COGO2026/02.039

NOTIFICACIÓ D'ACORD DEL CONSELL DE GOVERN

Acord d'aprovació de la Normativa de governança de tecnologies de la informació (TI) de la Universitat Miguel Hernández d'Elx

Vist l'informe de l'auditoria de governança TI de la Sindicatura de Comptes, i amb l'objectiu d'esmenar les deficiències observades, es presenta aquesta nova normativa que estableix el marc de direcció, control i gestió de les TI en la UMH;

La Normativa de governança de tecnologies de la informació (TI) indica com resoldre la coordinació entre les diferents comissions TI. Estableix la dotació pressupostària necessària per a complir els objectius de transformació digital de la Universitat, prioritza les accions sota els principis rectors d'eficiència, seguretat, transparència i alineació estratègica. El seu compliment és obligatori per a tot el personal (PDI, PI i PTGAS), estudiants, col·laboradors externs i empreses proveïdores que facen ús dels recursos de tecnologia de la informació de la Universitat;

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 Normativa de governança de tecnologies de la informació (TI) de la UMH en els termes establits a continuació:

NORMATIVA DE GOVERNANÇA DE LES TECNOLOGIES DE LA INFORMACIÓ (TI) DE LA UMH

ÍNDEX DE LA NORMATIVA DE GOVERNANÇA TI – UMH

NOTIFICACIÓN DE ACUERDO DEL CONSEJO DE GOBIERNO

Acuerdo de aprobación de la Normativa de Gobernanza de Tecnologías de la Información (TI) de la Universidad Miguel Hernández de Elche

A la vista del Informe de la Auditoría de Gobernanza TI de la Sindicalra de Comptes, y con el objetivo de subsanar las deficiencias observadas, se presenta esta nueva normativa que establece el marco de dirección, control y gestión de las TI en la UMH;

La Normativa de Gobernanza de Tecnologías de la Información (TI) indica cómo resolver la coordinación entre las diferentes comisiones TI. Establece la dotación presupuestaria necesaria para cumplir los objetivos de Transformación Digital de la Universidad, priorizando las acciones bajo los principios rectores de eficiencia, seguridad, transparencia y alineación estratégica. Su cumplimiento es obligatorio para todo el personal (PDI, PI y PTGAS), estudiantes, colaboradores externos y empresas proveedoras que hagan uso de los recursos de Tecnología de la Información de la Universidad;

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 Normativa de Gobernanza de Tecnologías de la Información (TI) de la UMH en los términos establecidos a continuación:

NORMATIVA DE GOBERNANZA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (TI) DE LA UMH

ÍNDICE DE LA NORMATIVA DE GOBERNANZA TI – UMH

TÍTOL I. DISPOSICIONS GENERALS

Article 1. Objecte i abast

Aquesta normativa té per objecte establir el marc de direcció, control i gestió de les tecnologies de la informació (TI) en la UMH. El seu compliment és obligatori per a tot el personal (PDI, PI i PTGAS), estudiants, col·laboradors externs i empreses proveïdores que facen ús dels recursos tecnològics de la Universitat.

Article 2. Marc legal de referència

Aquesta normativa es dicta a l'empara de l'Esquema Nacional de Seguretat (ENS), la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), el Reglament general de protecció de dades (RGPD), la Llei 39/2015 de procediment administratiu comú de les administracions públiques, la Llei 40/2015 de règim jurídic del sector Públic, així com els Estatuts de la UMH.

TÍTULO I. DISPOSICIONES GENERALES

Artículo 1. Objeto y Alcance

La presente normativa tiene por objeto establecer el marco de dirección, control y gestión de las Tecnologías de la Información (TI) en la UMH. Su cumplimiento es obligatorio para todo el personal (PDI, PI y PTGAS), estudiantes, colaboradores externos y empresas proveedoras que hagan uso de los recursos tecnológicos de la Universidad.

Artículo 2. Marco Legal de Referencia

Esta normativa se dicta al amparo del Esquema Nacional de Seguridad (ENS), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el Reglamento General de Protección de Datos (RGPD), la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 de Régimen Jurídico del Sector Público, así como los Estatutos de la UMH.

Article 3. Principis rectors
La governança TI de la UMH es regeix per quatre pilars que actuen com a filtre obligatori per a tota decisió tecnològica:

- **1. Eficiència**: Es prohibeix la duplicitat de sistemes. Tota inversió ha de prioritzar serveis compartits i centralitzats per a optimitzar el pressupost públic.

- **2. Seguretat:** La ciberseguretat és un requisit intrínsec, no opcional. Es prioritza la protecció de dades crítiques i la garantia que els serveis més crítics (Campus Virtual, Seu Electrònica, Portal UMH) funcionen sense interrupcions.

- **3. Transparència:** Totes les decisions de les comissions TI han de ser motivades i auditables. Es garanteix la integritat de la dada i es fomenta l'ús de dades obertes (*open data*) per a la investigació.

- **4. Alineació Estratègica**: La tecnologia és una eina al servei de la Universitat. Els projectes TI han de contribuir directament a les finalitats estatutàries de la Universitat.

TÍTOL II. ESTRUCTURA DE GOVERNANÇA I DIRECCIÓ

Article 4. L'Equip de Govern com a autoritat superior

El Consell de Direcció (Equip de Govern) és el màxim òrgan responsable de la política de TI. Les seues funcions inclouen:
1. Aprovar l'estratègia digital de la Universitat.
2. Definir el nivell de risc acceptable en matèria de ciberseguretat.
3. Assegurar la dotació pressupostària necessària per a la resiliència tecnològica.

Article 5. La direcció de tecnologies de la informació

La direcció del Servei d'Innovació i Planificació Tecnològica executa l'estratègia TI de l'Equip de Govern, i s'encarrega juntament amb el Servei d'Infraestructura Informàtica de la gestió operativa, l'arquitectura tècnica i el suport dels sistemes, sempre sota les directrius estratègiques aprovades.

TÍTOL III. COORDINACIÓ MITJANÇANT COMISSIONS ESTRATÈGIQUES

Article 6. Comissió de Cartera de Projectes TI
És l'encarregada d'acceptar o rebutjar i, si és el cas,

Artículo 3. Principios Rectores
La gobernanza TI de la UMH se rige por cuatro pilares que actúan como filtro obligatorio para toda decisión tecnológica:

- **1. Eficiencia:** Se prohíbe la duplicidad de sistemas. Toda inversión debe priorizar servicios compartidos y centralizados para optimizar el presupuesto público.

- **2. Seguridad:** La ciberseguridad es un requisito intrínseco, no opcional. Se prioriza la protección de datos críticos y la garantía de que los servicios más críticos (Campus Virtual, Sede Electrónica, Portal UMH) funcionen sin interrupciones.

- **3. Transparencia:** Todas las decisiones de las comisiones TI deben ser motivadas y auditables. Se garantiza la integridad del dato y se fomenta el uso de datos abiertos (*Open Data*) para la investigación.

- **4. Alineación Estratégica:** La tecnología es una herramienta al servicio de la Universidad. Los proyectos TI deberán contribuir directamente a los fines estatutarios de la Universidad.

TÍTULO II. ESTRUCTURA DE GOBERNANZA Y DIRECCIÓN

Artículo 4. El Equipo de Gobierno como Autoridad Superior
El Consejo de Dirección (Equipo de Gobierno) es el máximo órgano responsable de la política de TI. Sus funciones incluyen:
1. Aprobar la Estrategia Digital de la Universidad.
2. Definir el nivel de riesgo aceptable en materia de ciberseguridad.
3. Asegurar la dotación presupuestaria necesaria para la resiliencia tecnológica.

Artículo 5. La Dirección de Tecnologías de la Información
La dirección del Servicio de Innovación y Planificación Tecnológica ejecutará la estrategia TI del Equipo de Gobierno, encargándose junto con el Servicio de Infraestructura Informática de la gestión operativa, la arquitectura técnica y el soporte de los sistemas, siempre bajo las directrices estratégicas aprobadas.

TÍTULO III. COORDINACIÓN MEDIANTE COMISIONES ESTRATÉGICAS

Artículo 6. Comisión de Cartera de Proyectos TI
Será la encargada de aceptar o rechazar y, en su

prioritzar les sol·licituds de desenvolupament o adquisició de programari. Cap projecte tecnològic es pot iniciar sense el seu vistiplau, que es basa en criteris de retorn d'eficiència, necessitat, valor, viabilitat tècnica i alineació pressupostària.

Article 7. Comissió d'Administració Electrònica

És la responsable de definir els estàndards de tramitació digital. El seu objectiu és garantir la interoperabilitat dels sistemes i assegurar que qualsevol tràmit administratiu es puga fer de manera 100% digital amb plena validesa jurídica.

Article 8. Comissió de Tecnologies Web

Dicta les normes sobre la presència en línia de la UMH. Regula la imatge institucional, l'accessibilitat web i la seguretat dels portals, i evita la proliferació de webs o xarxes socials no autoritzades que en comprometen la marca o la seguretat.

Article 9. Comissió de Protecció de Dades

Vetla pel compliment del RGPD en tots els tractaments de la UMH. Especialment, garanteix l'aplicació dels principis de l'article 5 i la responsabilitat proactiva i impulsa la privacitat des del disseny i per defecte.

Article 10. Comissió de Seguretat TI

Garanteix la integritat, confidencialitat i disponibilitat de la infraestructura digital de la Universitat. Les seues funcions principals són la vigilància i protecció, la gestió del risc, la resposta davant d'incidents, el compliment de l'ENS i l'auditoria de sistemes.

Article 11. Interoperabilitat i coordinació de comissions

Per a garantir la coherència de la política digital i evitar el solapament de funcions, les comissions regulades en aquest títol han d'actuar sota el principi de cooperació reforçada.

En cas de discrepància tècnica entre comissions, el vicerectorat amb competències en TI, en representació de l'Equip de Govern, dirimeix les discrepàncies després d'escoltar les parts.

caso, priorizar las solicitudes de desarrollo o adquisición de software. Ningún proyecto tecnológico podrá iniciarse sin su visto bueno, basándose en criterios de retorno de eficiencia, necesidad, valor, viabilidad técnica y alineación presupuestaria.

Artículo 7. Comisión de Administración Electrónica

Será la responsable de definir los estándares de tramitación digital. Su objetivo es garantizar la interoperabilidad de los sistemas y asegurar que cualquier trámite administrativo pueda realizarse de forma 100% digital con plena validez jurídica.

Artículo 8. Comisión de Tecnologías Web

Dictará las normas sobre la presencia online de la UMH. Regulará la imagen institucional, la accesibilidad web y la seguridad de los portales, evitando la proliferación de webs o redes sociales no autorizadas que comprometan la marca o la seguridad.

Artículo 9. Comisión de Protección de Datos

Velará por el cumplimiento del RGPD en todos los tratamientos de la UMH. En especial, garantizará la aplicación de los principios de su artículo 5 y la responsabilidad proactiva e impulsará la privacidad desde el diseño y por defecto.

Artículo 10. Comisión de Seguridad TI

Garantizará la integridad, confidencialidad y disponibilidad de la infraestructura digital de la Universidad. Sus funciones principales son: Vigilancia y Protección, Gestión del Riesgo, Respuesta ante Incidentes, Cumplimiento del ENS y la Auditoría de Sistemas.

Artículo 11. Interoperabilidad y Coordinación de Comisiones

Para garantizar la coherencia de la política digital y evitar el solapamiento de funciones, las comisiones reguladas en este título actuarán bajo el principio de cooperación reforzada.

En caso de discrepancia técnica entre comisiones, el vicerrectorado con competencias en TI, en representación del Equipo de Gobierno, dirimirá las discrepancias tras escuchar a las partes.

TÍTOL IV. POLÍTICA DE CIBERSEGURETAT I RESILIÈNCIA

Article 12. Gestió de riscos TI

La UMH adopta un enfocament proactiu basat en l'anàlisi de riscos per a protegir els seus actius digitals i garantir la continuïtat de la seua activitat.

1. Anàlisi obligatòria: Tot sistema o projecte tecnològic crític ha de comptar amb una avaluació de riscos prèvia que identifique amenaces (ciberatacs, fallades tècniques o errors humans) i vulnerabilitats.

2. Classificació d'actius: La direcció TI ha de mantindre un inventari d'actius (dades d'alumnes, processos de nòmines, investigació) classificats segons la importància per al funcionament de la Universitat.

3. Decisions estratègiques: L'Equip de Govern, basant-se en els informes tècnics, decideix si un risc ha de ser mitigat (amb més inversió), transferit (amb assegurances), evitat o assumit formalment.

4. Millora contínua: El mapa de riscos de la UMH es revisa anualment per a adaptar-lo a les noves ciberamenaces i canvis legislatius, per tal d'assegurar que la Universitat siga sempre resilient.

Article 13. Resposta davant d'incidents i gestió de crisi

Davant d'una bretxa de seguretat o fallada crítica, la UMH ha d'activar un protocol de resposta immediata sota una jerarquia clara:

1. Comité de crisi: Es constitueix d'urgència un gabinet liderat pel rector o la rectora, juntament amb el vicerectorat competent en TI, el vicerectorat competent en comunicació, el Comité de Seguretat TI, el delegat o la delegada de protecció de dades i la direcció del Servei de Comunicació, per a dirigir la resposta política i legal.

2. Autoritat tècnica: La direcció TI està facultada per a aïllar o desconnectar sistemes preventivament per a frenar atacs, prioritzant sempre la recuperació dels serveis crítics segons l'impacte institucional.

3. Comunicació unificada: S'estableix un càrrec de portaveu únic a través de la direcció de Comunicació.

TÍTULO IV. POLÍTICA DE CIBERSEGURIDAD Y RESILIENCIA

Artículo 12. Gestión de Riesgos TI

La UMH adopta un enfoque proactivo basado en el análisis de riesgos para proteger sus activos digitales y garantizar la continuidad de su actividad.

1. Análisis Obligatorio: Todo sistema o proyecto tecnológico crítico deberá contar con una evaluación de riesgos previa que identifique amenazas (ciberataques, fallos técnicos o errores humanos) y vulnerabilidades.

2. Clasificación de Activos: La Dirección TI mantendrá un inventario de activos (datos de alumnos, procesos de nóminas, investigación) clasificados según su importancia para el funcionamiento de la Universidad.

3. Decisiones Estratégicas: El Equipo de Gobierno, basándose en los informes técnicos, decidirá si un riesgo debe ser mitigado (con más inversión), transferido (con seguros), evitado o asumido formalmente.

4. Mejora Continua: El mapa de riesgos de la UMH se revisará anualmente para adaptarse a las nuevas ciberamenazas y cambios legislativos, asegurando que la Universidad sea siempre resiliente.

Artículo 13. Respuesta ante Incidentes y gestión de crisis

Ante una brecha de seguridad o fallo crítico, la UMH activará un protocolo de respuesta inmediata bajo una jerarquía clara:

1. Comité de Crisis: Se constituirá de urgencia un gabinete liderado por el/la rector/a, junto con el vicerrectorado competente en TI, el vicerrectorado competente en Comunicación, el Comité de Seguridad TI, el/la delegado/a de protección de datos y la dirección del Servicio de Comunicación, para dirigir la respuesta política y legal.

2. Autoridad Técnica: La Dirección TI está facultada para aislar o desconectar sistemas preventivamente para frenar ataques, priorizando siempre la recuperación de los servicios críticos según su impacto institucional.

3. Comunicación Unificada: Se establece una portavocía única a través de la Dirección de

Queda prohibida qualsevol declaració externa no autoritzada per a evitar danys reputacionals i fuites d'informació sensible.

4. Notificacions legals: El delegat o la delegada de protecció de dades, juntament amb la direcció TI, han de comunicar a l'AEPD en el termini legal establit si hi ha dades personals compromeses. Així mateix, en cas que hi haja un alt risc per als drets i les llibertats de les persones afectades, ho han de comunicar pertinentment en els termes que estableix el RGPD.

5. Informe de millora: Després de cada incident, s'ha de presentar a l'Equip de Govern una anàlisi de les causes i les mesures correctives per a evitar-ne la repetició.

Article 14. Conscienciació i formació en seguretat TI

La seguretat TI de la UMH no depén només de la tecnologia, sinó del comportament responsable dels seus usuaris. Per això, la capacitació en ciberseguretat s'estableix com un pilar preventiu obligatori.

1. La formació específica sobre ciberseguretat i protecció de dades ha d'estar integrada en els plans de formació de la Universitat.

2. La formació en bones pràctiques digitals i en protecció de dades ha de ser part del procés d'acollida per a qualsevol nou empleat o col·laborador extern amb accés als sistemes institucionals.

3. Els programes formatius mínims s'han de centrar en la detecció de *phishing*, gestió segura de credencials, ús de dispositius personals (BYOD), protecció de dades i protocols de report d'incidents.

4. La Universitat ha de promoure campanyes periòdiques de conscienciació per a l'estudiantat, orientades a protegir-ne la identitat digital i l'ús ètic dels recursos tecnològics universitaris.

5. La Comissió de Seguretat TI pot dur a terme exercicis de simulació per a mesurar el nivell de preparació de la comunitat i ajustar les accions formatives segons els resultats.

Comunicación. Queda prohibida cualquier declaración externa no autorizada para evitar daños reputacionales y fugas de información sensible.

4. Notificaciones Legales: El/la delegado/a de protección de datos, junto con la Dirección TI, procederán a la comunicación a la AEPD en el plazo legal establecido si existen datos personales comprometidos. Asimismo, en el caso de que haya existencia de un alto riesgo de los derechos y libertades de las personas afectadas, procederán a su pertinente comunicación en los términos que establece el RGPD.

5. Informe de Mejora: Tras cada incidente, se presentará al Equipo de Gobierno un análisis de causas y medidas correctivas para evitar su repetición.

Artículo 14. Concienciación y Formación en seguridad TI

La seguridad TI de la UMH no depende solo de la tecnología, sino del comportamiento responsable de sus usuarios. Por ello, la capacitación en ciberseguridad se establece como un pilar preventivo obligatorio.

1. La formación específica sobre ciberseguridad y protección de datos estará integrada en los planes de formación de la Universidad.

2. La formación en buenas prácticas digitales y en protección de datos será parte del proceso de acogida para cualquier nuevo empleado o colaborador externo con acceso a los sistemas institucionales.

3. Los programas formativos mínimos se centrarán en la detección de *phishing*, gestión segura de credenciales, uso de dispositivos personales (BYOD), protección de datos y protocolos de reporte de incidentes.

4. La Universidad promoverá campañas periódicas de concienciación para el estudiantado, orientadas a proteger su identidad digital y el uso ético de los recursos tecnológicos universitarios.

5. La Comisión de Seguridad TI podrá realizar ejercicios de simulación para medir el nivel de preparación de la comunidad y ajustar las acciones formativas según los resultados.

TÍTOL V. GESTIÓ D'ACTIUS I RECURSOS

Article 15. Ús de tecnologies i serveis no autoritzats

Amb la finalitat de garantir la seguretat de la informació i l'eficiència en la despesa, la UMH estableix el control sobre l'adquisició i ús d'eines digitals:

1. Validació prèvia: Queda prohibida la contractació, instal·lació o ús de programari, serveis en el núvol (SaaS) o maquinari per a finalitats institucionals que no hagen sigut validats prèviament per la direcció TI o les comissions competents, si és el cas.

2. Inventari institucional: Només es consideren recursos oficials els integrats en l'inventari de la Universitat. Les dades s'han de tractar d'acord amb la la seua classificació i, en tot cas, les dades de caràcter institucional (acadèmiques, d'investigació o administratives) i les dades personals només poden ser tractades en aquestes plataformes autoritzades.

3. Riscos de la tecnologia no controlada: L'ús d'eines alienes a les vies oficials (com l'emmagatzematge en núvols personals o el programari sense llicència corporativa) suposa un risc crític per a la protecció de dades i la integritat de la xarxa universitària. Queda expressament prohibit emmagatzemar, sincronitzar, compartir, reexpedir o carregar dades personals o informació institucional en comptes personals o serveis no corporatius o no autoritzats.

4. Responsabilitat: L'ús de serveis no autoritzats per al tractament de dades de la UMH pot derivar en la revocació d'accessos i en les responsabilitats previstes en l'article 18.

Article 16. Gestió del cicle de vida dels actius tecnològics

La Universitat ha de garantir que tant el maquinari com el programari es mantinguen actualitzats, segurs i alineats amb les necessitats institucionals mitjançant una gestió integral del seu cicle de vida.

1. Manteniment i actualització: Tots els sistemes crítics i els equips de treball han de comptar amb suport tècnic vigent. És obligatori aplicar les actualitzacions de seguretat de manera prioritària per a mitigar les vulnerabilitats conegudes.

TÍTULO V. GESTIÓN DE ACTIVOS Y RECURSOS

Artículo 15. Uso de Tecnologías y Servicios No Autorizados

Con el fin de garantizar la seguridad de la información y la eficiencia en el gasto, la UMH establece el control sobre la adquisición y uso de herramientas digitales:

1. Validación Previa: Queda prohibida la contratación, instalación o uso de software, servicios en la nube (SaaS) o hardware para fines institucionales que no hayan sido validados previamente por la Dirección TI o las comisiones competentes, si procede.

2. Inventario Institucional: Solo se considerarán recursos oficiales aquellos integrados en el inventario de la Universidad. Los datos deberán tratarse conforme a su clasificación y, en todo caso, los datos de carácter institucional (académicos, investigadores o administrativos) y los datos personales sólo podrán ser tratados en estas plataformas autorizadas.

3. Riesgos de la Tecnología No Controlada: El uso de herramientas ajenas a los cauces oficiales (como almacenamiento en nubes personales o software sin licencia corporativa) supone un riesgo crítico para la protección de datos y la integridad de la red universitaria. Queda expresamente prohibido almacenar, sincronizar, compartir, reenviar o cargar datos personales o información institucional en cuentas personales o servicios no corporativos o no autorizados.

4. Responsabilidad: El uso de servicios no autorizados para el tratamiento de datos de la UMH podrá derivar en la revocación de accesos y en las responsabilidades previstas en el artículo 18.

Artículo 16. Gestión del Ciclo de Vida de los Activos Tecnológicos

La Universidad garantizará que tanto el hardware como el software se mantengan actualizados, seguros y alineados con las necesidades institucionales mediante una gestión integral de su ciclo de vida.

1. Mantenimiento y Actualización: Todos los sistemas críticos y equipos de trabajo deberán contar con soporte técnico vigente. Es obligatorio aplicar las actualizaciones de seguridad de forma prioritaria para mitigar las vulnerabilidades conocidas.

2. Pla de renovació de maquinari corporatiu: La direcció TI, sota la supervisió de la Comissió de Seguretat i de la de Cartera de Projectes, ha d'establir un pla plurianual de renovació d'equips (servidors, ordinadors, dispositius de xarxa). L'objectiu és substituir els actius que, per antiguitat, suposen un risc de fallada o una caiguda en la productivitat.

3. Gestió de programari i llicències: S'ha de prioritzar l'ús de programari corporatiu i solucions que garantisquen l'escalabilitat. S'ha de realitzar un inventari periòdic per a identificar i retirar el programari que haja deixat de rebre suport per part del fabricant.

4. Baixa i eliminació segura: Quan un equip o programari arribe al final de la seua vida útil, la retirada s'efectua seguint protocols de:
- Seguretat: Esborrament segur i certificat de les dades que contenen els suports físics.
- Sostenibilitat: Gestió de residus electrònics conforme a la normativa mediambiental vigent.

5. Estandardització: Per a optimitzar-ne el manteniment, la UMH ha de definir catàlegs de maquinari i programari estàndard. Qualsevol excepció per necessitats específiques d'investigació ha de ser validada tècnicament per a assegurar-ne la compatibilitat i seguretat.

TÍTOL VI: AUDITORIA I RÈGIM DE RESPONSABILITAT

Article 17. Supervisió, control i auditoria

Per a garantir el compliment d'aquesta normativa i l'eficàcia dels controls de seguretat, la UMH estableix un sistema de revisió contínua:

1. Auditories internes: La direcció TI i el responsable de seguretat han de revisar periòdicament els sistemes i processos per a detectar desviacions, verificar el compliment de les polítiques d'accés i avaluar-ne la robustesa tècnica.

2. Auditoria externa: La Universitat s'ha de sotmetre, segons la periodicitat legal exigida, a una auditoria externa duta a terme per entitats independents. Aquesta avaluació verifica el compliment de l'Esquema Nacional de Seguretat (ENS) i altres estàndards adoptats.

2. Plan de Renovación de Hardware corporativo: La Dirección TI, bajo la supervisión de la Comisión de Seguridad y de la de Cartera de Proyectos, establecerá un plan plurianual de renovación de equipos (servidores, ordenadores, dispositivos de red). El objetivo es sustituir aquellos activos que, por antigüedad, supongan un riesgo de fallo o una caída en la productividad.

3. Gestión de Software y Licencias: Se priorizará el uso de software corporativo y soluciones que garanticen la escalabilidad. Se realizará un inventario periódico para identificar y retirar aquel software que haya dejado de recibir soporte por parte del fabricante.

4. Baja y Eliminación Segura: Cuando un equipo o software llegue al final de su vida útil, su retirada se realizará siguiendo protocolos de:
- Seguridad: Borrado seguro y certificado de los datos contenidos en los soportes físicos.
- Sostenibilidad: Gestión de residuos electrónicos conforme a la normativa medioambiental vigente.

5. Estandarización: Para optimizar el mantenimiento, la UMH definirá catálogos de hardware y software estándar. Cualquier excepción por necesidades específicas de investigación deberá ser validada técnicamente para asegurar su compatibilidad y seguridad.

TÍTULO VI: AUDITORÍA Y RÉGIMEN DE RESPONSABILIDAD

Artículo 17. Supervisión, Control y Auditoría

Para garantizar el cumplimiento de esta normativa y la eficacia de los controles de seguridad, la UMH establece un sistema de revisión continua:

1. Auditorías Internas: La Dirección TI y el Responsable de Seguridad realizarán revisiones periódicas de los sistemas y procesos para detectar desviaciones, verificar el cumplimiento de las políticas de acceso y evaluar la robustez técnica.

2. Auditoría Externa: La Universidad se someterá según la periodicidad legal exigida a una auditoría externa realizada por entidades independientes. Esta evaluación verificará el cumplimiento del Esquema Nacional de Seguridad (ENS) y otros estándares adoptados.

3. Informes de control: Els resultats d'aquestes auditories s'han de plasmar en un informe tècnic que s'eleva a l'Equip de Govern. L'informe ha d'incloure un pla de mesures correctores per a esmenar les deficiències detectades.

4. Revisió de les comissions: Les comissions esmentades en el títol III avaluen anualment els seus propis indicadors de gestió (KPI) per a assegurar que estan complint els objectius estratègics de la Universitat.

5. Millora contínua: Les troballes de les auditories han de servir de base per a actualitzar aquesta normativa i el Pla estratègic TI, i assegurar que la UMH evolucione davant de les noves amenaces i els reptes tecnològics.

Article 18. Règim de responsabilitat

L'ús indegut dels recursos tecnològics o l'incompliment de les directrius de seguretat que s'hi exposen podrien donar lloc a les responsabilitats disciplinàries, administratives en matèria de protecció de dades, civils o penals que corresponguen segons la legislació vigent.

Disposició final

Aquesta normativa entra en vigor l'endemà de la publicació en el *Butlletí Oficial de la UMH* (BOUMH).

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

3. Informes de Control: Los resultados de estas auditorías se plasmarán en un informe técnico que será elevado al Equipo de Gobierno. El informe incluirá un plan de medidas correctoras para subsanar las deficiencias detectadas.

4. Revisión de las comisiones: Las comisiones citadas en el título III evaluarán anualmente sus propios indicadores de gestión (KPIs) para asegurar que están cumpliendo los objetivos estratégicos de la Universidad.

5. Mejora Continua: Los hallazgos de las auditorías servirán de base para actualizar esta normativa y el Plan Estratégico TI, asegurando que la UMH evolucione ante las nuevas amenazas y retos tecnológicos.

Artículo 18. Régimen de Responsabilidad.

El uso indebido de los recursos tecnológicos o el incumplimiento de las directrices de seguridad aquí expuestas podrían dar lugar a las responsabilidades disciplinarias, administrativas en materia de protección de datos, civiles o penales que correspondan según la legislación vigente.

Disposición Final

La presente normativa entrará en vigor al día siguiente de su publicación en el *Boletín Oficial de la UMH* (BOUMH).

Lo que comunico para su conocimiento y efectos oportunos.

LA SECRETÀRIA GENERAL

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