previndre i detectar contratemps en la utilització de sistemes de les tecnologies de la informació i la comunicació (TIC).

Es pot dir que no hi ha un sistema que garantisca al 100 % la seguretat del servei que presta i la informació que maneja a causa, en gran mesura, de les vulnerabilitats que presenten les tecnologies i, el que és més important, la impossibilitat de disposar dels suficients recursos per a fer-hi front. Per tant, sempre cal acceptar un risc; el conegut com a risc residual, assumint un compromís entre el nivell de seguretat, els recursos disponibles i la funcionalitat desitjada.

La present normativa té per objecte regular les condicions d'ús dels servidors connectats a la xarxa de la UMH intentant garantir el nivell de seguretat requerit en tots els recursos connectats a la xarxa UMH i minimitzant el risc residual en el servei. En concret es pretén definir un marc institucional de seguretat dels servidors connectats a la xarxa de la UMH, la supervisió del compliment de les obligacions de seguretat dels administradors de servidors i la gestió dels incidents de seguretat que s'hi produïsquen.

1. OBJECTE I ÀMBIT D'APLICACIÓ

La present normativa pretén definir els requisits mínims de seguretat que han de complir tots els servidors connectats a la xarxa de la Universitat Miguel Hernández (d'ara en avant UMH).

Aquesta normativa és aplicable i de compliment obligat per a tots els usuaris que administren un servidor connectat a la xarxa de la Universitat Miguel Hernández.

NORMATIVA DE SEGURIDAD EN SERVIDORES DE LA UNIVERSIDAD MIGUEL HERNÁNDEZ

PREÁMBULO

La concienciación, el sentido común y las buenas prácticas son las mejores defensas para prevenir y detectar contratiempos en la utilización de sistemas de las Tecnologías de la Información y la Comunicación (TIC).

Se puede decir que no existe un Sistema que garantice al 100% la seguridad del servicio que presta y la información que maneja debido, en gran medida, a las vulnerabilidades que presentan las tecnologías y lo que es más importante, la imposibilidad de disponer de los suficientes recursos para hacerlas frente. Por tanto, siempre hay que aceptar un riesgo; el conocido como riesgo residual, asumiendo un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada.

La presente normativa tiene por objeto regular las condiciones de uso de los servidores conectados a la red de la UMH intentando garantizar el nivel de seguridad requerido en todos los recursos conectados a la red UMH y minimizando el riesgo residual en el servicio. En concreto se pretende definir un marco institucional de seguridad de los servidores conectados a la red de la UMH, la supervisión del cumplimiento de las obligaciones de seguridad de los administradores de servidores y la gestión de los incidentes de seguridad que se produzcan en los mismos.

1. OBJETO Y ÁMBITO DE APLICACIÓN

La presente normativa pretende definir los requisitos mínimos de seguridad que deben cumplir todos los servidores conectados a la red de la Universidad Miguel Hernández (en adelante UMH).

Esta normativa será de aplicación y de obligado cumplimiento para todos los usuarios que administren un servidor conectado a la red de la Universidad Miguel Hernández.

UNIVERSITAS Miguel Hernández

SECRETARIA GENERAL

2. MARC NORMATIU

Són aplicables les lleis i normatives espanyoles, així com les que dimanen de la Unió Europea i de la Generalitat Valenciana en relació amb protecció de dades personals, propietat intel·lectual i ús d'eines telemàtiques, així com les que puguen aparéixer, en un futur, referent a això.

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

- Reial decret 3/2010, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica modificat pel RD 951/2015 de 23 d'octubre.
- REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL 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 orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Acord d'aprovació del Consell de Govern de 27 d'octubre de 2021 de la modificació de la política de seguretat de la informació de la Universitat Miguel Hernández.

3. DEFINICIONS

3.1. SERVIDOR

Un servidor és una unitat informàtica que proporciona diversos serveis a computadors que s'hi connecten a través d'una xarxa.

3.2. SISTEMA OPERATIU (SO)

Programa o conjunt de programes que realitzen funcions bàsiques i permeten el desenvolupament d'altres programes.

3.3. PROGRAMA

Conjunt unitari d'instruccions que permet a una computadora realitzar funcions diverses, com el tractament de textos, el disseny de gràfics, la resolució de problemes matemàtics, el maneig

2. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas, así como las que dimanan de la Unión Europea y de la Generalitat Valenciana en relación con protección de datos personales, propiedad intelectual y uso de herramientas telemáticas, así como las que puedan aparecer, en un futuro, a este respecto.

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

- Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica modificado por el RD 951/2015 de 23 de octubre.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Acuerdo de aprobación del Consejo de Gobierno de 27 de octubre de 2021 de la modificación de la Política de Seguridad de la Información de la Universidad Miguel Hernández.

3. DEFINICIONES

3.1. SERVIDOR

Un servidor es una unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red.

3.2. SISTEMA OPERATIVO (SO)

Programa o conjunto de programas que realizan funciones básicas y permiten el desarrollo de otros programas.

3.3. PROGRAMA

Conjunto unitario de instrucciones que permite a una computadora realizar funciones diversas, como el tratamiento de textos, el diseño de gráficos, la resolución de problemas

de bancs de dades, etc.

3.4. APLICACIÓ

Programa preparat per a una utilització específica, com el pagament de nòmines, el tractament de textos, etc.

3.5. COMISSIÓ TÈCNICA DE SEGURETAT TI DE LA UMH

La Comissió Tècnica de Seguretat TI de la Universitat Miguel Hernández és l'òrgan assessor del Consell de Direcció de la UMH en matèria de gestió de ciberseguretat de la UMH que assumeix les funcions indicades en el RD 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

3.6. RESPONSABLE DE SEGURETAT DE SERVIDOR

És la persona encarregada de l'administració d'un servidor, de l'actualització del seu sistema operatiu i dels seus programes o aplicacions instal·lades, i qui haurà d'executar la presenta normativa, així com la política de seguretat de la UMH, la Normativa general d'ús dels recursos i sistemes de la informació de la UMH, o qualsevol altra normativa o protocol aprovada per la Comissió Tècnica de Seguretat TI de la UMH.

4. ALTA DE SERVIDOR

Per a instal·lar un nou servidor connectat a la xarxa de la UMH, el seu responsable ha de fer una sol·licitud a través del formulari web indicant les dades tècniques necessàries per a la seua alta pel Servei d'Innovació i Planificació Tecnològica amb acceptació expressa de les normatives vigents.

4.1. RESPONSABLES DE SEGURETAT DE SERVIDORS UMH

El responsable de seguretat del servidor s'encarregarà de supervisar el servidor complint les normes detallades en aquesta normativa mentre el servidor estiga connectat a la xarxa de la UMH, així com totes les altres mesures que considere necessàries per a la seua correcta protecció i serà el responsable directe de

matemáticos, el manejo de bancos de datos, etc.

3.4. APLICACIÓN

Programa preparado para una utilización específica, como el pago de nóminas, el tratamiento de textos, etc.

3.5. COMISIÓN TÉCNICA DE SEGURIDAD TI DE LA UMH

La Comisión Técnica de Seguridad TI de la Universidad Miguel Hernández es el órgano asesor del Consejo de Dirección de la UMH en materia de gestión de ciberseguridad de la UMH que asume las funciones indicadas en el RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3.6. RESPONSABLE DE SEGURIDAD DE SERVIDOR

Es la persona encargada de la administración de un servidor, de la actualización de su sistema operativo y de sus programas o aplicaciones instaladas, y quien deberá dar cumpliendo a la presenta normativa, así como la Política de Seguridad de la UMH, la Normativa General de Uso de los Recursos y Sistemas de la Información de la UMH, o cualquier otra normativa o protocolo aprobada por la Comisión Técnica de Seguridad TI de la UMH.

4. ALTA DE SERVIDOR

Para instalar un nuevo servidor conectado a la red de la UMH, el responsable del mismo realizará una solicitud a través del formulario web indicando los datos técnicos necesarios para su alta por el Servicio de Innovación y Planificación Tecnológica con aceptación expresa de las normativas vigentes.

4.1. RESPONSABLES DE SEGURIDAD DE SERVIDORES UMH

El responsable de seguridad del servidor se encargará de supervisar el servidor cumpliendo las normas detalladas en esta normativa mientras el servidor esté conectado a la red de la UMH, así como todas las demás medidas que considere necesarias para su correcta protección. siendo el responsable directo de

qualsevol incident ocasionat per l'incompliment d'aquestes normes i dels problemes derivats que puguen afectar el mateix servidor i/o a altres servidors connectats a la xarxa de la UMH.
Qualsevol canvi del responsable d'un servidor es comunicarà al Servei d'Innovació i Planificació Tecnològica. No es podrà mantindre un servidor connectat a la xarxa de la UMH sense un responsable de servidor.

5. CONDICIONS D'ÚS

Els responsables de seguretat de servidors de la UMH han de preveure els següents requisits mínims de seguretat en la configuració dels seus servidors, si bé poden i han d'incorporar totes les mesures addicionals que consideren oportunes amb la finalitat de protegir la informació i els serveis que oferisca aquest servidor en funció del seu nivell de criticitat.

5.1. CONFIGURACION DE SEGURETAT

Es configuraran els servidors prèviament a la seua posada en marxa i connexió a la xarxa de la UMH, de manera que:

1. S'eliminen els comptes i les contrasenyes estàndard, tant de programes com del mateix SO.
2. Els privilegis de cada usuari es reduiran al mínim estrictament necessari per a complir les seues obligacions. D'aquesta manera es delimiten els danys que poguera causar a l'entitat, de manera accidental o intencionada.
3. Les contrasenyes aplicades compliran amb els requisits i les especificacions definits en la política de creació i ús de contrasenyes robustes en la UMH.
4. Tot el programari de seguretat (antivirus, microClaudia, etc.) subministrat per la universitat ha d'estar instal·lat i correctament configurat en el servidor.
5. S'aplicarà la regla de "mínima funcionalitat":

a. El sistema ha de proporcionar la funcionalitat requerida perquè l'usuari aconseguisca els seus objectius i cap altra funcionalitat.

b. No es proporcionaran funcions addicionals, ni d'operació, ni d'administració, ni

cualquier incidente ocasionado por el incumplimiento de estas normas y de los problemas derivados que puedan afectar al propio servidor y/o a otros servidores conectados a la red de la UMH.
Cualquier cambio del responsable de un servidor se comunicará al Servicio de Innovación y Planificación Tecnológica. No se podrá mantener un servidor conectado a la red de la UMH sin un responsable de servidor.

5. CONDICIONES DE USO

Los responsables de seguridad de servidores de la UMH deberán contemplar los siguientes requisitos mínimos de seguridad en la configuración de sus servidores, si bien, pueden y deben incorporar todas las medidas adicionales que consideren oportunas con el fin de proteger la información y los servicios que ofrezca dicho servidor en función del nivel de criticidad de los mismos.

5.1. CONFIGURACIÓN DE SEGURIDAD

Se configurarán los servidores previamente a su puesta en marcha y conexión a la red de la UMH, de forma que:

1. Se eliminen las cuentas y contraseñas estándar, tanto de programas como del propio SO.
2. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar a la entidad, de forma accidental o intencionada.
3. Las contraseñas aplicadas cumplirán con los requisitos y especificaciones definidos en la Política de creación y uso de contraseñas robustas en la UMH.
4. Todo el software de seguridad (antivirus, microClaudia, etc.) suministrado por la universidad debe estar instalado y correctamente configurado en el servidor.
5. Se aplicará la regla de "mínima funcionalidad":

a. El sistema debe proporcionar la funcionalidad requerida para que el usuario alcance sus objetivos y ninguna otra funcionalidad.

b. No se proporcionarán funciones adicionales, ni de operación, ni de administración, ni de

d'auditoria, que no s'utilitzen; d'aquesta manera es redueix el perímetre exposat al mínim imprescindible.
c. S'eliminaran o desactivaran, mitjançant el control de la configuració, aquells ports i funcions que no siguen d'interés, no calguen, i fins i tot, aquells que siguen inadequats per a la finalitat que es persegueix.
6. S'aplicarà la regla de "seguretat per defecte":
a. Les mesures de seguretat seran respectuoses amb l'usuari i el protegiran, llevat que s'expose conscientment a un risc.
b. Per a reduir la seguretat, l'usuari ha de realitzar accions conscients.
c. L'ús natural, en els casos que l'usuari no ha consultat el manual, serà un ús segur.
7. La connexió a les rosetes de xarxa es farà de manera individual, un servidor una roseta, i queda prohibida la connexió d'encaminadors o *switches* a aquestes o, si escau, ha de ser autoritzat prèviament pel Servei d'Infraestructura Informàtica.

5.2. ACTUALITZACIONS

Tot el programari instal·lat en el servidor ha d'estar sempre actualitzat a l'última versió i amb tots els pedaços de seguretat instal·lats. Això inclou el mateix SO i els programes i les aplicacions que tinga instal·lats.

5.3. CONEIXEMENTS DE SEGURETAT

El responsable de seguretat d'un servidor haurà de disposar de coneixements tècnics adequats a aquestes funcions i acreditar, com a mínim, la superació dels cursos bàsics de ciberseguretat del CCN-CERT, proposats per la Comissió de Seguretat de la UMH, per a verificar que posseeixen coneixements mínims de seguretat informàtica i administració.

5.4. GESTIÓ D'INCIDENTS

Sota l'autorització del responsable de Seguretat de la UMH, i en cas que es detecte una amenaça o es tinguen indicis que la seguretat del servidor o de la xarxa de la UMH s'ha vist compromesa, els tècnics administradors de la xarxa de la UMH podran operar, bloquejar i aïllar de la xarxa UMH qualsevol servidor. Es notificarà els responsables del servidor i es

auditoría, que no vayan a ser utilizadas, reduciendo de esta forma su perímetro expuesto al mínimo imprescindible.
c. Se eliminará o desactivará mediante el control de la configuración, aquellos puertos y funciones que no sean de interés, no sean necesarios, e incluso, aquellos que sean inadecuados al fin que se persigue.
6. Se aplicará la regla de "seguridad por defecto":
a. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
b. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
c. El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.
7. La conexión a las rosetas de red se hará de forma individual, un servidor una roseta, quedando prohibida la conexión de routers o switches a éstas, o en su caso, debe ser autorizado previamente por el Servicio de Infraestructura Informática.

5.2. ACTUALIZACIONES

Todo el software instalado en el servidor deberá estar siempre actualizado a la última versión y con todos los parches de seguridad instalados. Esto incluye el propio SO y los programas y aplicaciones que tenga instalados.

5.3. CONOCIMIENTOS DE SEGURIDAD

El responsable de seguridad de un servidor deberá disponer de conocimientos técnicos adecuados a estas funciones y acreditar, como mínimo, la superación de los cursos básico de ciberseguridad del CCN-CERT, propuestos por la Comisión de Seguridad de la UMH, para verificar que poseen conocimientos mínimos de seguridad informática y administración.

5.4. GESTIÓN DE INCIDENTES

Bajo la autorización del Responsable de Seguridad de la UMH, y en caso de que se detecte una amenaza o se tengan indicios de que la seguridad del servidor o de la red de la UMH se ha visto comprometida, los técnicos administradores de la red de la UMH podrán operar, bloquear y aislar de la red UMH a cualquier servidor. Se notificará a los

prendran les mesures oportunes abans de tornar a connectar el servidor a la xarxa de manera segura i així previndre que es repetisca l'incident.
En cas que el responsable de seguretat del servidor detecte un incident de seguretat, ho haurà de comunicar immediatament al Centre d'Atenció a l'Usuari de la UMH, en https://cau.umh.es, i explicar-ne els detalls.

5.5. PROTECCIÓ DE DADES

El responsable de seguretat del servidor haurà de vigilar el compliment amb la normativa vigent en matèria de protecció de dades.

6. RESPONSABILITATS

Tots els usuaris vinculats a la UMH afectats per aquesta normativa són responsables de conéixer les directrius de la present normativa que afecten el desenvolupament de les seues funcions, així com les conseqüències en què pogueren incórrer en cas d'incompliment.

En cas que es produïsca desvinculació del responsable de seguretat d'un servidor amb l'organització, si no es comunica prèviament al CAU el canvi de responsable, el servidor es bloquejarà temporalment.

El responsable de seguretat d'un servidor serà l'encarregat de complir amb les normes que es detallen en aquest document durant tot el període de temps que el servidor estiga connectat a les xarxes de la UMH, així com totes les altres mesures que considere necessàries per a la seua correcta protecció, i aquest serà el responsable directe de qualsevol incident ocasionat per l'incompliment d'aquestes normes i els problemes derivats que puguen afectar el servidor mateix i/o a altres servidors connectats a la xarxa de la UMH.

DISPOSICIÓ ADDICIONAL PRIMERA

En tot allò referent a qualsevol assumpte o matèria no regulat o previst en el present reglament, cal ajustar-se al que disposen els Estatuts i altra normativa aprovada per la UMH i les normatives estatals o autonòmiques que corresponguen.

responsables del servidor y se tomarán las medidas oportunas antes de volver a conectar el servidor a la red de forma segura y así prevenir que se repita el incidente.
En caso de que el responsable de seguridad del servidor detecte un incidente de seguridad, deberá comunicarlo inmediatamente al Centro de Atención al Usuario de la UMH, en https://cau.umh.es, explicando los detalles del mismo.

5.5. PROTECCIÓN DE DATOS

El responsable de seguridad del servidor deberá vigilar del cumplimiento con la normativa vigente en materia de protección de datos.

6. RESPONSABILIDADES

Todos los usuarios vinculados a la UMH afectados por esta normativa son responsables de conocer las directrices de la presente normativa que afectan al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

En caso de que se produzca desvinculación del responsable de seguridad de un servidor con la organización, si no se comunica previamente al CAU el cambio de responsable, el servidor se bloqueará temporalmente.

El responsable de seguridad de un servidor será el encargado de cumplir con las normas que en este documento se detallan durante todo el periodo de tiempo que el servidor esté conectado a las redes de la UMH, así como todas las demás medidas que considere necesarias para su correcta protección, siendo éste el responsable directo de cualquier incidente ocasionado por el incumplimiento de estas normas y los problemas derivados que puedan afectar al propio servidor y/o a otros servidores conectados a la red de la UMH.

DISPOSICIÓN ADICIONAL PRIMERA

En todo lo referente a cualquier asunto o materia no regulado o contemplado en el presente reglamento, se estará a lo dispuesto en los Estatutos y demás normativa aprobada por la UMH y las normativa estatales o autonómicas que correspondan.

UNIVERSITAS Miguel Hernández

SECRETARIA GENERAL

DISPOSICIÓ ADDICIONAL SEGONA

En aplicació de la Llei orgànica 3/2007, de 22 de març, per a la igualtat efectiva de dones i homes, així com la Llei 9/2003, de 2 d'abril, de la Generalitat, per a la igualtat entre dones i homes, tota referència a persones, col·lectius o càrrecs acadèmics, el gènere dels quals siga masculí, està fent referència al gènere gramatical neutre; inclou, per tant, la possibilitat de referir-se tant a dones com homes.

DISPOSICIÓ FINAL

La present normativa entra en vigor l'endemà de la 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 normativa.

Fet que comunique perquè en prengueu coneixement i tinga els efectes que pertoquen.

DISPOSICIÓN ADICIONAL SEGUNDA

En aplicación de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, así como la Ley 9/2003, de 2 de abril, de la Generalitat, para la igualdad entre mujeres y hombres, toda referencia a personas, colectivos o cargos académicos, cuyo género sea masculino, estará haciendo referencia al género gramatical neutro; incluyendo, por tanto, la posibilidad de referirse tanto a mujeres como hombres.

DISPOSICIÓN FINAL

La presente normativa 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 Normativa.

Lo que comunico para su conocimiento y efectos oportunos.

Signat electrònicament per:/Firmado electrónicamente por:
M. Mercedes Sánchez Castillo
SECRETÀRIA GENERAL

Edificio Rectorado y Consejo Social
Campus de Elche. Avda. de la Universidad s/n – 03202 Elche
c. electrónico: secretaria.general@umh.es