COGO2026/02.041

NOTIFICACIÓ D'ACORD DEL CONSELL DE GOVERN

Acord d'aprovació de la modificació integral de la Política de seguretat de la informació de la Universitat Miguel Hernández d'Elx

Vist l'informe d'auditoria de la Sindicatura de Comptes relatiu a la governança de les TI i la ciberseguretat, i amb l'objectiu d'esmenar les deficiències observades en la Política de seguretat de la informació de la UMH, es proposa modificar-la, i substituir l'última Política de seguretat de la informació de la Universitat Miguel Hernández, aprovada en Consell de Govern el 24 de març de 2021 (COGO2021/11.246);

Els canvis més rellevants són:

- Canvi del responsable de seguretat que deixa de ser una persona per a ser el Comité de Seguretat TI, que és un òrgan col·legiat.
- Canvi del responsable del sistema.
- Creació de l'oficina de seguretat TI.
- Actualització normativa

I vista la proposta que formula el vicerector d'Infraestructures, **el Consell de Govern, reunit en la sessió ordinària de 25 de febrer de 2026, ACORDA per unanimitat:**

Aprovar la modificació integral de la Política de seguretat de la informació de la UMH, en els termes reflectits a continuació:

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE LA UMH

ÍNDEX

NOTIFICACIÓN DE ACUERDO DEL CONSEJO DE GOBIERNO

Acuerdo de aprobación de la modificación integral de la Política de Seguridad de la Información de la Universidad Miguel Hernández de Elche

A la vista del Informe de Auditoría de la Sindicatura de Comptes relativo a la gobernanza de las TI y la ciberseguridad, y con el objetivo de subsanar las deficiencias observadas en la Política de Seguridad de la Información de la UMH, se propone la modificación de la misma, sustituyendo a la última Política de Seguridad de la Información de la Universidad Miguel Hernández, aprobada en Consejo de Gobierno el 24 de marzo de 2021 (COGO2021/11.246);

Los cambios más relevantes son:

- Cambio del responsable de seguridad que deja de ser una persona para ser el propio Comité de Seguridad TI, que es un órgano colegiado.
- Cambio del responsable del sistema.
- Creación de la oficina de seguridad TI.
- Actualización normativa

Y vista la propuesta que formula el vicerrector de Infraestructuras, **el Consejo de Gobierno, reunido en sesión ordinaria de 25 de febrero de 2026, ACUERDA por unanimidad:**

Aprobar la modificación integral de la Política de Seguridad de la Información de la UMH, en los términos reflejados a continuación:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UMH

ÍNDICE

1. INTRODUCCIÓ

La Política de seguretat de la informació s'elabora en compliment de l'exigència del Reial decret 311/2022, de 3 de maig, 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 12 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 present el que preveu la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques. En aquest sentit, la norma esmentada destaca en l'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

1. INTRODUCCIÓN

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS), que en su artículo 12 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

administracions. Perquè una Administració sense paper basada en un funcionament íntegrament electrònic no només serveix millor als principis d'eficàcia i eficiència, en estalviar costos a ciutadans i a 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, ja que permet oferir informació puntual, àgil i actualitzada als interessats".

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 exercir els drets i complir els deures a través d'aquests mitjans.

La Universitat Miguel Hernández d'Elx, d'ara en avant UMH, depén dels sistemes TI (tecnologies de la informació) per a assolir els seus objectius institucionals. En conseqüència, aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los davant 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 ràpidament 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.

Això implica que l'organització i el seu personal han

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".

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 la 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.

Esto implica que la organización y su personal deben

d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer 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 concepció fins a la 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 i respondre davant d'incidents, així com garantir la conservació de les dades i la informació, d'acord amb l'article 8 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.
- Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de manera 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 10 de l'ENS.

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 y responder ante incidentes, así como garantizar la conservación de los datos y la información, de acuerdo al artículo 8 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.
- 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 10 del ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 de l'ENS. Cal establir mecanismes de detecció, anàlisi i report que arriben als responsables regularment i quan es produïsca 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 un 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 els dos sentits, amb els equips de resposta a emergències (CERT) reconeguts en l'àmbit nacional com IRIS-CERT o CCN-CERT.

1.4. Recuperació

Per a garantir la disponibilitat dels serveis crítics, l'organització ha de disposar dels mitjans i les tècniques necessaris que permeten garantir la recuperació dels serveis més crítics.

2. MISSIÓ

Segons es reflecteix en els seus estatuts, actualment en vigor, la UMH és una entitat de dret públic, dotada de personalitat jurídica i patrimoni propi, que gaudeix d'autonomia, d'acord amb el que estableixen 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 estatuts esmentats 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 acomplir amb aquesta finalitat, 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 manera estretament relacionada amb el compliment d'aquesta missió, l'organització posa a la

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca 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 un 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. Recuperación

Para garantizar la disponibilidad de los servicios críticos, la organización debe disponer de los medios y técnicas necesarias que permitan garantizar la recuperación de los servicios más críticos.

2. MISIÓN

Según se refleja en sus estatutos, actualmente en vigor, la UMH 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 pone a

disposició de la ciutadania la realització de tràmits en línia i noves vies de participació que garantisquen el desenvolupament i l'eficàcia de les seues funcions i comeses.

En potenciar l'ús de les noves tecnologies en la UMH, es persegueix fomentar la relació electrònica de tots els actors (docents, estudiants, personal investigador, personal d'administració i serveis, i d'altres) amb la Universitat.

3. PRINCIPIS BÀSICS

Els principis bàsics són directrius fonamentals de seguretat que s'han de tindre sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació. S'estableixen els següents:

- Abast estratègic: La seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells directius de la Universitat, de manera que puga estar coordinada i integrada amb la resta d'iniciatives estratègiques de l'organització per a conformar un tot coherent i eficaç.
- Responsabilitat determinada: En els sistemes TI es determina:
  - Responsable de la informació, que determina els requisits de seguretat de la informació tractada.
  - Responsable del servei, que determina els requisits de seguretat dels serveis prestats.
  - Responsable del sistema, que té la responsabilitat sobre la prestació dels serveis.
  - Responsable de la seguretat, que determina les decisions per a satisfer els requisits de seguretat.
- Seguretat integral: La seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes TI, que ha de procurar evitar qualsevol actuació puntual o tractament conjuntural. Cal considerar la seguretat de la informació com a part de l'operativa habitual, per això ha d'estar present i aplicar-se des del disseny inicial dels sistemes TI.
- Gestió de riscos: L'anàlisi i gestió de riscos és part essencial del procés de seguretat. La gestió de riscos permet el manteniment d'un entorn controlat, que minimitza els riscos fins a nivells acceptables. Aquests nivells es redueixen mitjançant el desplegament de mesures de seguretat, que estableixen un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos als quals estiguen exposades i l'eficàcia i el cost de les mesures de seguretat. A l'hora d'avaluar el risc en relació amb la seguretat de les dades, s'han de tindre en compte els

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

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

3. PRINCIPIOS BÁSICOS

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

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- Responsabilidad determinada: En los sistemas TI se determinará:
  - Responsable de la Información, que determina los requisitos de seguridad de la información tratada.
  - Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados.
  - Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios.
  - Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TI, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TI.
- Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la

riscos que es deriven del tractament de les dades personals.

• Proporcionalitat: L'establiment de mesures de protecció, detecció i recuperació ha de ser proporcional als riscos potencials i a la criticitat i al valor de la informació i dels serveis afectats.
• Millora contínua: Les mesures de seguretat s'han de reavaluar i actualitzar periòdicament per a adequar-ne l'eficàcia a l'evolució constant dels riscos i els sistemes de protecció. La seguretat de la informació ha de ser atesa, revisada i auditada per personal qualificat, instruït i dedicat.
• Seguretat per defecte: Els sistemes s'han de dissenyar i configurar de manera que garantisquen un grau suficient de seguretat per defecte.

4. OBJECTIU DE LA SEGURETAT DE LA INFORMACIÓ

La UMH, estableix com a objectius de la seguretat de la informació els següents:

• Garantir la qualitat i protecció de la informació.

• Aconseguir la plena conscienciació dels usuaris respecte a la seguretat de la informació.
• Gestió d'actius d'informació: Els actius d'informació de la Universitat han d'estar inventariats i categoritzats i han d'estar associats a un responsable.
• Seguretat lligada a les persones: Cal implantar els mecanismes necessaris perquè qualsevol persona que accedisca o puga accedir als actius d'informació conega les seues responsabilitats i d'aquesta manera es reduïsca el risc derivat d'un ús indegut, i s'assolisca la plena conscienciació dels usuaris respecte a la seguretat de la informació.
• Seguretat física: Els actius d'informació s'han de situar en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat. Els sistemes i els actius d'informació que contenen aquestes àrees han d'estar prou protegits davant d'amenaces físiques o ambientals.
• Seguretat en la gestió de comunicacions i operacions: Cal establir els procediments necessaris per a assolir una gestió adequada de la seguretat, operació i actualització de les TI. La informació que es transmeta a través de xarxes de comunicacions ha de ser protegida adequadament, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que en garantisquen la seguretat.

• Control d'accés: Cal limitar l'accés als actius d'informació per part d'usuaris, processos i altres sistemes d'informació mitjançant la implantació dels

seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
• Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
• Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
• Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

4. OBJETIVO DE LA SEGURIDAD DE LA INFORMACIÓN

La UMH, establece como objetivos de la seguridad de la información los siguientes:

• Garantizar la calidad y protección de la información.
• Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
• Gestión de activos de información: Los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
• Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
• Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
• Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TI. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
• Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la

mecanismes d'identificació, autenticació i autorització segons la criticitat de cada actiu. A més, ha de quedar registrada la utilització del sistema a fi d'assegurar la traçabilitat de l'accés i auditar-ne l'ús adequat, conforme a l'activitat de l'organització.

- Adquisició, desenvolupament i manteniment dels sistemes d'informació: S'han de preveure els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, per tal de garantir-ne la seguretat per defecte.
- Gestió dels incidents de seguretat: Cal implantar els mecanismes apropiats per a identificar, registrar i resoldre correctament els incidents de seguretat.

- Garantir la prestació continuada dels serveis: Cal implantar els mecanismes apropiats per a assegurar la disponibilitat dels sistemes d'informació i mantindre la continuïtat dels seus processos de negoci, d'acord amb les necessitats de nivell de servei dels seus usuaris.
- Protecció de dades: Cal adoptar les mesures tècniques i organitzatives que corresponga implantar per a atendre els riscos generats pel tractament per a complir la legislació de seguretat i privacitat.

- Compliment: Cal adoptar les mesures tècniques, organitzatives i procedimentals necessàries per a complir la normativa legal vigent en matèria de seguretat de la informació.

5. ABAST

Aquesta política s'aplica als sistemes d'informació de la UMH relacionats amb l'exercici de les seues competències i a tots els usuaris amb accés autoritzat a aquests sistemes, siguen o no empleats públics i amb independència de la naturalesa de la seua relació jurídica amb la Universitat. Tots tenen l'obligació de conéixer i complir aquesta política de seguretat de la informació i la normativa de seguretat derivada, i és responsabilitat del Comité de Seguretat TI disposar els mitjans necessaris perquè la informació arribe al personal afectat.

6. MARC NORMATIU

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

implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

5. ALCANCE

Esta Política se aplicará a los sistemas de información de la UMH relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TI disponer los medios necesarios para que la información llegue al personal afectado.

6. 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.

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

- Llei orgànica 2/2023, de 22 de març, del sistema universitari (LOSU).

- 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 el 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 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció tècnica de seguretat de conformitat amb l'Esquema Nacional de Seguretat.

- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció tècnica de seguretat d'informe de l'estat de la seguretat.

- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat d'auditoria de la seguretat dels sistemes d'informació.

- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat de notificació d'incidents de seguretat.

- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

- 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).

Esta política se sitúa dentro del marco jurídico definido por las leyes y Reales Decretos siguientes:

- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU).

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

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

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

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

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

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

- 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).

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica.

- Reial decret 1308/1992, de 23 d'octubre, pel qual es declara el laboratori del Reial Institut i Observatori de l'Armada com a laboratori depositari del patró nacional de temps i laboratori associat al Centre Espanyol de Metrologia.

- Llei 57/2003, de 16 de desembre, de mesures per a la modernització del govern local.

- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.

- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.

- Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut bàsic de l'empleat públic.

- Reial decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.

- Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.

- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.

- Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.

- Reial decret llei 14/2019, de 31 d'octubre, pel

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

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

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

- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.

- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

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

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

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Real Decreto-ley 14/2019, de 31 de octubre, por

qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.

- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança en la matèria.

- Llei 11/2022, de 28 de juny, general de telecomunicacions, que transposa el Codi europeu de les comunicacions electròniques.

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

- Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local.

- 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, 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.

7. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ

7.1. Criteris utilitzats per a l'organització de la seguretat de la informació

La UMH, tenint en compte el que estableix l'avantdit Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS) i les pautes establides en la Guia CCN-STIC-801 sobre responsabilitats i funcions en l'ENS, per a organitzar la seguretat de la informació disposa de:

- Rols de seguretat: responsables dels serveis, responsables de la informació, responsable de la seguretat (RSEG), responsable del sistema (RSIS) i delegat o delegada de protecció de dades (DPD).

- Òrgan consultiu i estratègic per a la presa de decisions en matèria de seguretat de la informació. Aquest òrgan està constituït com un òrgan col·legiat i es denomina Comité de Seguretat TI. Està presidit per una persona física, que és la que assumeix la responsabilitat formal dels seus actes.

el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones, que transpone el Código Europeo de las Comunicaciones Electrónicas.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

- 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, 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.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. Criterios utilizados para la organización de la Seguridad de la Información

La UMH, teniendo en cuenta lo establecido en el antedicho Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS", para organizar la seguridad de la información dispone de:

- Roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad (RSEG), Responsable del Sistema (RSIS) y Delegado/a de Protección de Datos (DPD).

- Órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano está constituido como un órgano colegiado y se denomina Comité de Seguridad TI. Está presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2. Rols i òrgans de la seguretat de la informació

En la UMH, en el marc de l'ENS, els rols i òrgans de la seguretat de la informació, són els següents:

- Responsable de la informació: el secretari o la secretària general.

- Responsable del servei: el vicerector o la vicerectora amb competències en tecnologies de la informació.

- Responsable de seguretat de la informació: la figura està constituïda pel Comité de Seguretat TI (COMSEGTI)

- Responsable de sistema: El o la del Servei d'Innovació i Planificació Tecnològica (SIPT)

- Comité de Seguretat TI (COMSEGTI):
  - President: responsable del servei
  - Vocals:
  - Membres permanents:
    - Secretari o secretària del COMSEGTI: el secretari o la secretària general.
    - Responsable de sistema
    - Responsable de l'Oficina de Seguretat TI.
    - El delegat o la delegada de protecció de dades.
  - Membres no permanents:
    - El Comité de Seguretat TI pot invocar la presència en les seues reunions tant d'altres representants de la Universitat com d'especialistes externs, dels sectors públic, privat i/o acadèmic, la presència dels quals, per raó de la seua experiència o vinculació amb els assumptes tractats, siga necessària o aconsellable.

Els representants de la informació i els serveis són convocats per la presidència en funció dels assumptes que s'hi tracten, en representació dels diferents àmbits o àrees de seguretat TI de la Universitat. Cada àrea està representada per un vocal amb vot, sense perjudici que hi acudisquen diversos representants.

El delegat de protecció de dades participa amb veu però sense vot en les reunions del Comité de Seguretat de Tecnologies de la Informació quan s'hi aborden qüestions relacionades amb el tractament de dades de caràcter personal, així com sempre que se'n requerisca la participació. En tot cas, si un assumpte

7.2. Roles y Órganos de la Seguridad de la Información

En la UMH, en el marco del ENS, los roles y órganos de la Seguridad de la Información, serán los siguientes:

- Responsable de la Información: El/la secretario/a general

- Responsable del Servicio: El/la vicerrector/a con competencias en Tecnologías de la Información.

- Responsable de Seguridad de la Información: La figura estará constituida por el Comité de Seguridad TI (COMSEGTI)

- Responsable de sistema: El/la jefe/a del Servicio de Innovación y Planificación Tecnológica (SIPT)

- Comité de Seguridad TI (COMSEGTI):
  - Presidente: responsable del Servicio
  - Vocales:
  - Miembros permanentes:
    - Secretario/a del COMSEGTI: El/la secretario/a general.
    - Responsable de sistema
    - Responsable de la Oficina de Seguridad TI.
    - El/la delegado/a de protección de datos.
  - Miembros no permanentes:
    - El Comité de Seguridad TI podrá invocar la presencia en sus reuniones tanto de otros representantes de la universidad como de especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Los representantes de la información y los servicios serán convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de seguridad TI de la universidad. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de la misma.

El delegado de protección de datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo

se sotmetera a votació, es fa constar sempre en acta l'opinió del delegat de protecció de dades.

El secretari o la secretària del Comité convoca les reunions del Comité de Seguretat TI i n'estén les actes. A les sessions del Comité de Seguretat TI poden assistir en qualitat d'assessors les persones que en cada cas estime pertinents el president.

7.3. Responsabilitats dels rols associats a l'Esquema Nacional de Seguretat

7.3.1. Responsable de la informació i dels serveis

Són funcions dels responsables de la informació i dels serveis:

- Establir i elevar perquè els aprove el Comité de Seguretat TI els requisits de seguretat aplicables a la informació (nivells de seguretat de la informació) i als serveis (nivells de seguretat dels serveis), dins del marc establit en l'annex I del Reial decret ENS, se'n pot demanar una proposta al responsable de Seguretat i tenint en compte l'opinió del responsable del sistema.
- Dictaminar respecte als drets d'accés a la informació i els serveis.
- Acceptar els nivells de risc residual que afecten la informació i els serveis.
- Comunicar al responsable de seguretat qualsevol variació respecte a la informació i els serveis dels quals és responsable, especialment la incorporació de nous serveis o informació al seu càrrec.

7.3.2 Responsable de la seguretat de la informació (RSEG)

Tenint en compte que el rol de responsable de seguretat l'exerceix el Comité de Seguretat TI, en aquest punt es detallen les funcions específiques del COMSEGTI en la faceta de responsable de seguretat:

- Mantindre i verificar el nivell adequat de seguretat de la informació manejada i dels serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar els responsables de l'execució de l'anàlisi de riscos, de la declaració d'aplicabilitat, identificar les mesures de seguretat, determinar les configuracions necessàries, elaborar la documentació del sistema.
- Proporcionar assessorament per a la determinació

caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del delegado de protección de datos.

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

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

7.3.1. Responsable de la Información y de los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

- Establecer y elevar para su aprobación al Comité de Seguridad TI los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.

7.3.2 Responsable de la Seguridad de la Información (RSEG)

Teniendo en cuenta el rol Responsable de Seguridad lo desempeña el Comité de Seguridad TI, se relaciona en este punto las funciones específicas del COMSEGTI en su faceta de Responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la

de la categoria del sistema, en col·laboració amb el responsable del sistema.
• Participar en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat, i validar-los.

• Gestionar les revisions externes o internes del sistema.
• Gestionar els processos de certificació.
• Aprovar i ratificar els canvis significatius i els requisits del sistema, i assegurar-ne l'alineació amb la Política de seguretat de l'organització.
• Exercir la potestat d'aprovació sobre els procediments del mapa normatiu, i deixar constància en acta de les modificacions efectuades per a assegurar el control de versions i la coherència del sistema de seguretat.

7.3.3. Responsable del sistema (RSIS)
Són funcions del responsable del sistema:
• Desenvolupar, operar i mantindre el sistema d'informació durant tot el seu cicle de vida, i elaborar els procediments operatius necessaris.
• Definir la topologia i la gestió del sistema d'informació establint els criteris d'ús i els serveis disponibles.
• Detindre l'accés a informació o prestació de servei si té el coneixement que presenten deficiències greus de seguretat.
• Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
• Proporcionar assessorament per a determinar la categoria del sistema, en col·laboració amb el responsable de seguretat.
• Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat.
• Dur a terme, si és el cas, les funcions de l'administrador de la seguretat del sistema:
○ Gestionar, configurar i actualitzar, si és el cas, el maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
○ Gestionar les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seua correspondència amb el que s'ha autoritzat.
○ Aprovar els canvis en la configuració vigent del sistema d'informació.
○ Assegurar que els controls de seguretat establits són complits estrictament.
○ Assegurar que són aplicats els procediments

determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema.
• Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
• Gestionar las revisiones externas o internas del sistema.
• Gestionar los procesos de certificación.
• Aprobar y ratificar los cambios significativos y requisitos del sistema, asegurando su alineación con la Política de Seguridad de la organización.
• Ejercer la potestad de aprobación sobre los procedimientos del Mapa Normativo, dejando constancia en acta de las modificaciones efectuadas para asegurar el control de versiones y la coherencia del sistema de seguridad.

7.3.3. Responsable del Sistema (RSIS)
Serán funciones del responsable del Sistema:
• Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
• Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
• Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
• Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
• Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el responsable de Seguridad.
• Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
• Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:
○ La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
○ La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
○ Aprobar los cambios en la configuración vigente del Sistema de Información.
○ Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
○ Asegurar que son aplicados los procedimientos

aprovats per a manejar el sistema d'informació.
○ Supervisar les instal·lacions de maquinari i programari, les seues modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
○ Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

○ Informar el responsable de seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
○ Col·laborar en la investigació i resolució d'incidents de seguretat, des de la detecció fins a la resolució.

Quan la complexitat del sistema ho justifique, el responsable del sistema pot designar els responsables de sistema delegats que considere necessaris, que tenen dependència funcional directa d'ell i són responsables en el seu àmbit de totes les accions que els delegue. Igualment, també pot delegar altres funcions concretes de les responsabilitats que se li atribueixen.

7.4. Delegat o delegada de protecció de dades

Són funcions del delegat o la delegada de protecció de dades:
• Informar i assessorar la UMH i els usuaris que s'ocupen del tractament de les obligacions que els incumbeixen en virtut de la normativa vigent en matèria de protecció de dades.
• Supervisar el compliment del que disposen la normativa de seguretat i les polítiques internes de la UMH en matèria de protecció de dades, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament i les auditories corresponents.

• Oferir l'assessorament que se li sol·licite sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació.
• Cooperar amb l'Agència Espanyola de Protecció de Dades quan ho requerisca, i actuar-hi com a punt de contacte per a qüestions relatives al tractament de dades.
• El delegat o la delegada de protecció de dades exerceix les seues funcions parant atenció als riscos associats a les operacions de tractament. Per a això ha de ser capaç de:
○ Sol·licitar informació per a determinar les activitats

aprobados para manejar el Sistema de Información.
○ Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
○ Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
○ Informar al responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
○ Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

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

7.4. Delegado/a de Protección de Datos

Serán funciones del/la Delegado/a de Protección de Datos:
• Informar y asesorar a la UMH y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
• Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de la UMH, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
• Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
• Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
• El/la delegado/a de protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
○ Recabar información para determinar las

de tractament.
○ Analitzar i comprovar la conformitat de les activitats de tractament.
○ Informar, assessorar i emetre recomanacions al responsable o l'encarregat del tractament.
○ Sol·licitar informació per a supervisar el registre de les operacions de tractament.
○ Assessorar en el principi de la protecció de dades per disseny i per defecte.
○ Assessorar sobre si es duen a terme o no les avaluacions d'impacte, metodologia, salvaguardes que cal aplicar, etc.
○ Prioritzar activitats sobre la base dels riscos.
○ Assessorar el responsable de tractament sobre les àrees que cal auditar, sobre les activitats de formació que cal dur a terme i sobre les operacions de tractament a les quals cal dedicar més temps i recursos.

7.5. Comité de Seguretat TI (COMSEGTI)

Són funcions del Comité de Seguretat TI:

- Atribucions del Comité de Seguretat TI:

○ Estar permanentment informat de la normativa que regula la certificació de conformitat amb l'ENS, incloent-hi les normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.
○ Estar permanentment informat de la relació d'entitats de certificació acreditades i organitzacions públiques i privades certificades.
○ Estar permanentment informat de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració Pública té establits tractes o acords de reconeixement mutu de certificats.

○ Proposar directrius i recomanacions que han de ser arreplegades en les actes corresponents de les reunions del Comité, a les quals el president ha de respondre detalladament.
○ Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que siguen consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

○ Atendre les inquietuds, en matèria de seguretat de la informació, de l'administració i de les diferents àrees, i informar regularment de l'estat de la seguretat de la informació a la direcció.

○ Resoldre els conflictes de responsabilitat que puguen aparéixer entre els diferents responsables i/o entre diferents departaments, i elevar els casos en els quals no tinga suficient autoritat per a decidir.

actividades de tratamiento.
○ Analizar y comprobar la conformidad de las actividades de tratamiento.
○ Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
○ Recabar información para supervisar el registro de las operaciones de tratamiento.
○ Asesorar en el principio de la protección de datos por diseño y por defecto.
○ Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
○ Priorizar actividades en base a los riesgos.
○ Asesorar al responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

7.5. Comité de Seguridad TI (COMSEGTI)

Serán funciones del Comité de Seguridad TI:

- Atribuciones del Comité de Seguridad TI:

○ Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
○ Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
○ Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
○ Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
○ Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
○ Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
○ Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para

○ Assessorar en matèria de seguretat de la informació, sempre que li siga requerit.
○ Revisar la Política de seguretat de la informació amb l'aprovació prèvia de l'òrgan superior.
○ Aprovar la normativa d'ús de mitjans electrònics per a tot el personal.
○ Aprovar el mapa de normativa amb la llista de la normativa i els procediments de seguretat per a la implantació de l'ENS.

• Periodicitat de les reunions i adopció d'acords:

○ Durant el desenvolupament del projecte d'adequació a l'ENS, per a avaluar-ne el desenvolupament i possibilitar-ne un seguiment adequat, el Comité de Seguretat TI s'ha de reunir, almenys, una vegada al trimestre.
○ Una vegada aconseguida la certificació de conformitat amb l'ENS dels serveis prestats per la Universitat, el Comité de Seguretat TI s'ha de reunir, almenys, dues vegades a l'any amb caràcter semestral, sense perjudici que, ateses les necessitats derivades del compliment de les seues finalitats i atribucions, requerisca una freqüència major en les reunions.
○ En qualsevol cas, les reunions les convoca la presidència, a través del secretari, a iniciativa seua o per majoria dels membres permanents.

○ Les decisions s'adopten per consens dels membres permanents.

7.6. Oficina de Seguretat TI

Dins de l'estructura de governança de la ciberseguretat es constitueix l'Oficina de Seguretat TI, les competències de la qual estan relacionades amb les àrees de treball següents: adequació a l'ENS, normativa i gestió de riscos, anàlisis i millora contínua, seguretat en les interconnexions i connectivitat i altres funcions connexes o concordants. La seua composició és:
• Responsable de l'Oficina de Seguretat TI és el cap de secció de Sistemes, Usabilitat i Accessibilitat del Servei d'Innovació i Planificació Tecnològica que actua d'enllaç amb el Comité de Seguretat TI.

• Els i les especialistes de seguretat (AES) de la secció de Sistemes del Servei d'Innovació i Planificació Tecnològica.
• Tots els administradors especialistes de seguretat (AES) que el responsable de seguretat determine que siguen necessaris.

decidir.
○ Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
○ Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
○ Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
○ Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.

• Periodicidad de las reuniones y adopción de acuerdos:
○ Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el Comité de Seguridad TI se reunirá, al menos, una vez al trimestre.
○ Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados por la universidad, el Comité de Seguridad TI se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
○ En cualquier caso, las reuniones se convocarán por su presidencia, a través del secretario, a su iniciativa o por mayoría de sus miembros permanentes.
○ Las decisiones se adoptarán por consenso de los miembros permanentes.

7.6. Oficina de Seguridad TI

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la Oficina de Seguridad TI, cuyas competencias están relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad y otras funciones conexas o concordantes. Su composición será:
• Responsable de la Oficina de Seguridad TI será el jefe de sección de Sistemas, Usabilidad y Accesibilidad del Servicio de Innovación y Planificación Tecnológica que actuará de enlace con el Comité de Seguridad TI.
• Los y las especialistas de seguridad (AES) de la Sección de Sistemas del Servicio de Innovación y Planificación Tecnológica.
• Todos aquellos administradores especialistas de seguridad (AES) que el responsable de Seguridad determine que sean necesarios.

Les funcions de l'Oficina de Seguretat TI són, entre altres que li puguen ser encomanades pel Comité de Seguretat TI:

- Gestió i operativa de la seguretat del projecte d'adequació, implantació i gestió de conformitat amb l'ENS, anàlisi i gestió de riscos, explotació, normativa i manteniment.
- Redacció i presentació de propostes al Comité de Seguretat TI. Elabora els aspectes relacionats amb la ciberseguretat i els debat en primera instància, perquè siguen traslladats al Comité.
- Promoure la millora contínua del sistema de gestió de la Seguretat de la informació i les comunicacions. Per a això s'encarrega de:
  - Elaborar (i revisar regularment) la Política de seguretat de la informació per a traslladar-la al Comité de Seguretat TI perquè la revise i siga aprovada posteriorment per l'òrgan superior.
  - Elaborar la normativa de seguretat de la informació perquè l'aprove el responsable de seguretat, la figura del qual està constituïda pel Comité de Seguretat TI (COMSEGTI).
  - Verificar els procediments de seguretat de la informació i altra documentació per a aprovar-la.

  - Elaborar programes de formació destinats a formar i sensibilitzar el personal en matèria de seguretat de la informació i protecció de dades.
  - Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.

  - Proposar plans de millora de la seguretat de la informació, amb la dotació pressupostària corresponent, i prioritzar les actuacions en matèria de seguretat quan els recursos siguen limitats.

  - Fer un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions al respecte.

  - Promoure la realització de les auditories periòdiques ENS i RGPD que permeten verificar el compliment de les obligacions de la universitat en matèria de seguretat de la Informació i protecció de dades.

- Periodicitat de les reunions i adopció d'acords:

  - El responsable de l'Oficina de Seguretat TI convoca les reunions de treball dels seus membres i arreplega els acords assolits, dels quals dona compte

Las funciones de la Oficina de Seguridad TI serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad TI:

- Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.
- Redacción y presentación de propuestas al Comité de Seguridad TI. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información y las Comunicaciones. Para ello se encargará de:
  - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al Comité de Seguridad TI para su revisión y posterior aprobación del órgano superior.
  - Elaborar la normativa de Seguridad de la Información para su aprobación por el responsable de Seguridad, cuya figura estará constituida por el Comité de Seguridad TI (COMSEGTI).
  - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
  - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
  - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
  - Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
  - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
  - Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la Información y protección de datos.

- Periodicidad de las reuniones y adopción de acuerdos:
  - El responsable de la Oficina de Seguridad TI convocará las reuniones de trabajo de sus miembros y recabará los acuerdos alcanzados, de los que dará

al Comité de Seguretat TI, perquè els aprove, si és el cas.

○ L'Oficina pot desenvolupar les seues funcions en ple o en grups de treball per a analitzar i dur a terme propostes específiques. Les propostes plantejades en l'Oficina de Seguretat TI les ha de sotmetre a anàlisi, debat i aprovació, si és el cas, el Comité de Seguretat TI.

7.8. Fòrum de seguretat TIC de les universitats

El fòrum de seguretat TIC es constitueix com un punt de trobada de les universitats en l'àmbit de l'Esquema Nacional de Seguretat.

La sectorial CRUE-TIC, entre les missions de la qual està la d'"estudiar les necessitats i aplicacions de les TIC en la gestió, la docència i la investigació, i proposar actuacions i projectes conjunts a les universitats", disposa d'un grup de treball específic de seguretat i auditoria TI. En aquesta sectorial estan representades totes les universitats espanyoles, tant públiques com privades. Aquest grup de treball constitueix el marc ideal per a ser el fòrum de seguretat TIC per a universitats. A causa del caràcter sectorial del món universitari, és de gran ajuda en l'àmbit de la governança en ciberseguretat.

El funcionament del Fòrum es regeix segons el reglament intern de la sectorial CRUE-TIC. En el fòrum de la seguretat es plantegen, entre d'altres, les necessitats de seguretat de les universitats adherides. Les propostes plantejades pel fòrum de seguretat de les universitats són traslladades a cada universitat pels seus representants perquè les analitze, debata i aprove, si és el cas, el Comité de Seguretat TIC.

Aquest fòrum de seguretat TIC es pot coordinar amb altres fòrums de caràcter sectorial, local o regional.

7.9. Procediments de designació

El rector de la UMH crea el COMSEGTI, en nomena els integrants i designa els responsables identificats en aquesta política. El nomenament es revisa cada 4 anys o quan el lloc quede vacant.

8. DADES PERSONALS

La UMH només arreplega i tracta dades personals quan siguen adequades, pertinents i no excessives i tinguen relació amb l'àmbit i les finalitats per als quals s'han obtingut. Igualment, adopta les mesures d'índole tècnica i organitzatives necessàries per a

cuenta al Comité de Seguridad TI, para su aprobación, en su caso.

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

7.8. Foro de seguridad TIC de las Universidades

El Foro de seguridad TIC se constituye como un punto de encuentro de las universidades en el ámbito del Esquema Nacional de Seguridad.

La Sectorial CRUE-TIC, entre cuyas misiones está la de "Estudiar las necesidades y aplicaciones de las TIC en la gestión, la docencia y la investigación, proponiendo actuaciones y proyectos conjuntos a las Universidades", dispone de un Grupo de Trabajo específico de Seguridad y Auditoría TI. En dicha Sectorial están representadas todas las universidades españolas, tanto públicas como privadas. Dicho Grupo de Trabajo constituye el marco ideal para ser el Foro de Seguridad TIC para universidades. Debido al carácter sectorial del mundo universitario, será de gran ayuda en el ámbito de la Gobernanza en ciberseguridad.

El funcionamiento del Foro se regirá según el Reglamento interno de la Sectorial CRUE-TIC. En el Foro de la Seguridad se plantearán, entre otras, las necesidades de seguridad de las universidades adheridas. Las propuestas planteadas por el Foro de Seguridad de las Universidades serán trasladadas a cada universidad por sus representantes para su análisis, debate y aprobación, si procede, por parte del Comité de Seguridad TIC.

Este Foro de Seguridad TIC podrá coordinarse con otros foros de carácter sectorial, local o regional.

7.9. Procedimientos de designación

La creación del COMSEGTI, el nombramiento de sus integrantes y la designación de los responsables identificados en esta Política, se realizará por el rector de la UMH. El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

8. DATOS PERSONALES

La UMH sólo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y

complir la normativa de protecció de dades.

La Universitat Miguel Hernández publica en la Seu Electrònica la seua política de privacitat.

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 de la política, i és responsabilitat de la Comissió de Seguretat disposar els mitjans necessaris perquè la informació arribe als afectats, tenint en compte sempre les disponibilitats pressupostàries de la UMH.

Cal establir un programa d'accions en conscienciació contínua per a atendre a 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 han de rebre formació per al maneig segur dels sistemes en la mesura que la necessiten per a fer el seu treball. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en el lloc.

10. GESTIÓ DE RISCOS

Tots els sistemes afectats per aquesta política de seguretat de la informació estan subjectes a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos als quals estan exposats. Aquesta anàlisi s'ha de repetir:

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

El responsable de seguretat és l'encarregat que es duga a terme l'anàlisi de riscos, així com d'identificar manques i febleses i posar-les en coneixement del Comité de Seguretat TI.

El Comité de Seguretat TI dinamitza la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes i promou inversions de caràcter horitzontal.

organizativas necesarias para el cumplimiento de la Normativa de Protección de Datos.
La Universidad Miguel Hernández, publicará en la Sede Electrónica su Política de Privacidad.

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. GESTIÓN DE RIESGOS

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

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

El responsable de Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad TI.

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

El procés de gestió de riscos comprén les fases següents:

- Categorització dels sistemes.
- Anàlisi de riscos.
- El COMSEGTI selecciona les mesures de seguretat que cal aplicar, les quals han de ser proporcionals als riscos i estar justificades.

Les fases d'aquest procés es duen a terme segons el que disposen els annexos I i II del Reial decret 311/2022, de 3 de maig, i seguint les normes, instruccions, guies CCN-STIC i recomanacions per a aplicar-les elaborades pel Centre Criptològic Nacional.

En particular, per a fer l'anàlisi de riscos, com a norma general, s'utilitza una metodologia reconeguda d'anàlisi i gestió de riscos.

11. NOTIFICACIÓ D'INCIDENTS

De conformitat amb el que disposa l'article 33 del Reial decret 311/2022, de 3 de maig, la UMH ha de notificar al Centre Criptològic Nacional els incidents que tinguen un impacte significatiu en la seguretat de la informació manejada i dels serveis prestats en relació amb la categorització de sistemes que arreplega l'annex I d'aquest cos legal.

12. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta política de seguretat de la informació és complementada per mitjà de normativa diversa i recomanacions de seguretat (normatives i procediments de seguretat, procediments tècnics de seguretat, informes, registres i evidències electròniques). En correspon al Comité de Seguretat TI la revisió anual i/o el manteniment, i proposar-ne millores, en cas que calga.

El cos normatiu sobre seguretat de la informació es desenvolupa en tres nivells per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment, de manera que cada norma d'un determinat nivell de desenvolupament es fonamente en les normes de nivell superior. Aquests nivells de desenvolupament normatiu són els següents:

- Primer nivell normatiu: constituït per aquesta política de seguretat de la informació, la Normativa interna de l'ús dels mitjans electrònics i les directrius generals de seguretat aplicables als organismes o

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El COMSEGTI procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

11. NOTIFICACIÓN DE INCIDENTES

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

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad TI su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

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

- Primer nivel normativo: constituido por la presente Política de Seguridad de la Información, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables a

unitats de la Universitat als quals siguen aplicables aquests documents.

- Segon nivell normatiu: constituït per les normes de seguretat derivades de les anteriors.
- Tercer nivell normatiu: constituït per procediments, guies i instruccions tècniques. Són documents que, complint amb el que exposa la Política de seguretat de la informació, determinen les accions o tasques que cal dur a terme en l'acompliment d'un procés.

Correspon al Consell de Govern de la Universitat Miguel Hernández aprovar la Política de seguretat de la informació i la normativa interna de l'ús dels mitjans electrònics de la Universitat, i el COMSEGTI és l'òrgan responsable d'aprovar els documents restants, i és també el responsable de difondre'ls perquè els coneguen les parts afectades.

De la mateixa manera, aquesta política de seguretat de la informació complementa la Política de privacitat de la Universitat Miguel Hernández en matèria de protecció de dades.

La normativa de seguretat i, molt especialment, la Política de seguretat de la informació i la Normativa interna de l'ús dels mitjans electrònics, han de ser conegudes i estar a la disposició de tots els membres de la Universitat, en particular, els que utilitzen, operen o administren els sistemes d'informació i comunicacions. Està disponible per a ser consultada en la intranet de la Universitat; en suport paper, aquesta documentació és custodiada pel Servei d'Innovació i Planificació Tecnològica.

13. RESOLUCIÓ DE CONFLICTES

En cas de conflicte entre els diferents responsables que componen l'estructura organitzativa de la Política de seguretat de la informació de la UMH, preval la decisió del Comité de Seguretat TI.

14. TERCERES PARTS

Quan la UMH preste serveis a altres organismes o manege informació d'altres organismes, se'ls ha de fer partícips d'aquesta política de seguretat de la informació, i s'han d'establir canals per a reportar i coordinar els comités de seguretat TI respectius i procediments d'actuació per a reaccionar davant d'incidents de seguretat.

los organismos o unidades de la universidad a los que sea de aplicación dichos documentos.

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

Corresponde al Consejo de Gobierno de la Universidad Miguel Hernández la aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de la universidad, siendo el COMSEGTI el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de la Universidad Miguel Hernández en materia de protección de datos.

La normativa de seguridad y, muy especialmente, la Política de seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos, será conocida y estará a disposición de todos los miembros de la universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet de la Universidad, en soporte papel, esta documentación será custodiada por el Servicio de Innovación y Planificación Tecnológica.

13. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información de la UMH, prevalecerá la decisión del Comité de Seguridad TI.

14. 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 ha de fer partícips d'aquesta política de seguretat i de la Normativa de Seguretat que concernisca a aquests serveis o informació. Aquesta tercera part queda subjecta a les obligacions establides en aquesta normativa, i pot desenvolupar els seus procediments operatius per a satisfer-la. Cal establir procediments específics de report i resolució d'incidències. Cal garantir que el personal de tercers estiga conscienciat adequadament en matèria de seguretat, almenys al mateix nivell que estableix aquesta política.

Quan algun aspecte d'aquesta política de seguretat de la informació 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 manera de tractar-los. Es requerirà que aquest informe siga aprovat pels responsables de la informació i els serveis afectats abans de seguir avant.

15. MILLORA CONTÍNUA

La gestió de la seguretat de la informació és un procés subjecte a actualització permanent. Els canvis en l'organització, les amenaces, les tecnologies i/o la legislació són exemples en els quals cal una millora contínua dels sistemes. Per això, cal implantar un procés permanent que comporta, entre altres accions:

- Revisió de la Política de seguretat de la informació.
- Revisió dels serveis i la informació i la seua categorització.
- Execució amb periodicitat anual de l'anàlisi de riscos.
- Realització d'auditories internes o, quan siguen procedents, externes.
- Revisió de les mesures de seguretat.
- Revisió i actualització de les normes i procediments.

16. ENTRADA EN VIGOR

Aquesta política de seguretat de la informació entra en vigor l'endemà de la publicació en el *Butlletí Oficial de la Universitat Miguel Hernández* (BOUMH), amb l'aprovació prèvia per part del Consell de Govern, i fins que siga reemplaçada per una nova política.

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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

15. MEJORA CONTINUA

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

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas o, cuando procedan, externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de las normas y procedimientos.

16. 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 l'anterior política de seguretat de la informació de la Universitat Miguel Hernández, que va ser aprovada pel Consell de Govern, en la sessió de 27 d'octubre de 2021.

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

Queda derogada la anterior política de seguridad de la información de la Universidad Miguel Hernández, que fue aprobada por el Consejo de Gobierno, reunido en sesión de 27 de octubre de 2021.

Lo que comunico para su conocimiento y efectos oportunos.

LA SECRETÀRIA GENERAL

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