

Títol: NORMATIVA DE SEGURETAT I ÚS DELS SERVIDORS ALIENS AL SERVEI D'INFORMÀTICA DE LA UNIVERSITAT D'ALACANT
Secció: DISPOSICIONS GENERALS
Òrgan: Consell de Govern
Data d'aprovació: dijous, 26 de setembre de 2024

Título: NORMATIVA DE SEGURIDAD Y USO DE LOS SERVIDORES AJENOS AL SERVICIO DE INFORMÁTICA DE LA UNIVERSIDAD DE ALICANTE
Sección: DISPOSICIONES GENERALES
Órgano: Consejo de Gobierno
Fecha de aprobación: jueves, 26 de septiembre 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.

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 SEGURETAT I ÚS DELS SERVIDORS ALIENS AL SERVEI D'INFORMÀTICA DE LA UNIVERSITAT D'ALACANT

NORMATIVA DE SEGURIDAD Y USO DE LOS SERVIDORES AJENOS AL SERVICIO DE INFORMÁTICA DE LA UNIVERSIDAD DE ALICANTE

Preàmbul

Preámbulo

TÍTOL PRELIMINAR

TÍTULO PRELIMINAR

Objecte i àmbit d'aplicació

Objeto y ámbito de aplicación

Article 1. Objecte

Artículo 1. Objeto

Article 2. Àmbit d'aplicació

Artículo 2. Ámbito de aplicación

Article 3. Revisió i avaluació

Artículo 3. Revisión y evaluación

Article 4. Definicions

Artículo 4. Definiciones

TÍTOL I

TÍTULO I

Llocs web oficials

Sitios Web Oficiales

Article 5. Sistema d'informació relatiu a llocs web oficials

Artículo 5. Sistema de información referente a sitios web oficiales

TÍTOL II

TÍTULO II

Autoritzacions

Autorizaciones

Article 6. Autorització per a la connexió d'un sistema d'informació a la infraestructura de la UA

Artículo 6. Autorización para la conexión de un sistema de información a la infraestructura de la UA

Article 7. Autorització per a la utilització d'un sistema d'informació en infraestructura externa sota dominis de la UA

Artículo 7. Autorización para la utilización de un sistema de información en infraestructura externa bajo dominios de la UA

TÍTOL III

TÍTULO III

Obligacions

Obligaciones

Article 8. Obligacions de la persona titular del sistema d'informació

Artículo 8. Obligaciones de la persona titular del sistema de información

Article 9. Obligacions del personal administrador del sistema d'informació

Artículo 9. Obligaciones del personal administrador del sistema de información

TÍTOL IV

TÍTULO IV

Responsabilitats i mesures que cal adoptar

Responsabilidades y medidas a adoptar

Article 10. Responsabilitats

Artículo 10. Responsabilidades

Article 11. Incompliment

Artículo 11. Incumplimiento

Disposició transitòria

Disposición transitoria

Disposició addicional

Disposición adicional

Disposició final primera

Disposición final primera

Disposició final segona

Disposición final segunda

Annex I

Anexo I

Annex II

Anexo II

Preàmbul

Preámbulo

La Política de seguretat de la Universitat d'Alacant (UA) que es va aprovar el 15 de desembre del 2022 estableix un marc general sobre el tractament de la seguretat de la informació en l'àmbit de la UA i disposa, en l'article 12, que s'ha de desenvolupar i complementar amb normes, procediments i instruccions més específiques.

Dins d'aquest marc normatiu, la UA va aprovar la Normativa reguladora dels drets i les obligacions de les persones usuaris de serveis i recursos informàtics i la Normativa d'ús dels recursos informàtics i de comunicacions. Els servidors informàtics poden ser font de riscos i objecte d'amenaques des d'Internet, sobretot si no estan subjectes a una sèrie d'accions i bones pràctiques. Per tant, amb la finalitat de protegir aquests recursos i, per extensió, la resta de la infraestructura tecnològica de la UA, es dicta aquesta norma per a la instal·lació, la posada en funcionament i el manteniment de servidors i serveis aliens al Servei d'Informàtica de la UA, que desenvolupa i complementa les normes i condicions esmentades anteriorment.

TÍTOL PRELIMINAR

Objecte i àmbit d'aplicació

Article 1. Objecte

L'objecte d'aquest document és establir la normativa que permet a les i els titulars i administradors dels servidors i sistemes d'informació departamentals, d'instituts o qualsevol altra unitat de la universitat, garantir els drets de les persones usuàries, protegir la infraestructura TI de la universitat i assegurar el compliment de les normatives que afecten els sistemes d'informació de l'administració pública.

Article 2. Àmbit d'aplicació

Aquesta normativa és aplicable a tot l'àmbit d'actuació de la Universitat d'Alacant. També és aplicable i d'obligat compliment per a totes i tots els titulars i administradors dels servidors i sistemes d'informació connectats a la xarxa de la Universitat d'Alacant o que s'allotgen fora de la universitat, siga físicament o virtualment, però que continguin informació, serveis o dades de la Universitat d'Alacant.

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 puguin sorgir en l'aplicació d'aquesta norma.
- Revisar-la quan calga per a actualitzar-ne el contingut o quan es complisquen els terminis màxims establits per a fer-ho.
- 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 esdevinguts en el marc legal, infraestructura tecnològica, organització general, etc.

Article 4. Definicions

- Titular del sistema d'informació: responsable final del sistema d'informació i la o el sol·licitant d'aquest.
- Personal administrador del sistema d'informació: personal tècnic i, per tant, encarregat de la gestió i supervisió dels servidors i del programari desplegat. La seua principal responsabilitat és garantir que els serveis funcionen de manera eficient, segura i de confiança.
- RSIS: responsable del sistema definit en la Política de seguretat de la informació de la UA.

La Política de Seguridad de la Universidad de Alicante (UA) que se aprobó el 15 de diciembre del 2022 supone un 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.

Dentro de este marco normativo, la UA aprobó la "Normativa reguladora de los derechos y obligaciones de las personas usuarios de servicios y recursos informáticos" y la "Normativa de uso de los recursos informáticos y de comunicaciones". Los servidores informáticos pueden ser fuente de riesgos y objeto de amenazas desde Internet, sobre todo si no están sujetos a una serie de acciones y buenas prácticas. Por tanto, con el fin de proteger estos recursos y, por extensión, al resto de la infraestructura tecnológica de la UA, se dicta la presente norma para la instalación, puesta en funcionamiento y mantenimiento de servidores y servicios ajenos al Servicio de Informática de la UA que desarrolla y complementa las normas y condiciones anteriormente citadas.

TÍTULO PRELIMINAR

Objeto y ámbito de aplicación

Artículo 1. Objeto

El objeto del presente documento es establecer la normativa que permita a las y los titulares y administradores de los servidores y sistemas de información departamentales, de institutos y/o cualquier otra unidad de la universidad, garantizar los derechos de las personas usuarias de los mismos, proteger la infraestructura TI de la universidad y asegurar el cumplimiento de las normativas que afectan a los sistemas de información de la administración pública.

Artículo 2. Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación de la Universidad de Alicante. La presente normativa es de aplicación y de obligado cumplimiento para todas las y los titulares y administradores de los servidores y sistemas de información conectados a la red de la Universidad de Alicante o que se alojen fuera de ella, bien físicamente, bien virtualmente, pero contengan información, servicios o datos de la Universidad de Alicante.

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.

Artículo 4. Definiciones

- Titular del sistema de información. Responsable final del sistema de información y la o el solicitante del mismo.
- Personal administrador del sistema de información. Personal técnico y, por tanto, encargado de la gestión y supervisión de los servidores y del software desplegado. Su principal responsabilidad es garantizar que los servicios funcionen de manera eficiente, segura y confiable.
- RSIS. Responsable del Sistema definido en la Política de Seguridad de la Información de la UA

- RSEG: responsable de seguretat de la informació definit en la Política de seguretat de la informació de la UA
- Servidor: un servidor informàtic és un sistema de maquinari i programari dissenyat per a proporcionar serveis i recursos a altres dispositius o usuaris en una xarxa.
- Sistema d'informació: un sistema d'informació és el conjunt de components de programari o maquinari interrelacionats que treballen junts per a recopilar, emmagatzemar, processar i distribuir informació. També pot estar format per un únic servidor.
- Sistema d'informació aliè al Servei d'Informàtica: tot aquell sistema d'informació no gestionat pel personal del Servei d'Informàtica de la UA.

TÍTOL I

Llocs web oficials

Article 5. Sistema d'informació relatiu a llocs web oficials

Els llocs web de centres, departaments, unitats, serveis i instituts s'hauran de realitzar amb les eines i amb les infraestructures facilitades pel Servei d'Informàtica i complir la normativa interna vigent per al desenvolupament d'aquests llocs web.

TÍTOL II

Autoritzacions

Article 6. Autorització per a la connexió d'un sistema d'informació a la infraestructura de la UA

1. El procés que ha de seguir el personal de la UA que necessite desplegar un sistema d'informació en infraestructura de la UA és:

- La persona titular del sistema d'informació justificarà la impossibilitat d'utilitzar els recursos TI centralitzats disponibles a la UA i gestionats pel Servei d'Informàtica.
- La persona titular del sistema d'informació farà una sol·licitud electrònica en la qual es recollirà la informació següent:
 - Justificació del no ús de sistemes centrals
 - Dades necessàries per a la connexió a la xarxa
 - Nom de domini sol·licitat, si cal.
 - Identificació de l'administrador del sistema.
 - Maquinari que suporta el sistema.
 - Programari a desplegar i versions (S.O., servidors d'aplicacions, etc.).

2. L'autorització o no d'aquesta petició correspon al vicerectorat amb competències en tecnologies de la informació de la Universitat d'Alacant.

Article 7. Autorització per a la utilització d'un sistema d'informació en infraestructura externa sota dominis de la UA

1. El procés que ha de seguir el personal de la UA que necessite desplegar un sistema d'informació en infraestructura externa a la UA és:

- La persona titular del sistema d'informació justificarà la impossibilitat d'utilitzar els recursos TI centralitzats disponibles a la UA i gestionats pel Servei d'Informàtica.
- La persona titular del sistema d'informació farà una sol·licitud electrònica en la qual es recollirà la informació següent:
 - Justificació del no ús de sistemes centrals.
 - Nom de domini sol·licitat, si és necessari.
 - Identificació de l'administrador de sistemes.

- RSEG. Responsable de Seguridad de la Información definido en la Política de Seguridad de la Información de la UA
- Servidor. Un servidor informático es un sistema de hardware y software diseñado para proporcionar servicios y recursos a otros dispositivos o usuarios en una red.
- Sistema de información. Un sistema de información es conjunto de componentes software y/o hardware interrelacionados que trabajan juntos para recopilar, almacenar, procesar y distribuir información. También puede estar formado por un único servidor.
- Sistema de información ajeno al Servicio de Informática. Todo aquel sistema de información no gestionado por el personal del Servicio de Informática de la UA.

TÍTULO I

Sitios Web Oficiales

Artículo 5. Sistema de información referente a sitios web oficiales

Los sitios web de centros, departamentos, unidades, servicios e institutos deberán realizarse con las herramientas y con las infraestructuras facilitadas por el Servicio de Informática y cumpliendo la normativa interna vigente para el desarrollo de estos sitios web.

TÍTULO II

Autorizaciones

Artículo 6. Autorización para la conexión de un sistema de información a la infraestructura de la UA

1. El proceso a seguir por el personal de la UA que necesite desplegar un sistema de información en infraestructura de la UA es:

- La persona titular del sistema de información justificará la imposibilidad de utilizar los recursos TI centralizados disponibles en la UA y gestionados por el Servicio de Informática.
- La persona titular del sistema de información realizará una solicitud electrónica en la que se recogerá la siguiente información:
 - Justificación de no uso de sistemas centrales
 - Datos necesarios para la conexión a la red
 - Nombre de dominio solicitado, si fuera necesario.
 - Identificación del administrador del sistema.
 - Hardware que soporta el sistema.
 - Software a desplegar y versiones (S.O, servidores de aplicaciones, etc.)

2. La autorización o no de esta petición recae en el Vicerrectorado con competencias en Tecnologías de la Información de la Universidad de Alicante.

Artículo 7. Autorización para la utilización de un sistema de información en infraestructura externa bajo dominios de la UA.

1. El proceso a seguir por el personal de la UA que necesite desplegar un sistema de información en infraestructura externa a la UA es:

- La persona titular del sistema de información justificará la imposibilidad de utilizar los recursos TI centralizados disponibles en la UA y gestionados por el Servicio de Informática.
- La persona titular del sistema de información realizará una solicitud electrónica en la que se recogerá la siguiente información:
 - Justificación de no uso de sistemas centrales
 - Nombre de dominio solicitado, si fuera necesario.
 - Identificación del administrador de sistemas

- Programari a desplegar i versions (S.O., servidors d'aplicacions, etc.).

- Identificació de l'empresa en què es desplega el sistema d'informació.

2. L'autorització o no d'aquesta petició correspon al vicerectorat amb competències en tecnologies de la informació de la Universitat d'Alacant.

TÍTOL III

Obligacions

Article 8. Obligacions de la persona titular del sistema d'informació

1. Les obligacions que ha de complir la persona titular del sistema la sol·licitud de la qual haja sigut autoritzada són:

a) Disposar sempre d'una persona administradora del sistema i, addicionalment, si cal, d'una persona responsable del programari desplegat.

b) Facilitar a la persona administradora del sistema el compliment de les seues obligacions detallades en l'article 9 d'aquesta normativa.

c) Garantir el compliment del que disposa la legislació europea i espanyola en matèria de protecció de dades de caràcter personal. De manera molt especial:

- La necessitat de complir amb el deure d'informació que recull la legislació de protecció de dades.

- Si el servidor es troba fora de la infraestructura de la UA i conté dades personals segons el «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» es requereix un contracte d'encarregat de tractament amb el proveïdor de serveis d'allotjament, el qual haurà de ser signat pel gerent.

d) En cap cas es poden recollir ni tractar dades especialment protegides (regulades en l'art. 9 del 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).

e) La persona titular ha d'actuar amb diligència davant dels requeriments que puga rebre relatius a temes de seguretat o protecció de dades personals.

f) La persona titular haurà de mantenir informat el RSIS de la UA dels canvis de personal administrador del sistema o del personal responsable del programari.

g) Anualment, o quan el Servei d'Informàtica ho sol·licite, la persona titular ha de remetre al RSIS de la UA un informe amb el programari instal·lat en el sistema, les seues versions i quins dels serveis habilitats són accessibles des d'Internet.

h) La persona titular és la responsable de determinar quan deixa de ser necessari el sistema d'informació i fer les gestions necessàries per al seu desmantellament. A més, ha d'informar-ne el RSIS de la UA mitjançant el mecanisme que s'indique per a aquesta finalitat.

- Software a desplegar y versiones (S.O, servidores de aplicaciones, etc.)

- Identificación de la empresa donde se despliega el sistema de información.

2. La autorización o no de esta petición recae en el Vicerrectorado con competencias en Tecnologías de la Información de la Universidad de Alicante.

TÍTULO III

Obligaciones

Artículo 8. Obligaciones de la persona titular del sistema de información

1. Las obligaciones que debe cumplir la persona titular del sistema cuya solicitud haya sido autorizada son:

a) Disponer siempre de una persona administradora del sistema y, adicionalmente si fuera necesario, de una persona responsable del software desplegado.

b) Facilitar a la persona administradora del sistema el cumplimiento de sus obligaciones detalladas en el artículo 9 de la presente normativa.

c) Garantizar el cumplimiento de lo dispuesto en la legislación europea y española en materia de protección de datos de carácter personal. De forma muy especial:

- La necesidad de cumplir con el deber de información que recoge la legislación de protección de datos.

- Si el servidor se encuentra fuera de la infraestructura de la UA y contiene datos personales según el "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" se requiere un contrato de encargado de tratamiento con el proveedor de servicios de alojamiento, el cual deberá ser firmado por el Gerente.

d) En ningún caso, se pueden recabar y/o tratar datos especialmente protegidos (contemplados en el art. 9 del 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).

e) La persona titular debe actuar con diligencia ante los requerimientos que pueda recibir relativos a temas de seguridad o protección de datos personales.

f) La persona titular deberá mantener informada al RSIS de la UA de los cambios de personal administrador del sistema y/o del personal responsable del software.

g) Anualmente o cuando el Servicio de Informática lo solicite, la persona titular debe remitir al RSIS de la UA un informe con el software instalado en el sistema, las versiones del mismo y cuáles de los servicios habilitados son accesibles desde Internet.

h) La persona titular es la responsable de determinar cuándo deja de ser necesario el sistema de información y realizar las gestiones necesarias para su desmantelamiento. Además, debe informar al RSIS de la UA mediante el mecanismo que se indique para tal fin.

2. A més de les obligacions anteriors, la persona titular del sistema haurà de complir amb la normativa aplicable tant de la Universitat d'Alacant com l'autonòmica, nacional i europea, amb especial atenció a l'Esquema Nacional de Seguretat (Reial decret 311/2022, de 3 de maig), Llei de propietat intel·lectual (Reial decret legislatiu 1/1996, de 12 d'abril), accessibilitat (Reial decret 1112/2018 sobre accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic), a les normatives de la UA i la Comunitat Valenciana relatives al bilingüisme i qualsevol altra que puga ser aplicable.

3. Si el servei entra dins de l'àmbit del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS):

· La contractació ha de seguir les directrius establides en el Procediment per a la contractació de subministraments i serveis de tecnologies de la informació de la UA.

· El o els servidors en els quals s'allotge han de complir els principis i les mesures de seguretat establides en aquest RD per al nivell MITJÀ.

· El Centre de Processament de Dades (CPD) on s'allotge aquest servidor ha de disposar, com a mínim, de la certificació de conformitat en la categoria MITJANA (categoria establida per a la Universitat d'Alacant).

Article 9. Obligacions del personal administrador del sistema d'informació

1. El personal administrador és el responsable de mantenir la infraestructura tecnològica del sistema en condicions operatives. En el cas que siga una persona sense vinculació amb la UA o un servei prestat per una empresa externa, el contracte ha de recollir les obligacions indicades en aquesta normativa.

2. El personal administrador ha de mantenir el sistema actualitzat de manera que siga possible el compliment de les normes establides en el punt anterior.

3. El personal administrador del sistema ha de dissenyar i configurar el sistema de manera que garantisca un grau suficient de seguretat per defecte, establiment de les mesures de protecció, detecció i recuperació proporcionals als riscos potencials i a la criticitat i valor de la informació del sistema. Per a fer-ho, i llevat de motius degudament justificats:

· S'hi instal·laran les eines de seguretat que marque la Divisió de Seguretat de la Informació de la Universitat d'Alacant.

· S'hi aplicaran els procediments, les instruccions i els requisits publicats per la Divisió de Seguretat de la Informació de la Universitat d'Alacant.

4. El personal administrador ha de seguir el Procediment de gestió d'incidents de la UA (<https://si.ua.es/va/normativa/normativa/procedimiento-de-gestion-de-incidentes-de-seguridad-ua.pdf>) i, a més, dur a terme les accions que des de la Divisió de Seguretat de la Informació de la Universitat d'Alacant se li indiquen, amb l'obligació de participar en la gestió i resolució de qualsevol incidència que sorgisca en aquest àmbit. En la línia d'aquest procediment, en el cas que el personal administrador detecte un incident de seguretat haurà de comunicar-lo immediatament seguint el procediment de gestió esmentat en aquest paràgraf.

TÍTOL IV

Responsabilitats i mesures que cal adoptar

Article 10. Responsabilitats

1. Tota persona membre de la UA afectada per aquesta normativa és responsable de conèixer les directrius d'aquest document, així com de les conseqüències en què pugen incórrer en cas d'incompliment.

2. Además de las obligaciones anteriores, la persona titular del sistema deberá cumplir con la normativa aplicable tanto de la Universidad de Alicante, como la autonómica, nacional y europea, con especial atención al Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo), Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996, de 12 de abril), accesibilidad (Real Decreto 1112/2018 sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público), a las normativas de la UA y la Comunidad Valenciana referentes al bilingüismo, y cualquier otra que pueda ser de aplicación.

3. Si el servicio entra dentro del ámbito del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS):

· la contratación debe seguir las directrices establecidas en el "Procedimiento para la contratación de suministros y servicios de Tecnologías de la Información de la UA"

· el o los servidores en los que se aloje deben cumplir los principios y las medidas de seguridad establecidas en dicho RD para el nivel MEDIO

· y el Centro de Proceso de Datos (CPD) donde se aloje dicho servidor debe disponer, como mínimo, de la certificación de conformidad en la categoría MEDIA (categoría establecida para la Universidad de Alicante).

Artículo 9. Obligaciones del personal administrador del sistema de información

1. El personal administrador es el responsable de mantener la infraestructura tecnológica del sistema en condiciones operativas. En el caso de que sea una persona sin vinculación con la UA o un servicio prestado por una empresa externa, el contrato debe recoger las obligaciones indicadas en esta normativa.

2. El personal administrador debe mantener el sistema actualizado de forma que sea posible el cumplimiento de las normas establecidas en el punto anterior.

3. El personal administrador del sistema debe diseñar y configurar el sistema de forma que garantice un grado suficiente de seguridad por defecto, establecimiento las medidas de protección, detección y recuperación proporcionales a los potenciales riesgos y a la criticidad y valor de la información del sistema. Para ello, salvo motivos debidamente justificados:

· Se instalarán las herramientas de seguridad que marque la División de Seguridad de la Información de la Universidad de Alicante.

· Se aplicarán los procedimientos, instrucciones y requisitos publicados por la División de Seguridad de la Información de la Universidad de Alicante.

4. El personal administrador debe seguir el procedimiento de Gestión de Incidentes de la UA (<https://si.ua.es/es/normativa/normativa/procedimiento-de-gestion-de-incidentes-de-seguridad-ua.pdf>) y, además, realizar las acciones que desde la División de Seguridad de la Información de la Universidad de Alicante se le indiquen, estando obligado a participar en la gestión y resolución de cualquier incidencia que surja en este ámbito. En la línea de este procedimiento, en el caso de que el personal administrador detecte un incidente de seguridad deberá comunicarlo inmediatamente, siguiendo el procedimiento de gestión mencionado en este párrafo.

TÍTULO IV

Responsabilidades y medidas a adoptar

Artículo 10. Responsabilidades

1. Toda persona miembro de la UA afectada por esta normativa es responsable de conocer las directrices del presente documento, así como de las consecuencias que pudieran incurrir en caso de incumplimiento.

2. La persona titular del sistema té la responsabilitat que es complisca, durant tot el temps que el sistema d'informació estiga en funcionament:

- aquesta norma i les obligacions que s'hi indiquen;
- la normativa aplicable tant de la Universitat d'Alacant, com l'autonòmica, nacional i europea.

3. El personal administrador del sistema és l'encarregat de complir les directrius que s'indiquen en aquest document durant tot el temps que el sistema d'informació estiga en funcionament, així com totes les altres mesures que considere oportunes per a la seua correcta protecció. És responsable directe dels incidents ocasionats per l'incompliment d'aquestes normes i els problemes derivats que puguin afectar terceres persones, el mateix sistema o d'altres connectats a la infraestructura de la UA.

4. En l'annex I es detallen les responsabilitats del personal.

Article 11. Incumpliment

El Servei d'Informàtica, atenent els protocols de seguretat establits en la universitat o per incompliment de les condicions expressades en els articles 8 i 9 d'aquesta normativa, podrà bloquejar i aïllar l'accés a aquests sistemes d'informació. Es notificarà al titular i a l'administrador del sistema i es prendran les mesures i comprovacions oportunes abans de tornar a connectar el sistema d'informació a fi de prevenir que es repetisca l'incident.

Disposició transitòria

Els sistemes d'informació que estiguen en funcionament quan entre en vigor aquesta norma i que en resulten afectats disposaran de quaranta dies hàbils, comptadors des de l'endemà de la publicació d'aquesta normativa en el BOUA, perquè el titular del sistema sol·licite l'autorització corresponent tal com indiquen els articles 6 i 7 d'aquesta normativa.

Disposició adicional

S'inclouen en annex II les normes i els procediments presents de la UA que cal tenir en compte en l'aplicació d'aquesta normativa

Disposició final primera

En tot allò que no estiga regulat en aquesta normativa caldrà atènyer-se al que disposa la Política de seguretat i altres normes aprovades per la UA i la normativa estatal o autonòmica que corresponga.

Disposició final segona

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

Annex I

En aquesta taula s'indiquen les responsabilitats del personal

Taula 1. Matriu RACI: Responsable, Aprova, Consultat o Informat

2. La persona titular del sistema tiene la responsabilidad de que se cumpla, durante todo el tiempo que el sistema de información esté en funcionamiento:

- con la presente norma y las obligaciones indicadas en ella.
- con la normativa aplicable tanto de la Universidad de Alicante, como la autonómica, nacional y europea

3. El personal administrador del sistema es el encargado de cumplir con las directrices que se indican en este documento durante todo el tiempo que el sistema de información esté en funcionamiento así como de todas las demás medidas que considere oportunas para su correcta protección, siendo responsable directo de los incidentes ocasionados por el incumplimiento de estas normas y los problemas derivados que puedan afectar a terceras personas, al propio sistema u otros conectados a la infraestructura de la UA.

4. En el Anexo I se detallan las responsabilidades del personal.

Artículo 11. Incumplimiento

El Servicio de Informática, atendiendo a los protocolos de seguridad establecidos en la universidad y/o por incumplimiento de las condiciones expresadas en los artículos 8 y 9 de esta normativa, podrá bloquear y/o aislar el acceso a estos sistemas de información. Se notificará al titular y al administrador del sistema y se tomarán las medidas y comprobaciones oportunas antes de volver a conectar el sistema de información con el objeto de prevenir que se repita el incidente.

Disposición transitoria

Los sistemas de información que se encuentren en funcionamiento cuando entre en vigor esta norma y que estén afectados por ella dispondrán de 40 días hábiles, a contabilizar desde el día siguiente de la publicación de esta normativa en el BOUA, para que el titular del sistema solicite la autorización correspondiente tal y como se indica en los artículos 6 y 7 de la presente normativa.

Disposición adicional

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

Disposición final primera

Lo que no esté contemplado en la presente normativa, se está a lo dispuesto en la Política de Seguridad y demás normas aprobadas por la UA y 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 I

En la siguiente tabla se indican las responsabilidades del personal

Tabla 1.- Matriz RACI: Responsable, Aprueba, Consultado o Informado

Activitat	RSIS	RSEG	Comissió TI	Titular sistema	Administrador sistema
Sol·licitud	C	I	A	R	I
Nomenament personal administrador sistemes	I	I		R	C
Compliment normatiu	I	I	I	R	C
Informes situació sistema	I	I		R	C
Manteniment del sistema				I	R
Protecció del sistema	I	C		C	R
Gestió d'incidents		I/C		I	R
Sancions per incompliment	R	C	A	I	I

Annex II

- Política de seguretat de la informació
- Normativa reguladora dels drets i obligacions de les persones usuàries de serveis i recursos informàtics de la Universitat d'Alacant
- Normativa de seguretat i ús dels recursos i serveis informàtics de la Universitat d'Alacant.
- Procediment de gestió d'incidents de seguretat en la UA

Actividad	RSIS	RSEG	Comisión TI	Titular sistema	Administrador Sistema
Solicitud	C	I	A	R	I
Nombramiento personal Administrador Sistemas	I	I		R	C
Cumplimiento normativo	I	I	I	R	C
Informes Situación Sistema	I	I		R	C
Mantenimiento del Sistema				I	R
Protección del Sistema	I	C		C	R
Gestión de incidentes		I/C		I	R
Sanciones por incumplimiento	R	C	A	I	I

Anexo II

- "Política de seguridad de la Información"
- "Normativa reguladora de los derechos y obligaciones de las personas usuarias de servicios y recursos informáticos de la Universidad de Alicante"
- "Normativa de seguridad y uso de los recursos y servicios informáticos de la Universidad de Alicante"
- "Procedimiento de gestión de incidentes de seguridad en la UA"