Títol: NORMATIVA DE SEGURETAT I ÚS DELS RECURSOS INFORMÀTICS I DE COMUNICACIONS DE LA UNIVERSITAT D'ALACANT

Secció: DISPOSICIONS GENERALS

Òrgan: Consell de Govern

Data d'aprovació: dijous, 26 de setembre de 2024

Aprovada per unanimitat pel Consell de Govern de la Universitat d'Alacant en la sessió ordinària del dia 26 de setembre de 2024.

NORMATIVA DE SEGURETAT I ÚS DELS RECURSOS INFORMÀTICS I DE COMUNICACIONS DE LA UNIVERSITAT D'ALACANT

Título: NORMATIVA DE SEGURIDAD Y USO DE LOS RECURSOS INFORMÁTICOS Y DE COMUNICACIONES DE LA UNIVERSIDAD DE ALICANTE

Sección: DISPOSICIONES GENERALES

Órgano: Consejo de Gobierno

Fecha de aprobación: jueves, 26 de septiembre de 2024

Aprobada por unanimidad por el Consejo de Gobierno de la Universidad de Alicante en la sesión ordinaria del día 26 de septiembre de 2024.

NORMATIVA DE SEGURIDAD Y USO DE LOS RECURSOS INFORMÁTICOS Y DE COMUNICACIONES DE LA UNIVERSIDAD DE ALICANTE

Responsabilitats i mesures que cal adoptar

Article 18. Responsabilitats

Article 19. Incompliment

Disposició addicional

Disposició derogatòria

Disposició final primera

Disposició final segona

Annex

Preàmbul

D'acord amb el que disposa el Reial decret 311/2022, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (ENS), aquest document conté la Normativa de Seguretat i ús dels recursos i els serveis informàtics de la Universitat d'Alacant (UA), gestionats o sota la responsabilitat de la UA, i assenyala, així mateix, els compromisos que adquireixen les persones usuàries respecte a la seua seguretat i bon ús.

La utilització d'equipament informàtic i de comunicacions és actualment una necessitat en qualsevol organització del sector públic. Atès que aquests recursos i serveis són àmpliament utilitzats i que la xarxa informàtica sobre la qual estan suportats està integrada, al seu torn, en altres d'una índole més àmplia (especialment Xarxa IRIS) es fa necessària l'aprovació d'una normativa que, partint de l'adequació a la legislació vigent, aclarisca la forma correcta d'ús d'aquests, delimite les responsabilitats i proporcione un marc per a la regulació de l'ús de cadascun d'aquests.

El 8 de maig de l'any 2007 el Consell de Govern de la Universitat d'Alacant (UA) va aprovar la normativa "CONDICIONS D'ÚS DELS RECURSOS INFORMÀTICS I DE COMUNICACIONS DE LA UNIVERSITAT D'ALACANT". El 15 de desembre del 2022, el Consell de Govern va aprovar la Política de Seguretat de la Universitat d'Alacant que suposa el marc general sobre el tractament de la seguretat de la informació en l'àmbit de la UA i estableix, en l'article 12, que s'ha de desenvolupar i complementar amb normes, procediments i instruccions més específiques.

Aquesta norma substitueix l'aprovada el 8 de maig del 2007 i està alineada amb la nova Política de Seguretat i amb el marc normatiu establit ENS.

TÍTOL PRELIMINAR

Objecte i àmbit d'aplicació

Article 1. Objecte

D'acord amb el que disposa el Reial decret 311/2022 pel qual es regula l'ENS, l'objectiu d'aquesta normativa és regular l'ús dels recursos i els serveis informàtics que la UA proporciona a la comunitat universitària per a la seua utilització en activitats acadèmiques, d'investigació, desenvolupament i innovació, incloent les tasques administratives associades de la UA i també garantir la qualitat i la seguretat dels nostres serveis informàtics i de comunicacions.

Article 2. Àmbit d'aplicació

1. L'àmbit d'aplicació d'aquesta normativa arriba a la totalitat de la comunitat universitària, com també a totes aquelles persones que fan ús dels sistemes informàtics i de comunicacions de la Universitat d'Alacant o dels serveis proporcionats per aquests. Qualsevol persona que utilitze els recursos informàtics i de comunicacions de la UA, de manera permanent o eventual, queda subjecta a les normes i les condicions contingudes en aquest document.

2. Així mateix, l'exposat en aquesta normativa s'aplicarà també a tots els dispositius connectats a la infraestructura de la UA o amb adreçament IP dins del rang de la UA o que estiga sota el domini ua.es.

Responsabilidades y medidas a adoptar

Artículo 18. Responsabilidades

Artículo 19. Incumplimiento

Disposición adicional

Disposición derogatoria

Disposición final primera

Disposición final segunda

Anexo

Preámbulo

Conforme a lo dispuesto en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), este documento contiene la Normativa de Seguridad y uso de los recursos y servicios informáticos de la Universidad de Alicante (UA), gestionados o bajo la responsabilidad de la UA, señalando asimismo los compromisos que adquieren sus usuarios y usuarias respecto a su seguridad y buen uso.

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Dado que estos recursos y servicios son ampliamente utilizados y que la red informática sobre la que están soportados está integrada a su vez en otras de índole más amplia (en especial Red IRIS) se hace necesaria la aprobación de una normativa que, partiendo de la adecuación a la legislación vigente, clarifique la forma correcta de uso de los mismos, delimite las responsabilidades y proporcione un marco para la regulación del uso de cada uno de ellos.

El 8 de mayo de 2007 el Consejo de Gobierno de la Universidad de Alicante (UA) aprobó la normativa "CONDICIONES DE USO DE LOS RECURSOS INFORMÁTICOS Y DE COMUNICACIONES DE LA UNIVERSIDAD DE ALICANTE". El 15 de diciembre de 2022, el Consejo de Gobierno aprobó la Política de Seguridad de la Universidad de Alicante que supone el marco general sobre el tratamiento de la seguridad de la información en el ámbito de la UA y establece, en su artículo 12, que se debe desarrollar y complementar con normas, procedimientos e instrucciones más específicas.

Esta norma sustituye a la aprobada el 8 de mayo del 2007 y está alineada con la nueva Política de Seguridad y con el marco normativo establecido ENS.

TÍTULO PRELIMINAR

Objeto y ámbito de aplicación

Artículo 1. Objeto

Conforme a lo dispuesto en el Real Decreto 311/2022 por el que se regula el ENS, el objetivo de esta normativa es regular el uso de los recursos y servicios informáticos que la UA proporciona a la comunidad universitaria para su utilización en actividades académicas, de investigación, desarrollo e innovación, incluyendo las tareas administrativas asociadas de la UA y así como garantizar la calidad y seguridad de nuestros servicios informáticos y de comunicaciones.

Artículo 2. Ámbito de aplicación

1. El ámbito de aplicación de la presente normativa alcanza a la totalidad de la comunidad universitaria, así como a todas aquellas personas que hacen uso de los sistemas informáticos y de comunicaciones de la Universidad de Alicante o de los servicios proporcionados por éstos. Cualquier persona que utilice los recursos informáticos y de comunicaciones de la UA, de manera permanente o eventual, queda sujeta a las normas y condiciones contenidas en este documento.

2. Así mismo, lo expuesto en esta normativa se aplicará también a todos los dispositivos conectados a la infraestructura de la UA o con direccionamiento IP dentro del rango de la UA o que esté bajo el dominio ua.es.

Article 3. Revisió i avaluació

1. La persona responsable del Servei definida en la Política de Seguretat de la Informació de la UA és competent per a:

· Interpretar els dubtes que puguen sorgir en l'aplicació d'aquesta norma.

· Revisar-la quan siga necessari per a actualitzar-ne el contingut o quan es complisquen els terminis màxims establits per a això.

· Verificar-ne l'efectivitat.

2. Amb una periodicitat mínima anual, es revisarà aquesta normativa amb la finalitat d'identificar oportunitats de millora en la gestió de la qualitat dels processos de seguretat de la informació o adaptar-la als canvis haguts en el marc legal, infraestructura tecnològica, organització general, etc.

TÍTOL I

Normes d'ús dels recursos i els serveis informàtics

Article 4. Identificació i autenticació en els recursos i serveis

1.- La utilització de recursos i serveis de la UA es fa a través de comptes personals i intransferibles creats per a aquesta finalitat, i està prohibit l'ús d'aquests comptes per persones alienes al seu titular ja siga amb el seu consentiment o sense aquest.

2.- Podran existir comptes institucionals d'unitats per a tasques i accés a recursos d'aquestes unitats i el responsable de les quals serà la persona responsable de la unitat.

CAPÍTOL 1

Ús dels recursos informàtics i de comunicacions de la UA

Article 5. Condicions d'ús generals

1.- La utilització dels recursos informàtics i de comunicacions de la UA està subjecta a l'ordenament jurídic, especialment en matèria de protecció de dades de caràcter personal, propietat intel·lectual i industrial i protecció de l'honor i la intimitat i, si escau, a les pròpies de la UA. El personal usuari de la UA que, d'acord amb la seua activitat professional o acadèmica, poguera tindre accés a dades de caràcter personal, està obligat a guardar la confidencialitat deguda sobre aquestes; aquest deure es mantindrà de manera indefinida, fins i tot més enllà de la relació amb la UA.

Article 6. Criteris generals d'utilització

1. Els recursos informàtics i dispositius de comunicacions, tant fixos com mòbils, i la informació, programes i altres serveis informàtics proporcionats a les persones usuàries per al desenvolupament de l'activitat professional o docent han d'utilitzar-se exclusivament per al desenvolupament de les funcions encomanades.

2. Com a norma general, els equips informàtics propietat de la UA s'instal·len i configuren sota la supervisió o directrius del personal tècnic del Servei d'Informàtica de la UA. Seguint el principi de "mínim privilegi" s'ha de limitar en la mesura que siga possible la capacitat que la persona usuària puga fer canvis en la configuració. Tot i això, quan, per raons justificades, dispose de permisos per a administrar l'equip propietat de la UA, la persona usuària serà responsable de complir amb les directrius generals del "Procediment d'accés local i remot" de la UA i les següents:

a) Actualitzar els sistemes operatius i aplicacions, per al que comptarà, si és necessari, amb l'ajuda del Centre d'Atenció a l'Usuari del Servei d'Informàtica de la UA

b) Instal·lar i mantenir actualitzades les eines de seguretat corporatives que li proporcione el Servei d'Informàtica de la UA, per a la qual cosa comptarà, si és necessari, amb l'ajuda del Centre d'Atenció a l'Usuari del Servei d'Informàtica de la UA

Artículo 3. Revisión y evaluación

1. La persona Responsable del Servicio definida en la Política de Seguridad de la Información de la UA es competente para:

· Interpretar las dudas que puedan surgir en la aplicación de la presente norma.

· Proceder a su revisión cuando sea necesario para actualizar su contenido o cuando se cumplan los plazos máximos establecidos para ello.

· Verificar su efectividad.

2. Con una periodicidad mínima anual, se revisará la presente normativa con la finalidad de identificar oportunidades de mejora en la gestión de la calidad de los procesos de seguridad de la información o adaptar a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

TÍTULO I

Normas de uso de los recursos y servicios informáticos

Artículo 4. Identificación y autenticación en los recursos y servicios

1.- La utilización de recursos y servicios de la UA se realiza a través de cuentas personales e intransferibles creadas para tal fin, estando prohibido el uso de dichas cuentas por personas ajenas a su titular ya sea con o sin su consentimiento.

2.- Podrán existir cuentas institucionales de unidades para tareas y acceso a recursos de dichas unidades y cuyo responsable será el o la responsable de la unidad.

CAPÍTULO 1

Uso de los recursos informáticos y de comunicaciones de la UA

Artículo 5. Condiciones de uso generales

1.- La utilización de los recursos informáticos y de comunicaciones de la UA está sujeta al ordenamiento jurídico, especialmente en materia de protección de datos de carácter personal, propiedad intelectual e industrial y protección del honor e intimidad y, en su caso, a las propias de la UA. El personal usuario de la UA que, en virtud de su actividad profesional o académica, pudiera tener acceso a datos de carácter personal, está obligado a guardar la confidencialidad debida sobre los mismos; deber que se mantendrá de manera indefinida, incluso más allá de la relación con la UA.

Artículo 6. Criterios generales de utilización

1. Los recursos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, y la información, programas y otros servicios informáticos proporcionados a las y los usuarios para el desarrollo de su actividad profesional o docente deben utilizarse exclusivamente para el desarrollo de las funciones encomendadas.

2. Como norma general, los equipos informáticos propiedad de la UA se instalan y configuran bajo la supervisión y/o directrices del personal técnico del Servicio de Informática de la UA. Siguiendo el principio de "mínimo privilegio" se debe limitar en la medida de lo posible la capacidad de que la persona usuaria pueda realizar cambios en su configuración. Aún así, cuando, por razones justificadas, disponga de permisos para administrar el equipo propiedad de la UA, la persona usuaria será responsable de cumplir con las directrices generales del "Procedimiento de acceso local y remoto" de la UA y las siguientes:

a) Actualizar los sistemas operativos y aplicaciones, para lo que contará, si es necesario, con la ayuda del Centro de Atención al Usuario del Servicio de Informática de la UA

b) Instalar y mantener actualizado las herramientas de seguridad corporativas que le proporcione el Servicio de Informática de la UA, para lo que contará, si es necesario, con la ayuda del Centro de Atención al Usuario del Servicio de Informática de la UA

c) Instal·lar únicament programes per als quals la UA té llicència d'ús, bé perquè és programari lliure o perquè s'haja adquirit. No es permet instal·lar programari per al qual no es dispose de llicència, ni executar o guardar arxius que no siguen de confiança.

d) Complir amb els procediments, les instruccions i les recomanacions del Servei d'Informàtica, les existents i les que pogueren publicar posteriorment i hi siguen aplicables:

- les directrius indicades del document "Protecció del lloc de treball informàtic" i del "Lloc de treball buidat i equip bloquejat". Especialment important és que l'equip o lloc de treball caldrà:

· Configurar perquè es bloquege al cap d'un temps prudencial d'inactivitat, i que requerisca una nova autenticació de la persona usuària per a reprendre l'activitat en curs.

· Apagar, excepte causa justificada, fora de la jornada laboral de la persona usuària.

- Procediment per a l'esborrat i la destrucció de suports d'emmagatzematge d'informació" i "Procediment d'ofuscació de dades i eliminació de metadades"

- "Procediment de gestió d'incidents de seguretat en la UA"

e) Eliminar serveis o aplicacions no necessàries: Els equips informàtics hauran de comptar amb els serveis i les aplicacions mínimes necessàries per al desenvolupament de les funcions exercides per a la persona usuària. Si una aplicació no és necessària per al seu treball, no ha d'estar instal·lada i des del Servei d'Informàtica se li'n podrà requerir la desinstal·lació.

f) Protegir l'equip davant d'accessos remots seguint el "Procediment d'accés local i remot de la UA". En cas de ser necessari, es farà exclusivament utilitzant els mecanismes definits pel Servei d'Informàtica en aquest procediment i aplicant les instruccions tècniques de seguretat que s'hagen publicat.

3. Les persones usuàries dels recursos informàtics i de comunicacions de la UA hauran de facilitar, tant el personal de suport tècnic com el de resposta a incidents, l'accés als seus equips informàtics propietat de la UA per a faenes de reparació, instal·lació, manteniment o resolució de ciberincidents. Si el personal detectara qualsevol anomalia que indicara una utilització dels recursos contrària a aquesta norma, ho posarà en coneixement de la persona definida com a responsable de Seguretat o del responsable del Sistema en la Política de Seguretat de la UA, que prendran les oportunes mesures correctores.

4. Les persones usuàries dels recursos informàtics i de comunicacions de la UA hauran de fer un ús adequat dels mitjans materials posats a la seua disposició, assumir la responsabilitat de l'ús adequat d'aquests i procurar els coneixements imprescindibles per al maneig segur i bon ús dels sistemes d'informació.

5. Les persones usuàries dels recursos informàtics i de comunicacions de la UA hauran de notificar, com més prompte millor, qualsevol comportament anòmal del seu ordinador personal, especialment quan hi haja sospites que s'haja produït algun incident de seguretat en aquest. Per a això, hauran de seguir el que indicat el "Procés de Gestió d'Incidents de Seguretat de la UA".

c) Instalar únicamente programas para los cuales la UA tiene licencia de uso, bien porque sea software libre o porque se haya adquirido. No se permite instalar software para el cual no se disponga de licencia, ni ejecutar o guardar archivos no confiables.

d) Cumplir con los procedimientos, instrucciones y recomendaciones del Servicio de Informática, las existentes y las que pudieran publicarse posteriormente y le sean de aplicación:

- las directrices indicadas del documento "Protección del puesto de trabajo informático" y del "Puesto de trabajo despejado y equipo bloqueado". Especialmente importante es que el equipo o puesto de trabajo se deberá:

· Configurar para que se bloquee al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

· Apagar, salvo causa justificada, fuera de la jornada laboral de la persona usuaria.

- "Procedimiento para el borrado y la destrucción de soportes de almacenamiento de información" y "Procedimiento de ofuscación de datos y eliminación de metadatos"

- "Procedimiento de gestión de incidentes de seguridad en la UA"

e) Eliminar servicios o aplicaciones no necesarias: Los equipos informáticos deberán contar con los servicios y aplicaciones mínimas necesarias para el desarrollo de las funciones desempeñadas por el usuario o usuaria. Si una aplicación no es necesaria para su trabajo, no debe estar instalada y desde el Servicio de Informática se le podrá requerir la desinstalación de ésta.

f) Proteger el equipo ante accesos remotos siguiendo el "Procedimiento de acceso local y remoto de la UA". En caso de ser necesario, se hará exclusivamente utilizando los mecanismos definidos por el Servicio de Informática en dicho procedimiento y aplicando las instrucciones técnicas de seguridad que se hayan publicado.

3. Las personas usuarias de los recursos informáticos y de comunicaciones de la UA deberán facilitar, tanto al personal de soporte técnico como al de respuesta a incidentes, el acceso a sus equipos informáticos propiedad de la UA para labores de reparación, instalación, mantenimiento o resolución de ciberincidentes. Si el personal detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento de la persona definida como Responsable de Seguridad y/o del Responsable del Sistema en la Política de Seguridad de la UA, que tomarán las oportunas medidas correctoras.

4. Las personas usuarias de los recursos informáticos y de comunicaciones de la UA deberán realizar un adecuado uso de los medios materiales puestos a su disposición, asumiendo la responsabilidad del uso adecuado de los mismos, procurándose los conocimientos imprescindibles para el manejo seguro y buen uso de los sistemas de información.

5. Las personas usuarias de los recursos informáticos y de comunicaciones de la UA deberán notificar, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Para ello, deberán seguir lo indicado en el "Proceso de Gestión de Incidentes de Seguridad de la UA".

6. La persona usuària serà responsable de tota la informació extreta fora de l'organització a través de dispositius mòbils, emmagatzematge o serveis en el núvol. És imprescindible un ús responsable d'aquests, especialment quan es tracte informació sensible, confidencial o protegida. Per a això caldrà seguir les directrius de la "Normativa de qualificació de la Informació de la UA" i les proteccions que s'indiquen. A més, haurà d'eliminar de manera segura, seguint el "Procediment per a l'esborrat i la destrucció de suports d'emmagatzematge d'informació", les dades i la informació sensible, confidencial o protegida, que pogueren emmagatzemar en aquests equips.

7. Amb caràcter general, la informació emmagatzemada de manera local en els ordinadors personals no serà objecte de salvaguarda mitjançant cap procediment corporatiu de còpia de seguretat. Per tant, quan aquest emmagatzematge estiga autoritzat en les normes internes corresponents, es recomana a les persones usuàries la realització periòdica de còpies de seguretat, especialment de la informació important per al desenvolupament de la seua activitat professional.

8. No està permès emmagatzemar informació privada, de qualsevol naturalesa, en els recursos d'emmagatzematge compartits o locals, excepte autorització prèvia.

9. En cas de robatori o pèrdua de l'equip s'ha de comunicar immediatament a la Gerència de la Universitat.

SECCIÓ 1a ACCÉS I ÚS DE LA XARXA DE LA UA

Article 7. Sobre l'accés i l'ús de la xarxa de la UA

1. Només està permesa la connexió a la xarxa cablejada de la UA d'equips informàtics inventariats en la mateixa Universitat, a excepció del que indica l'article 8 d'aquesta normativa.

2. Per a la connexió a aquesta xarxa se seguirà, a més de l'indicat en aquesta normativa i totes les que siguen aplicable, les directrius que marque el Servei d'Informàtica de la UA.

3. En el cas dels servidors aliens al Servei d'Informàtica de la UA (entenent aquest tipus de servidors com els servidors no gestionats pel personal del Servei d'Informàtica), ha de quedar clarament definida la persona que actua com a responsable d'aquest, a més de complir amb la normativa específica desenvolupada a aquest efecte ("Normativa de seguretat i ús dels servidors aliens al Servei d'Informàtica de la Universitat d'Alacant"). Aquesta persona haurà de respondre davant d'incidències i incompliment d'aquesta normativa, com també de les normes aplicables vigents.

4. No està permesa la instal·lació i la posada en funcionament de xarxes d'àrea local (cablejades o no) sense l'autorització expressa del Vicerectorat amb competències en TI. Aquestes xarxes han de complir aquesta normativa i la normativa específica desenvolupada a aquest efecte, si n'hi haguera.

5. La xarxa de la UA només tindrà enllaços amb Internet l'administració i correcte funcionament de la qual siga responsabilitat del Servei d'Informàtica de la UA. El punt de presència en Internet principal serà el proporcionat per RedIRIS raó per la qual les persones usuàries de la xarxa no han d'utilitzar aquesta infraestructura i serveis per a altres usos que no siguen els permesos en la política d'ús de RedIRIS (publicada en el portal web de RedIRIS) o els necessaris per a l'acompliment de la seua activitat.

Article 8. Connexió d'equips a la xarxa de la UA

1. De manera excepcional es podrà permetre la connexió d'altres equips i dispositius aliens a la UA, amb una duració limitada en el temps, sempre que estiga degudament justificada; l'autorització correspondrà a la persona responsable de Seguretat o responsable del Sistema definida en la Política de Seguretat de la Informació de la UA. Això només s'exceptua en els casos següents:

a) Les sales d'actes o sales similars per al personal extern que proporcione xarrades, lectures etc. en les condicions d'ús establides per a aquestes dependències i serveis.

6. El usuario o usuaria será responsable de toda la información extraída fuera de la organización a través de dispositivos móviles, almacenamiento o servicios en la nube. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida. Para ello deberá seguir las directrices de la "Normativa de calificación de la Información de la UA" y las protecciones que se indican. Además, deberá eliminar de forma segura, siguiendo el "Procedimiento para el borrado y la destrucción de soportes de almacenamiento de información", los datos y la información sensible, confidencial o protegida, que pudieran almacenarse en estos equipos.

7. Con carácter general, la información almacenada de forma local en los ordenadores personales no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a las y los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.

8. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa.

9. En caso de robo o extravío del equipo se debe comunicar inmediatamente a la Gerencia de la Universidad.

SECCIÓN 1ª ACCESO Y USO DE LA RED DE LA UA

Artículo 7. Sobre el acceso y uso de la red de la UA

1. Solo está permitida la conexión a la red cableada de la UA de equipos informáticos inventariados en la propia Universidad, a excepción de lo indicado en el artículo 8 de esta normativa.

2. Para la conexión a dicha red se seguirá, además de lo indicado en la presente normativa y todas las que sean de aplicación, las directrices que marque el Servicio de Informática de la UA.

3. En el caso de los servidores ajenos al Servicio de Informática de la UA (entendiendo este tipo de servidores como los servidores no gestionados por el personal del Servicio de Informática), debe quedar claramente definida la persona que actúa como responsable del mismo, además de cumplir con la normativa específica desarrollada a tal efecto ("Normativa de seguridad y uso de los servidores ajenos al Servicio de Informática de la Universidad de Alicante"). Esta persona deberá responder ante incidencias e incumplimiento de esta normativa, así como de las normas aplicables vigentes.

4. No está permitida la instalación y puesta en funcionamiento de redes de área local (cableadas o no) sin la autorización expresa del Vicerrectorado con competencias en TI. Estas redes deben cumplir con la presente normativa y con la normativa específica desarrollada a tal efecto, si la hubiera.

5. La red de la UA sólo tendrá enlaces con Internet cuya administración y correcto funcionamiento sea responsabilidad del Servicio de Informática de la UA. El punto de presencia en Internet principal será el proporcionado por RedIRIS por lo que las y los usuarios de la red no deben utilizar esta infraestructura y servicios para otros usos que no sean los permitidos en la Política de uso de RedIRIS (publicada en el portal web de RedIRIS) o los propios necesarios para el desempeño de su actividad.

Artículo 8. Conexión de equipos a la red de la UA

1. De forma excepcional se podrá permitir la conexión de otros equipos y dispositivos ajenos a la UA, con una duración limitada en el tiempo, siempre que esté debidamente justificada; la autorización corresponderá a la persona Responsable de Seguridad y/o Responsable del Sistema definida en la Política de Seguridad de la Información de la UA. Esto solo se exceptúa en los siguientes casos:

a) los salones de actos o salas similares para el personal externo que proporcione charlas, lecturas etc. en las condiciones de uso establecidas para estas dependencias y servicios.

b) Les aules i laboratoris d'informàtica que s'hagen habilitat per a aquesta finalitat i en les condicions d'ús que s'hagen establit.

c) Equipament propietat del personal de la UA adscrit a un pla de teletreball

d) A la xarxa sense fil de la universitat (xarxa eduroam).

e) Sol·licituds autoritzades pel Vicerectorat amb competències en TI.

2. Qualsevol equip informàtic de propietat particular que es connecte a la xarxa de la UA ha de complir aquesta normativa, el "Procediment d'accés local i remot" i les normatives d'ús particulars si n'hi haguera, com també la resta d'instruccions que la desenvolupen. A més, aquestes connexions només es poden fer mitjançant els mecanismes que el Servei d'Informàtica de la UA hi proporcione.

3. Tots els equips que es connecten a la xarxa de la UA han de rebre una adreça IP assignada pel Servei d'Informàtica, a més de ser inclosos en el registre corresponent. No està permesa la connexió d'equips amb direccions no registrades.

4. Les persones usuàries que utilitzen dispositius personals per a connectar a recursos de la UA, han d'assegurar que aquest dispositiu compleix amb els requisits mínims de seguretat establits pel Servei d'Informàtica de la UA.

5. Així mateix, les persones usuàries que utilitzen dispositius personals són responsables de la informació institucional i de caràcter personal que pogueren manejar en aquests dispositius, i estan obligats a conèixer i complir les normes associades i aplicar les mesures de protecció que garantisquen els nivells de seguretat adequats a aquesta informació.

CAPÍTOL II

Ús inapropiat dels recursos

Article 9. Ús incorrecte dels recursos

1. En l'ús dels recursos i serveis informàtics de la UA, les persones usuàries han de respectar els Estatuts de la Universitat, l'ordenament jurídic i els drets reconeguts en la Constitució espanyola.

2. A més del que hem indicat abans, es considera un mal ús o ús inacceptable aquella actuació de la persona usuària que pot afectar la disponibilitat d'un servei, al treball de la resta d'usuaris i usuàries, a la confidencialitat i integritat de la informació o que, en general, pose en risc qualsevol de les dimensions de seguretat (disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat) de la informació i els serveis.

3. A més dels usos incorrectes abans indicats, es consideren també mals usos els que es relacionen en els articles següents, 10, 11, 12 i 13.

Article 10. Ús inadequat en relació amb la finalitat i naturalesa de l'ús

1. L'ús dels recursos per a finalitats privades, personals, lúdiques o altres no estrictament relacionats amb les activitats pròpies de la UA, llevat que medie autorització.

2. L'ús amb finalitats comercials no relacionat amb les activitats pròpies de la UA i no degudament autoritzat.

3. Transmetre contingut il·legal de qualsevol tipus i, particularment, difondre continguts de caràcter racista, xenòfob, pornogràfic, sexista, d'apologia del terrorisme, perillós, amenaçador, difamatori, obscè, que atempte contra els drets humans o actue en perjudici dels drets a la intimitat, a l'honor, a la imatge pròpia o contra la dignitat de les persones i a la protecció de les dades de caràcter personal.

4. La distribució i ús de material que viole els drets de propietat intel·lectual.

b) las aulas y laboratorios de informática que se hayan habilitado para tal fin y en las condiciones de uso que se hayan establecido.

c) Equipamiento propiedad del personal de la UA adscrito a un plan de teletrabajo

d) A la red inalámbrica de la universidad (red eduroam).

e) Solicitudes autorizadas por el vicerrectorado con competencias en TI.

2. Todo equipo informático de propiedad particular que se conecte a la red de la UA debe cumplir esta normativa, el "Procedimiento de acceso local y remoto" y las normativas de uso particulares si las hubiera, así como el resto de instrucciones que la desarrollen. Además, estas conexiones solo se pueden realizar mediante los mecanismos que el Servicio de Informática de la UA proporcione.

3. Todos los equipos que se conectan a la red de la UA deben recibir una dirección IP asignada por el Servicio de Informática, además de ser incluidos en el registro correspondiente. No está permitida la conexión de equipos con direcciones no registradas.

4. Las personas usuarias que utilicen dispositivos personales para conectarse a recursos de la UA, deben asegurarse que dicho dispositivo cumple con los requisitos mínimos de seguridad establecidos por el Servicio de Informática de la UA.

5. Así mismo, las personas usuarias que utilicen dispositivos personales son responsables de la información institucional y de carácter personal que pudieran manejar en dichos dispositivos, estando obligados a conocer y cumplir las normas asociadas y de aplicar las medidas de protección que garanticen los niveles de seguridad adecuados a dicha información.

CAPÍTULO II

Uso inapropiado de los recursos

Artículo 9. Uso incorrecto de los recursos

1. En el uso de los recursos y servicios informáticos de la UA, las y los usuarios tienen que respetar los Estatutos de la Universidad, el ordenamiento jurídico y los derechos reconocidos en la Constitución española.

2. Además de lo antes indicado, se considera un mal uso o uso inaceptable a aquella actuación de la persona usuaria que puede afectar a la disponibilidad de un servicio, al trabajo del resto de usuarios y usuarias, a la confidencialidad e integridad de la información o que, en general, ponga en riesgo cualquiera de las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) de la información y los servicios.

3. Además de los usos incorrectos antes indicados, se consideran también malos usos los que se relacionan en los artículos siguientes, 10, 11, 12 y 13.

Artículo 10. Uso inadecuado en relación con la finalidad y naturaleza del uso

1. El uso de los recursos para fines privados, personales, lúdicos u otros no estrictamente relacionados con las actividades propias de la UA, salvo que medie autorización.

2. El uso con fines comerciales no relacionado con las actividades propias de la UA y no debidamente autorizado.

3. Transmitir contenido ilegal de cualquier tipo y, particularmente, difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, peligroso, amenazador, difamatorio, obsceno, atentatorio contra los derechos humanos o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas y a la protección de los datos de carácter personal.

4. La distribución y uso de material que viole los derechos de propiedad intelectual.

5. L'abús deliberat dels recursos posats a la disposició de les persones usuàries.

6. En general, la transmissió d'informació o acte que viole la legislació vigent.

Article 11. Ús inadequat en relació amb confidencialitat i suplantació d'identitat

1. Accedir a dispositius, aplicacions, dades o informació o xarxes per a les quals no estiguen degudament autoritzats. Tampoc hauran de permetre que altres persones ho facen.

2. Fer accions la finalitat de les quals siga l'obtenció de contrasenyes d'altres persones sense el consentiment d'aquestes.

3. Compartir recursos (fitxers, directoris, etc.) sense els mecanismes de seguretat necessaris i disponibles en cada sistema operatiu o aplicacions que garantisquen la seguretat del seu equip i la xarxa.

4. La destrucció, la manipulació o l'apropiació indeguda de la informació que circula per la xarxa o pertanga a altres usuaris o usuàries.

Article 12. Ús inadequat en relació amb la integritat i disponibilitat dels recursos

1. L'intent de causar qualsevol tipus de mal físic o lògic als recursos informàtics de la UA: equips, aplicacions, programes, documentació, etc.

2. El desenvolupament o ús de programes que puguen provocar caigudes o falta de disponibilitat en servidors, equips de xarxa o qualsevol altre recurs (atacs de denegació de servei).

3. El desenvolupament, ús o distribució intencionada de programes l'objectiu dels quals és danyar altres sistemes o accedir a recursos restringits (malware, virus, troians, portes posteriors, etc.) o que puga resultar nociu per al correcte funcionament dels sistemes informàtics de la UA.

4. La modificació no autoritzada de permisos o privilegis en sistemes informàtics.

5. La instal·lació de programes sense la llicència corresponent en els ordinadors de la UA.

Article 13. Ús inadequat en relació amb l'ús de les infraestructures i la xarxa de la UA

1. La connexió d'equips de xarxa actius (hubs, commutadors, encaminadors) que pertorbe el correcte funcionament de la xarxa de la UA o comprometa la seguretat, excepte autorització expressa del Vicerectorat amb competències en Tecnologies de la Informació.

2. Proporcionar accés extern des de la mateixa xarxa de comunicacions, mitjançant la instal·lació de dispositius d'accés remot, excepte expressa autorització del Vicerectorat amb competències en Tecnologies de la Informació

3. L'allotjament de dominis diferents a ua.es, excepte expressa autorització del Vicerectorat amb competències en Tecnologies de la Informació.

4. La instal·lació de servidors telemàtics o d'un altre tipus (web, correu, etc.), sense complir la normativa vigent.

5. La connexió, desconnexió o reubicació d'equips sense l'expressa autorització dels responsables d'aquests.

6. Facilitar l'accés als recursos de xarxa a persones no autoritzades.

7. Utilitzar analitzadors del trànsit que circula per la xarxa de la UA. Igualment està prohibit utilitzar eines de rastreig de ports o que permeten detectar-hi vulnerabilitats. L'ús d'aquestes eines només està permès al personal d'administració de la xarxa i de seguretat de la UA.

5. El abuso deliberado de los recursos puestos a disposición de las y los usuarios.

6. En general, la transmisión de información o acto que viole la legislación vigente.

Artículo 11. Uso inadecuado en relación con confidencialidad y suplantación de identidad.

1. Acceder a dispositivos, aplicaciones, datos o información o redes para los que no estén debidamente autorizados. Tampoco deberán permitir que otros lo hagan.

2. Realizar acciones cuyo fin sea la obtención de contraseñas de otras personas sin el consentimiento de éstas.

3. Compartir recursos (ficheros, directorios, etc.) sin los mecanismos de seguridad necesarios y disponibles en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.

4. La destrucción, manipulación o apropiación indebida de la información que circula por la red o pertenece a otros usuarios o usuarias.

Artículo 12. Uso inadecuado en relación con la integridad y disponibilidad de los recursos

1. El intento de causar cualquier tipo de daño físico o lógico a los recursos informáticos de la UA: equipos, aplicaciones, programas, documentación, etc.

2. El desarrollo o uso de programas que puedan provocar caídas o falta de disponibilidad en servidores, equipos de red o cualquier otro recurso (ataques de denegación de servicio).

3. El desarrollo, uso o distribución intencionada de programas cuyo objetivo es dañar otros sistemas o acceder a recursos restringidos (malware, virus, troyanos, puertas traseras, etc.) o que pueda resultar nocivo para el correcto funcionamiento de los sistemas informáticos de la UA.

4. La modificación no autorizada de permisos o privilegios en sistemas informáticos.

5. La instalación de programas sin la licencia correspondiente en los ordenadores de la UA.

Artículo 13. Uso inadecuado en relación con el uso de las infraestructuras y red de la UA

1. La conexión de equipos de red activos (hubs, conmutadores, routers) que perturbe el correcto funcionamiento de la red de la UA o comprometa la seguridad, salvo expresa autorización del Vicerrectorado con competencias en Tecnologías de la Información.

2. Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto, salvo expresa autorización del Vicerrectorado con competencias en Tecnologías de la Información

3. El alojamiento de dominios distintos a ua.es, salvo expresa autorización del Vicerrectorado con competencias en Tecnologías de la Información.

4. La instalación de servidores telemáticos o de otro tipo (web, correo, etc.), sin cumplir la normativa vigente.

5. La conexión, desconexión o reubicación de equipos sin la expresa autorización de los responsables de los mismos.

6.Facilitar el acceso a los recursos de red a personas no autorizadas.

7. Utilizar analizadores del tráfico que circula por la red de la UA. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido al personal de administración de la red y de seguridad de la UA.

8. No fer un ús racional, eficient i considerat dels recursos disponibles, com ara: l'espai en disc, la memòria, les línies telefòniques, terminals, canals de comunicació, etc.

9. Tecnologies per a emmascarar accions, que no permeten complir amb el Protocol de Retenció de logs de la UA i que no estiguen autoritzades pel Servei d'Informàtica.

TÍTOL II

Condicions de prestació de serveis

Article 14. Limitacions d'ús

1. La UA, a través de l'òrgan amb competències en matèria de Tecnologies de la Informació, podrà establir limitacions respecte a l'ús dels serveis, a fi de mantenir l'operativitat i la disponibilitat dels serveis, sense menyscapte de garantir l'autenticació, la confidencialitat i la integritat de la informació i les comunicacions.

2. Així mateix, quan es detecte un ús incorrecte o no acceptable per part d'alguna persona, es podrà recordar la desconnexió de la xarxa del recurs afectat o bé bloquejar l'accés a determinats serveis.

Article 15. Retenció d'informació sobre el trànsit generat i l'ús dels serveis

1. Per raons de seguretat i operativitat dels serveis informàtics i de comunicacions oferits per la UA i amb l'objectiu de vetlar per la seua correcta utilització, com també complir amb la legalitat vigent, el Servei d'Informàtica farà, amb caràcter ordinari, un seguiment de l'ús d'aquests serveis i recursos, i respectar, en tot cas, el dret a la intimitat i al secret de les comunicacions. Aquest seguiment inclou la generació i arxiu de log, el monitoratge de les comunicacions i quals altres tècniques que permeten determinar i prevenir problemes en el funcionament d'aquests.

2. Es podran aplicar totes les tècniques que es consideren necessàries per a assegurar el funcionament dins de la normalitat (programes de detecció i eliminació de virus, programes de filtre anti-spam...).

3. Els esdeveniments registrats i els terminis de retenció seran els indicats en el "Protocol de retenció de Logs de la UA".

4. La UA, a través de l'òrgan que tinga assumides les competències en aquestes matèries, i previ informe del Servei Jurídic, podrà fer seguiments específics dels accessos que facen les persones usuàries en casos molt justificats que facen necessari un acte d'ingerència imprescindible per al desenvolupament correcte i ordenat de la seua activitat, per a l'esclariment d'infraccions laborals, penals o, si escau, d'una altra naturalesa.

Article 16. Compromís de confidencialitat

1. Tot el personal vinculat a la UA, independentment del tipus de contracte i incloent aquell que pertany a empreses externes amb les quals s'ha establit alguna relació contractual, assumeix un "compromís implícit de confidencialitat" pel qual ha de complir amb l'obligació de secret i confidencialitat respecte als arxius i els continguts a què tinga accés pel seu treball.

2. La confidencialitat de continguts i contrasenyes a què fa referència aquest apartat no exclou la possibilitat que, en estricte compliment dels pertinents requeriments judicials o, si escau, autoritat legalment autoritzada, hagen de revelar els continguts i també la identitat dels autors o autores.

Article 17. Exempció de responsabilitat pel funcionament i ús dels serveis

1. La persona usuària accepta que la UA no té responsabilitat o obligació legal per l'eliminació o error en guardar missatges o altres comunicacions, o qualsevol altre contingut mantingut o transmès pels serveis.

8. No hacer un uso racional, eficiente y considerado de los recursos disponibles, tales como: el espacio en disco, la memoria, las líneas telefónicas, terminales, canales de comunicación, etc.

9. Tecnologías para enmascarar acciones, que no permitan cumplir con el Protocolo de Retención de logs de la UA y que no estén autorizadas por el Servicio de Informática.

TÍTULO II

Condiciones de prestación de servicios

Artículo 14. Limitaciones de uso.

1. La UA, a través del órgano con competencias en materia de Tecnologías de la Información, podrá establecer limitaciones con respecto al uso de los servicios, en aras de mantener la operatividad y disponibilidad de los servicios, sin menoscabo de garantizar la autenticación, confidencialidad e integridad de la información y las comunicaciones.

2. Asimismo, cuando se detecte un uso incorrecto o no aceptable por parte de alguna persona, se podrá acordar la desconexión de la red del recurso afectado o bien bloquear el acceso a determinados servicios.

Artículo 15. Retención de información sobre el tráfico generado y el uso de los servicios.

1. Por razones de seguridad y operatividad de los servicios informáticos y de comunicaciones ofrecidos por la UA y con el objetivo de velar por su correcta utilización, así como cumplir con la legalidad vigente, el Servicio de Informática realizará, con carácter ordinario, un seguimiento del uso de éstos servicios y recursos, respetando, en todo caso, el derecho a la intimidad y al secreto de las comunicaciones. Este seguimiento incluye la generación y archivo de log, la monitorización de las comunicaciones y cuales otras técnicas que permitan determinar y prevenir problemas en el funcionamiento de los mismos.

2. Se podrán aplicar cuantas técnicas se consideren necesarias para asegurar el funcionamiento dentro de la normalidad (programas de detección y eliminación de virus, programas de filtro anti-spam,...).

3. Los eventos registrados y los plazos de retención serán los indicados en el "Protocolo de retención de Logs de la UA".

4. La UA, a través del órgano que tenga asumidas las competencias en estas materias, y previo informe del Servicio Jurídico, podrá efectuar seguimientos específicos de los accesos que realicen las personas usuarias en casos muy justificados que hagan necesario un acto de injerencia imprescindible para el correcto y ordenado desarrollo de su actividad, para el esclarecimiento de infracciones laborales, penales o, en su caso, de otra naturaleza.

Artículo 16. Compromiso de confidencialidad.

1. Todo el personal vinculado a la UA, independientemente del tipo de contrato e incluyendo aquel perteneciente a empresas externas con las que se ha establecido alguna relación contractual, asume un "compromiso implícito de confidencialidad" por el que debe cumplir con la obligación de secreto y confidencialidad respecto a los archivos y los contenidos a los que por su trabajo tenga acceso.

2. La confidencialidad de contenidos y contraseñas a las que se refiere este apartado no excluye la posibilidad de que, en estricto cumplimiento de los pertinentes requerimientos judiciales o, en su caso, autoridad legalmente autorizada, deban revelarse los contenidos, así como la identidad de los autores o autoras.

Artículo 17. Exención de responsabilidad por el funcionamiento y uso de los servicios

1. La persona usuaria acepta que la UA no tiene responsabilidad u obligación legal por la eliminación o fallo al guardar mensajes u otras comunicaciones, o cualquier otro contenido mantenido o transmitido por los servicios.

2. La UA queda eximida de qualsevol responsabilitat pels danys i els perjudicis que pogueren derivar de l'accés, i manipulació eventual, de la informació gestionada mitjançant aquests serveis.

3. La UA queda eximida de qualsevol responsabilitat derivada del mal funcionament dels serveis que tinga l'origen en una circumstància accidental, força major, treballs necessaris de manteniment o qualsevol altra causa no imputable a aquesta.

TÍTOL III

Responsabilitats i mesures que cal adoptar

Article 18. Responsabilitats

1. Cada membre de la UA és responsable de conèixer i complir amb aquesta la normativa i és responsable exclusiu de l'ús que faça dels serveis i els recursos oferits per la UA, i ha de fer-se responsable, en tot cas, de la custòdia de la seua clau d'accés. Així mateix, la persona usuària ha d'assegurar que la seua sessió de treball quede tancada.

2. L'usuari o usuària, quan se li sol·licite, ha de col·laborar amb el personal del Servei d'Informàtica en qualsevol investigació que es faça sobre ciberincidents, mal ús dels recursos o qualsevol investigació que es faça per a esclarir el compliment d'aquesta normativa. Per a això el personal usuari ha d'aportar la informació que se li sol·licite i, quan la situació ho requerisca, permetre l'accés a l'equipament afectat.

3. Les persones usuàries que detecten qualsevol anomalia, ús no autoritzat de la contrasenya o compte, o de qualsevol altre error de seguretat que puga comprometre el bon ús i funcionament dels Sistemes d'Informació de la UA o la seua imatge, hauran d'informar immediatament el Servei d'Informàtica mitjançant els mecanismes indicats en el "Procés de Gestió d'Incidents de la UA" que ho registrarà degudament i elevarà, si escau.

4. El Servei d'Informàtica serà el responsable de definir les mesures de seguretat que han d'instal·lar i configurar en aquests equips, i el personal usuari, d'aplicar-les. Per a qualsevol canvi, la persona responsable de la unitat, servei, departament o centre al qual estiga adscrita la persona usuària haurà de sol·licitar-ho i justificar-ho al Responsable de Sistemes de la UA qui valorarà la idoneïtat d'autoritzar aquests canvis o no.

5. El Servei d'Informàtica de la UA, amb la col·laboració de les altres unitats de la UA, vetlaran pel compliment d'aquesta Normativa i informaran el Comité de Seguretat TI sobre els incompliments o deficiències de seguretat observats, amb la finalitat que es prenguen les mesures oportunes.

Article 19. Incompliment

1. Si el personal del Servei d'Informàtica detecta l'existència d'un mal ús dels recursos o un ciberincident i aquest procedeix de les activitats d'una persona usuària determinada, pot prendre les mesures següents per a protegir les altres persones usuàries i, en general, la infraestructura tecnològica de la UA:

a) Notificar la incidència al personal afectat i també a la persona responsable de la unitat a què estiga adscrit.

b) Informar el Comité de Seguretat TI i els òrgans de govern corresponents del succés perquè adopten les mesures disciplinàries que consideren.

c) Suspendre o restringir l'accés o l'ús dels recursos, temporalment o definitiva. Quan la suspensió de l'ús dels recursos i serveis informàtics, siga una mesura preventiva que calga adoptar com a conseqüència d'un ús inadequat d'aquests, el Comité de Seguretat serà l'òrgan competent per a acordar, de forma motivada, aquesta suspensió. Una vegada valorat el risc per part d'aquest Comité, s'iniciaria d'ofici el procediment de suspensió corresponent d'ús dels recursos TI i es traslladarà a la persona interessada de la presumpta infracció perquè faça les al·legacions que crega pertinents en els terminis establits.

2. La UA queda eximida de cualquier responsabilidad por los daños y perjuicios que pudieran derivarse del acceso, y eventual manipulación, de la información gestionada mediante estos servicios.

3. La UA queda eximida de cualquier responsabilidad derivada del mal funcionamiento de los servicios que tenga su origen en una circunstancia accidental, fuerza mayor, trabajos necesarios de mantenimiento o cualquier otra causa no imputable a la misma.

TÍTULO III

Responsabilidades y medidas a adoptar

Artículo 18. Responsabilidades

1. Cada miembro de la UA es responsable de conocer y cumplir con la presente la normativa y es responsable exclusivo del uso que realice de los servicios y recursos ofrecidos por la UA, debiendo en todo caso hacerse responsable de la custodia de su clave de acceso. Asimismo, la o el usuario debe asegurarse de que su sesión de trabajo quede cerrada.

2. El usuario o usuaria, cuando se le solicite, debe colaborar con el personal del Servicio de Informática en cualquier investigación que se realice sobre ciberincidentes, mal uso de los recursos o cualquier investigación que se realice para esclarecer el cumplimiento de la presente normativa. Para ello el personal usuario debe aportar la información que se le solicite y, cuando la situación lo requiera, permitir el acceso al equipamiento afectado.

3. Las personas usuarias que detecten cualquier anomalía, uso no autorizado de su contraseña o cuenta, o de cualquier otro fallo de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la UA o su imagen, deberán informar inmediatamente al Servicio de Informática mediante los mecanismos indicados en el "Proceso de Gestión de incidentes de la UA" que lo registrará debidamente y elevará, en su caso.

4. El Servicio de Informática será el responsable de definir las medidas de seguridad que deben instalarse y configurarse en dichos equipos, y el personal usuario, de aplicarlas. Para cualquier cambio, la o el responsable de la unidad, servicio, departamento o centro al que esté adscrita la persona usuaria deberá solicitarlo y justificarlo al Responsable de Sistemas de la UA quien valorará la idoneidad de autorizar o no estos cambios.

5. El Servicio de Informática de la UA, con la colaboración de las restantes unidades de la UA, velarán por el cumplimiento de la presente Normativa e informarán al Comité de Seguridad TI sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

Artículo 19. Incumplimiento

1. Si el personal del Servicio de Informática detecta la existencia de un mal uso de los recursos o un ciberincidente y éste procede de las actividades de una persona usuaria determinada, puede tomar las siguientes medidas para proteger a otras personas usuarias y, en general, a la infraestructura tecnológica de la UA:

a) Notificar la incidencia al personal afectado, así como a la persona responsable de la unidad al que esté adscrito.

b) Informar al Comité de Seguridad TI y órganos de gobierno correspondientes de lo sucedido para que adopten las medidas disciplinarias que consideren.

c) Suspender o restringir el acceso o uso de los recursos, temporal o definitivamente. Cuando la suspensión del uso de los recursos y servicios informáticos, sea una medida preventiva a adoptar como consecuencia de un uso inadecuado de los mismos, el Comité de Seguridad será el órgano competente para acordar, de forma motivada, dicha suspensión. Una vez valorado el riesgo por parte de dicho Comité, se iniciaría de oficio el correspondiente procedimiento de suspensión de uso de los recursos TI y se dará traslado a la persona interesada de la presunta infracción para que realice las alegaciones que estime pertinentes en los plazos establecidos.

2. En qualsevol cas, la inobservança d'aquesta normativa, com també de les normes particulars d'altres serveis informàtics actuals o futurs, podrà donar lloc a l'inici de les accions legals, disciplinàries o de qualsevol altra índole, que pogueren correspondre, sense perjudici de la suspensió del servei prestat o el bloqueig temporal dels sistemes que com a mesures preventives pogueren adoptar.

3. La Universitat d'Alacant posarà en coneixement de l'autoritat judicial i de les Forces i Cossos de Seguretat de l'Estat aquelles infraccions que puguen ser constitutives de delicte.

Disposició addicional

S'inclou en Annex les normes i els procediments de la UA que cal tindre en compte en l'aplicació d'aquesta normativa

Disposició derogatòria

Queda derogada la normativa "CONDICIONS D'ÚS DELS RECURSOS INFORMÀTICS I DE COMUNICACIONS DE LA UNIVERSITAT D'ALACANT" aprovada pel Consell de Govern de la Universitat d'Alacant en la sessió del 8 de maig de 2007.

Disposició final primera

Sense perjudici del que disposa aquesta normativa, s'estarà també subjecte a altres normes particulars com ara:

· Normativa reguladora dels drets i obligacions de les persones usuàries dels serveis i recursos informàtics de la Universitat d'Alacant.

· Normatives reguladores específiques de serveis com el correu electrònic, xarxes sense fils, aules informàtiques de lliure accés, serveis multimèdia, plataforma Moodle, sistemes d'informació departamentals i altres noves que puguen aparèixer i que puguen tindre relació amb l'objecte d'aquesta.

Tot allò que no estiga previst en aquesta normativa, estarà subjecte al que disposa la Política de Seguretat i altres normes aprovades per la UA i a la normativa estatal o autonòmica que corresponga.

Disposició final segona

Aquesta normativa ha sigut revisada pel Comité de Seguretat TI de la Universitat d'Alacant en la sessió de 19 de setembre de 2024 i entrarà en vigor l'endemà de la seua publicació en el BOUA, una vegada aprovada pel Consell de Govern.

Annex

· "Política de seguretat de la Informació"

· "Normativa de seguretat i ús dels servidors aliens al Servei d'Informàtica de la Universitat d'Alacant"

· "Procediment d'accés local i remot"

· "Protecció del lloc de treball informàtic"

· "Lloc de treball net i equip bloquejat"

· "Procediment per a l'esborrament i la destrucció de suports d'emmagatzematge d'informació"

· "Procediment d'ofuscació de dades i eliminació de metadades"

· "Procediment de gestió d'incidents de seguretat en la UA"

· "Protocol de retenció de Log de la UA"

2. En cualquier caso, la inobservancia de esta normativa, así como las normas particulares de otros servicios informáticos actuales o futuras, podrá dar lugar al inicio de las acciones legales, disciplinarias o de cualquier otra índole, que pudieran corresponder, sin perjuicio de la suspensión del servicio prestado y/o el bloqueo temporal de los sistemas que como medidas preventivas pudieran adoptarse.

3. La Universidad de Alicante pondrá en conocimiento de la autoridad judicial y de las Fuerzas y Cuerpos de Seguridad del Estado aquellas infracciones que puedan ser constitutivas de delito.

Disposición adicional

Se incluye en Anexo las normas y los procedimientos de la UA a tener en cuenta en la aplicación de la presente normativa

Disposición derogatoria

Queda derogada la normativa "CONDICIONES DE USO DE LOS RECURSOS INFORMÁTICOS Y DE COMUNICACIONES DE LA UNIVERSIDAD DE ALICANTE" aprobada por el consejo de gobierno de la Universidad de Alicante en la sesión del 8 de mayo de 2007.

Disposición final primera

Sin perjuicio de lo que dispone esta normativa, se estará también sujeto a otras normas particulares tales como:

· Normativa reguladora de los derechos y obligaciones de las personas usuarias de los servicios y recursos informáticos de la Universidad de Alicante.

· Normativas reguladoras específicas de servicios como el correo electrónico, redes inalámbricas, aulas informáticas de libre acceso, servicios multimedia, plataforma Moodle, sistemas de información departamentales y otras nuevas que puedan aparecer y que puedan tener relación con el objeto de la presente.

Lo que no esté contemplado en la presente normativa, estará sujeto a lo dispuesto en la Política de Seguridad y demás normas aprobadas por la UA y a la normativa estatal o autonómica que corresponda.

Disposición final segunda

La presente normativa ha sido revisada por el Comité de Seguridad TI de la Universidad de Alicante en su sesión de 19 de septiembre de 2024 y entrará en vigor al día siguiente de su publicación en el BOUA, una vez aprobada por el Consejo de Gobierno.

Anexo

· "Política de seguridad de la Información"

· "Normativa de seguridad y uso de los servidores ajenos al Servicio de Informática de la Universidad de Alicante"

· "Procedimiento de acceso local y remoto"

· "Protección del puesto de trabajo informático"

· "Puesto de trabajo despejado y equipo bloqueado"

· "Procedimiento para el borrado y la destrucción de soportes de almacenamiento de información"

· "Procedimiento de ofuscación de datos y eliminación de metadatos"

· "Procedimiento de gestión de incidentes de seguridad en la UA"

· "Protocolo de retención de Logs de la UA"