

Títol: NORMATIVA DE QUALIFICACIÓ I TRACTAMENT DE LA INFORMACIÓ
Secció: DISPOSICIONS GENERALS
Òrgan: Consell de Govern
Data d'aprovació: dijous, 23 de febrer de 2023

NORMATIVA DE QUALIFICACIÓ I TRACTAMENT DE LA INFORMACIÓ

Preàmbul

La informació és un dels actius principals de qualsevol organització i, com a tal, hem de protegir-la adequadament. La Universitat d'Alacant maneja informació d'índole diversa. Gran part és d'ús intern i pot tenir diferents graus de confidencialitat. Per al maneig segur d'aquesta, un requisit indispensable és classificar la informació segons la seua naturalesa i el seu nivell de confidencialitat, i això afecta el tractament dels documents i sistemes d'informació (SI) i als mitjans d'emmagatzematge i transferència de la informació.

Article 1. Objecte

D'acord amb el que disposa el Reial decret 311/2022, de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (d'ara endavant, ENS), aquest document té el propòsit de normalitzar el maneig de la informació per part de la comunitat universitària quan hi accedeix o la tracta.

Aquesta normativa haurà de ser complementada, si escau i en la mesura oportuna, amb l'aplicació de les mesures de seguretat previstes en l'Annex II de l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica quan la informació continga dades personals protegides per la Llei de Protecció de Dades de Caràcter Personal (d'ara endavant, LOPD).

Article 2. Àmbit d'aplicació

Aquesta normativa és aplicable a tot l'àmbit d'actuació de la Universitat d'Alacant, i els seus continguts porten causa de les directrius de caràcter més general definides en la Política de Seguretat de la Informació i en les Normes de Seguretat d'aquesta.

Aquesta normativa és aplicable i de compliment obligat per a tot el personal de la Universitat d'Alacant. En l'àmbit de aquesta normativa, s'entén per usuari o usuària qualsevol empleat públic pertanyent o aliè a la Universitat d'Alacant, com també personal d'organitzacions privades externes, entitats col·laboradores o qualsevol altre amb alguna mena de vinculació amb la Universitat i que utilitze o tinga accés als Sistemes d'Informació d'aquesta.

Aquesta normativa aplica a la qualificació i el tractament de la informació que manegen els sistemes d'informació de la UA afectats per l'ENS. Tota informació en suport no electrònic, que haja sigut causa o conseqüència directa de la informació electrònica a què es refereix l'ENS haurà d'estar protegida amb el mateix grau de seguretat que aquesta. Per a això s'aplicaran les mesures que corresponen a la naturalesa del suport en què es troben, d'acord amb les normes d'aplicació a la seguretat d'aquests.

Adicionalment, si la informació en qüestió conté dades de caràcter personal, s'actuarà d'acord amb el que disposa la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, que la UA articula a través del Document de Seguretat.

Article 3. Revisió i avaluació

La gestió d'aquesta normativa correspon al director del Servei d'Informàtica de la Universitat, que és competent per a:

Título: NORMATIVA DE CALIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN
Sección: DISPOSICIONES GENERALES
Órgano: Consejo de Gobierno
Fecha de aprobación: jueves, 23 de febrero de 2023

NORMATIVA DE CALIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN

Preámbulo

La información es uno de los principales activos de cualquier organización y, como tal, tenemos que protegerla adecuadamente. La Universidad de Alicante maneja información de diversa índole. Gran parte es de uso interno y puede tener distintos grados de confidencialidad. Para el manejo seguro de ésta, un requisito indispensable es clasificar la información según su naturaleza y su nivel de confidencialidad, afectando al tratamiento de los documentos y sistemas de información (SI) y a los medios de almacenamiento y transferencia de la información.

Artículo 1. Objeto

Conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), este documento tiene el propósito de normalizar el manejo de la información por parte de la comunidad universitaria cuando accede a ella o la trata.

La presente normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica cuando la información contenga datos personales protegidos por la Ley de Protección de Datos de Carácter Personal (en adelante, LOPD).

Artículo 2. Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación de la Universidad de Alicante, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad de la misma.

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal de la Universidad de Alicante. En el ámbito de la presente normativa, se entiende por usuario o usuaria cualquier empleado público perteneciente o ajeno a la Universidad de Alicante, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Universidad y que utilice o posea acceso a los Sistemas de Información de la misma.

Esta normativa aplica a la calificación y tratamiento de la información que manejan los sistemas de información de la UA afectados por el ENS. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que la UA articula a través del Documento de Seguridad.

Artículo 3. Revisión y evaluación

La gestión de esta normativa corresponde al director del Servicio de Informática de la Universidad, que es competente para:

- Interpretar els dubtes que puguem sorgir en l'aplicació d'aquesta.
- 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.

Anualment (o amb menor periodicitat, si hi ha circumstàncies que així ho aconsellen), el Comitè de Seguretat TI revisarà aquesta normativa.

La revisió s'orientarà tant a la identificació d'oportunitats de millora, com a l'adaptació als canvis haguts en el marc legal, infraestructura tecnològica, organització general, etc.

Serà la persona responsable de Seguretat de la Informació l'encarregada de la custòdia i divulgació de la versió aprovada d'aquest document.

Article 4. Qualificació i tractament de la informació

Article 4.1 Criteris de qualificació de la informació

La qualificació de la informació que maneja la Universitat d'Alacant fa fan les persones responsables de cada informació.

La valoració de la informació ha de tenir en compte les diferents dimensions de la seguretat: disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat.

La qualificació de la informació determina com la informació s'assegura, es maneja, es reté i es disposa.

La qualificació de la informació en la Universitat d'Alacant, d'acord amb la mesura mp.info.2 de l'ENS, es correspon amb:

- Ús no oficial: informació pública
- Ús oficial, amb 2 nivells: intern i restringit.

La qualificació i, si escau, el nivell, es determinarà d'acord amb els criteris següents, sense perjudici del que assenyalat l'article 40 i els criteris generals assenyalats en l'annex I de l'ENS:

- Valor de la informació: segons l'impacte d'aquesta en l'organització
- Accessibilitat: qui ha d'accedir a la informació
- Obligacions: legals i/o contractuals.

D'acord amb el valor de la informació, la informació es classificarà:

- Ús no oficial (per tant, pública): quan no pot danyar l'organització de cap manera.
- Ús oficial intern: quan l'accés no autoritzat a la informació podria ser perjudicial per a la reputació de la Universitat d'Alacant o ocasionar danys materials a les persones o a la Universitat.

· Ús oficial restringit: informació sensible de la Universitat d'Alacant la pèrdua de la qual podria tenir com a conseqüència un menyscapte greu en la reputació, conseqüències legals o en les finances de l'organització. S'inclouen dins d'aquest grup els fitxers de caràcter personal amb categories especials de dades.

D'acord amb el nivell d'accessibilitat:

- Ús no oficial: informació que l'organització posa a la disposició del públic dins de la pàgina web, o que l'organització haja fet pública a través de xarxes socials o mitjans de comunicació.
- Ús oficial intern: informació que només ha de ser accessible per membres de la Universitat d'Alacant.
- Ús oficial restringit: informació és accessible per la direcció o personal concret.

- Interpretar las dudas que puedan surgir en su aplicación.

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

- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad TI revisará la presente normativa.

La revisión se orientará tanto a la identificación de oportunidades de mejora, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad de la Información la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

Artículo 4. Calificación y tratamiento de la información

Artículo 4.1 Criterios de calificación de la información

La calificación de la información que maneja la Universidad de Alicante la realizan las personas responsables de cada información.

La valoración de la información debe tener en cuenta las diferentes dimensiones de la seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La calificación de la información determina cómo la información se asegura, maneja, retiene y dispone.

La calificación de la información en la Universidad de Alicante, de acuerdo con la medida mp.info.2 del ENS, se corresponde con:

- Uso no Oficial: información pública
- Uso oficial, con 2 niveles: Interno y restringido.

La calificación y, en su caso, el nivel, se determinará en función de los siguientes criterios, sin perjuicio de lo señalado en el artículo 40 y los criterios generales señalados en el anexo I del ENS:

- Valor de la información: según el impacto de esta en la organización
- Accesibilidad: quién debe acceder a la información
- Obligaciones: legales y/o contractuales.

En función del valor de la información, la información se clasificará:

- Uso No Oficial (por tanto, pública): cuando no puede dañar a la organización de ninguna forma.
- Uso Oficial Interno: cuando el acceso no autorizado a la información podría ser perjudicial para la reputación de la Universidad de Alicante u ocasionar daños materiales a las personas o a la Universidad.

· Uso Oficial Restringido: información sensible de la Universidad de Alicante cuya pérdida pudiera tener como consecuencia un menoscabo grave en la reputación, consecuencias legales o en las finanzas de la organización. Se incluyen dentro de este grupo los ficheros de carácter personal con categorías especiales de datos.

En función de su nivel de accesibilidad:

- Uso No Oficial: información que la organización pone a disposición del público dentro de su página Web, o que la organización haya hecho pública a través de redes sociales o medios de comunicación.
- Uso Oficial Interno: información que sólo debe ser accesible por miembros de la Universidad de Alicante.
- Uso Oficial Restringido: información es accesible por la dirección o personal concreto.

La regla general serà qualificar en el nivell de confidencialitat més baix i garantir un adequat nivell de protecció.

Els documents que siguen qualificats com a Oficial (tant intern com restringit) s'etiquetaran depenent del tipus de suport utilitzat i es farà d'acord amb el "Procediment de qualificació i tractament de la informació de la UA".

Article 5.2 Tractament de la informació qualificada

Per a la correcta protecció de la informació qualificada seran aplicable totes les normatives, procediments, guies, recomanacions i codis de bones pràctiques vigents per als sistemes d'informació de la Universitat d'Alacant.

Article 5.2.1 Informació d'ús no oficial

Qualsevol informació que es publiqui a través dels mitjans que la Universitat d'Alacant tinga establits per a això, ha d'haver passat per una qualificació prèvia que assegure que no s'exposa informació interna o restringida al públic en general.

A causa de la gran diversitat d'informació que la Universitat d'Alacant maneja i a la dificultat de qualificar-la íntegrament, inicialment tota la informació sense valoració es considerarà informació d'ús no oficial, tret que hi haja regulació expressa en un altre sentit.

El responsable de la publicació de la informació s'assegurarà que la informació pot fer-se pública i no ha d'estar qualificada com a ús oficial intern o restringit.

Que una informació siga d'ús no oficial en un moment determinat no assegura que ho haja de ser en tot moment. El responsable de la publicació ha de revisar, sobretot la que conté dades personals, si aquesta informació pública ha deixat de ser necessària i ha de ser retirada.

Article 4.2.2 Informació d'ús oficial intern

Les persones responsables de cada aplicació en què se situe o tracte informació d'aquest nivell de classificació han de gestionar les autoritzacions d'accés a aquestes aplicacions, i revisar-les periòdicament. Les persones usuàries dels Sistemes d'Informació i els processos automàtics només obtindran l'accés, els privilegis o els permisos que necessiten per a fer la seua comesa, amb la finalitat de limitar els danys resultants d'accidents, errors o ús no autoritzat de recursos dels Sistemes d'Informació.

Intercanvi d'informació. S'ha de ser especialment acurat en l'enviament d'aquesta informació per correu electrònic, mitjançant dispositius extraïbles o la utilització d'emmagatzematge en el núvol. Sempre que siga possible, s'utilitzaran sistemes corporatius.

Qualsevol incidència relacionada amb la informació classificada com a ús oficial intern serà posada en coneixement de la persona responsable d'aquesta informació que farà els tràmits oportuns per a gestionar la incidència com més prompte millor per a poder complir amb els terminis legals.

Per al tractament d'aquesta informació s'aplicaran les mesures de seguretat següents:

- Respectar de manera escrupolosa les directrius de protecció del lloc de treball informàtic de la Universitat d'Alacant, lloc de treball buidat i equip bloquejat i procediment per a la neteja de metadades i procediment per a l'esborrat i la destrucció de suports d'emmagatzematge d'informació.
- Les persones responsables de cada entorn en què se situe o tracte informació d'aquest nivell de confidencialitat han de gestionar les autoritzacions d'accés a aquests entorns, revisar-les periòdicament, i monitorar els accessos, d'acord amb el procediment d'accés local i remot de la Universitat d'Alacant.

La regla general será calificar en el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección.

Los documentos que se califique como Oficial (tanto interno como restringido) se etiquetarán dependiendo del tipo de soporte utilizado y se realizará conforme al "Procedimiento de calificación y tratamiento de la información de la UA".

Artículo 4.2 Tratamiento de la información calificada

Para la correcta protección de la información calificada serán de aplicación todas las normativas, procedimientos, guías, recomendaciones y códigos de buenas prácticas vigentes para los sistemas de información de la Universidad de Alicante.

Artículo 4.2.1 Información de Uso No Oficial

Cualquier información que se publiqui a través de los medios que la Universidad de Alicante tenga establecidos para ello, debe haber pasado por una calificación previa que asegure que no se expone información interna o restringida al público en general.

Debido a la gran diversidad de información que la Universidad de Alicante maneja y a la dificultad de calificarla en su totalidad, inicialmente toda la información sin valoración se considerará información de Uso No Oficial, salvo que exista regulación expresa en otro sentido.

El responsable de la publicación de la información se asegurará que la información puede hacerse pública y no debe estar calificada como Uso Oficial Interno o Restringido.

Que una información sea de uso no oficial en un momento determinado no asegura que lo deba ser en todo momento. El responsable de la publicación ha de revisar, sobre todo la que contiene datos personales, si esta información pública ha dejado de ser necesaria y debe ser retirada.

Artículo 4.2.2 Información de Uso Oficial Interno

Los y las responsables de cada aplicación en los que se ubique o trate información de este nivel de clasificación deben gestionar las autorizaciones de acceso a dichas aplicaciones, revisándolas periódicamente. Los usuarios de los Sistemas de Información y los procesos automáticos solo obtendrán el acceso, los privilegios o los permisos que necesiten para realizar su cometido, con el fin de limitar los daños resultantes de accidentes, errores o uso no autorizado de recursos de los Sistemas de Información.

Intercambio de información. Se debe ser especialmente cuidadoso en el envío de esta información por correo electrónico, mediante dispositivos extraïbles o la utilización de almacenamiento en la nube. Siempre que sea posible, se utilizarán sistemas corporativos.

Cualquier incidencia relacionada con la información clasificada como Uso Oficial Interno será puesto en conocimiento del responsable de esa información que realizará los trámites oportunos para gestionar la incidencia a la mayor brevedad posible para poder cumplir con los plazos legales.

Para el tratamiento de esta información se aplicarán las siguientes medidas de seguridad:

- Respetar de forma escrupolosa las directrices de Protección del puesto de trabajo informático de la Universidad de Alicante, Puesto de trabajo despejado y equipo bloqueado y procedimiento para la limpieza de metadatos y procedimiento para el borrado y destrucción de soportes de almacenamiento de información.
- Los responsables de cada entorno en los que se ubique o trate información de este nivel de confidencialidad deben gestionar las autorizaciones de acceso a dichos entornos, revisándolas periódicamente, y monitorizando los accesos, conforme a procedimiento de acceso local y remoto de la Universidad de Alicante.

· La informació d'aquest nivell de confidencialitat que haja d'utilitzar-se fora de les dependències de la Universitat ha de ser mínima i complir amb les mesures de seguretat establides en procediment d'accés local i remot de la Universitat d'Alacant.

Qualsevol incidència associada amb la disponibilitat o la confidencialitat de la informació haurà de ser immediatament reportada al responsable de seguretat seguint el procés de gestió d'incidents de seguretat de la informació habilitat per a aquesta finalitat.

Article 4.2.3 Informació d'ús oficial restringit

El personal responsable de cada aplicació en què se situe o tracte informació d'aquest nivell de classificació ha de gestionar les autoritzacions d'accés a aquestes aplicacions, revisar-les periòdicament, i monitorar-hi els accessos.

Les persones usuàries dels Sistemes d'Informació i els processos automàtics només obtindran l'accés, els privilegis o els permisos que necessiten per a fer la seua comesa, amb la finalitat de limitar els danys resultants d'accidents, errors o ús no autoritzat de recursos dels Sistemes d'Informació.

Tota la informació restringida que continga dades personals amb categories especials de dades s'haurà de xifrar tant en l'emmagatzematge d'aquesta com en la transmissió, mitjançant un dels algorismes autoritzats per a aquesta finalitat i amb la fortaleza requerida en la Guia CCN-STIC 807 Criptologia d'ocupació en l'Esquema Nacional de Seguretat.

No podrà publicar-se en Internet sense restriccions d'accés la informació catalogada com a informació d'ús oficial restringit.

Intercanvi d'informació. S'ha de ser especialment acurat en l'enviament d'aquesta informació per correu electrònic, mitjançant dispositius extraïbles o la utilització d'emmagatzematge en el núvol. Sempre que siga possible, s'utilitzaran sistemes corporatius i la informació es transmetrà i emmagatzemarà xifrada mitjançant un dels algorismes autoritzats per a aquesta finalitat i amb la fortaleza requerida en la Guia CCN-STIC 807 Criptologia d'ocupació en l'Esquema Nacional de Seguretat.

Qualsevol incidència associada amb la disponibilitat o la confidencialitat de la informació haurà de ser immediatament comunicada al responsable de seguretat d'acord amb el procés de gestió d'incidents de seguretat de la informació habilitat per a aquesta finalitat com més prompte millor per a poder complir amb els terminis legals.

Per al tractament d'aquesta informació s'aplicaran les mesures de seguretat següents:

· Respectar de manera escrupolosa les directrius de protecció del lloc de treball informàtic de la Universitat d'Alacant, lloc de treball buidat i equip bloquejat i procediment per a la neteja de metadades i procediment per a l'esborrat i la destrucció de suports d'emmagatzematge d'informació.

· Les persones responsables de cada entorn en què se situe o tracte informació d'aquest nivell de confidencialitat han de gestionar les autoritzacions d'accés a aquests entorns, revisar-les periòdicament, i monitorar els accessos, d'acord amb el procediment d'accés local i remot de la Universitat d'Alacant.

· La informació d'aquest nivell de confidencialitat que haja d'utilitzar-se fora de les dependències de la Universitat ha de ser mínima i complir amb les mesures de seguretat establides en Procediment d'accés local i remot de la UA.

· Quan la informació ja no siga necessària s'esborrarà i destruirà de manera segura tenint en compte que s'han complit els requeriments de retenció de dades en cada Sistema d'Informació de cara a la realització d'accions administratives, disciplinàries, civils o penals. Per a això s'ha de seguir el procediment per a l'esborrat i la destrucció de suports d'emmagatzematge d'informació.

· La información de este nivel de confidencialidad que deba utilizarse fuera de las dependencias de la Universidad ha de ser mínima y cumplir con las medidas de seguridad establecidas en Procedimiento de acceso local y remoto de la Universidad de Alicante.

Cualquier incidencia asociada con la disponibilidad o confidencialidad de la información deberá ser inmediatamente reportada al responsable de seguridad siguiendo el proceso de gestión de incidentes de seguridad de la información habilitado para tal fin.

Artículo 4.2.3 Información de Uso Oficial Restringido

El personal responsable de cada aplicación en los que se ubique o trate información de este nivel de clasificación deben gestionar las autorizaciones de acceso a dichas aplicaciones, revisándolas periódicamente, y monitorizando los accesos.

Los usuarios o usuarias de los Sistemas de Información y los procesos automáticos solo obtendrán el acceso, los privilegios o los permisos que necesiten para realizar su cometido, con el fin de limitar los daños resultantes de accidentes, errores o uso no autorizado de recursos de los Sistemas de Información.

Toda la información restringida que contenga datos personales con categorías especiales de datos se deberá cifrar tanto en su almacenamiento como en su transmisión, mediante uno de los algoritmos autorizados para tal fin y con la fortaleza requerida en la Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

No podrá publicarse en Internet sin restricciones de acceso la información catalogada como información de Uso Oficial Restringido.

Intercambio de información. Se debe ser especialmente cuidadoso en el envío de esta información por correo electrónico, mediante dispositivos extraïbles o la utilización de almacenamiento en la nube. Siempre que sea posible, se utilizarán sistemas corporativos y la información se transmitirá y almacenará cifrada mediante uno de los algoritmos autorizados para tal fin y con la fortaleza requerida en la Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

Cualquier incidencia asociada con la disponibilidad o confidencialidad de la información deberá ser inmediatamente reportada al responsable de seguridad siguiendo el proceso de gestión de incidentes de seguridad de la información habilitado para tal fin a la mayor brevedad posible para poder cumplir con los plazos legales.

Para el tratamiento de esta información se aplicarán las siguientes medidas de seguridad:

· Respetar de forma escrupolosa las directrices de Protección del puesto de trabajo informático de la Universidad de Alicante, Puesto de trabajo despejado y equipo bloqueado y procedimiento para la limpieza de metadatos y procedimiento para el borrado y destrucción de soportes de almacenamiento de información.

· Los responsables de cada entorno en los que se ubique o trate información de este nivel de confidencialidad deben gestionar las autorizaciones de acceso a dichos entornos, revisándolas periódicamente, y monitorizando los accesos, conforme a procedimiento de acceso local y remoto de la Universidad de Alicante.

· La información de este nivel de confidencialidad que deba utilizarse fuera de las dependencias de la Universidad ha de ser mínima y cumplir con las medidas de seguridad establecidas en Procedimiento de acceso local y remoto de la UA.

· Cuando la información ya no sea necesaria se procederá a su borrado y destrucción segura teniendo en cuenta que se han cumplido los requerimientos de retención de datos en cada Sistema de Información de cara a la realización de acciones administrativas, disciplinarias, civiles o penales. Para esto se debe seguir el procedimiento para el borrado y la destrucción de soportes de almacenamiento de información.

La informació d'ús oficial restringit de la Universitat d'Alacant haurà d'utilitzar-se exclusivament durant l'acompliment de les tasques de la Universitat. Es prohibeix l'ús d'aquesta per a altres propòsits que estiguen fora de l'interès de l'organització.

Article 5. Responsabilitats

Cada membre de la Universitat d'Alacant vetlarà, dins del seu àmbit, pel compliment de la normativa i revisarà la correcta implantació o compliment d'aquesta.

L'ús inadequat d'informació d'ús oficial restringit està prohibit en la Universitat. Les persones usuàries autoritzades no utilitzaran els sistemes d'informació per a ús no apropiat, i tindran en compte els punts següents:

- Es prohibeix l'accés no autoritzat a qualsevol informació de naturalesa restringida.
- Es prohibeix als usuaris o usuàries tenir accés a la informació, de qualsevol naturalesa o mitjà, tret que hi tinguen autorització.
- Es prohibeix compartir informació d'ús oficial restringit de qualsevol índole amb persones que no estiguen autoritzades a conèixer aquesta informació.
- Els usuaris o usuàries autoritzats tenen la responsabilitat de saber que si fan un ús inapropiat de la confidencialitat de la informació universitària, se'ls pot negar l'accés futur a la informació i estaran subjectes a les sancions disciplinàries establides.

Disposició final. Aprovació i entrada en vigor

Aquest document ha sigut revisat per la Comissió de seguretat TI de la UA amb data 3 de novembre del 2022, i estableix d'aquesta forma les directrius generals per a l'ús adequat dels recursos de tractament d'informació que la UA posa a la disposició dels usuaris per a l'exercici de les seues funcions i que, correlativament, assumeixen les obligacions descrites, i es comprometen a complir amb el que disposen els epígrafs següents.

Entrarà en vigor l'endemà de la seua publicació en el BOUA, prèvia aprovació pel Consell de Govern de la Universitat d'Alacant. Aquesta Normativa és efectiva des d'aquesta data de publicació i fins que siga reemplaçada per una de nova.

La información de uso oficial restringido de la Universidad de Alicante deberá utilizarse exclusivamente durante el desempeño de las tareas de la Universidad. Se prohíbe su uso para otros propósitos que estén fuera del interés de la organización.

Artículo 5. Responsabilidades

Cada miembro de la Universidad de Alicante velará, dentro de su ámbito, por el cumplimiento de la normativa y revisará su correcta implantación o cumplimiento.

El uso inadecuado de información de uso oficial restringido está prohibido en la Universidad. Los usuarios o usuarias autorizados no utilizarán los sistemas de información para uso no apropiado, teniendo en cuenta los siguientes puntos:

- Se prohíbe el acceso no autorizado a cualquier información de naturaleza restringida.
- Se prohíbe a los usuarios o usuarias tener acceso a la información, de cualquier naturaleza o medio, salvo que dispongan de autorización.
- Se prohíbe compartir información de uso oficial restringido de cualquier índole con personas que no estén autorizadas a conocer dicha información.
- Los usuarios o usuarias autorizados tienen la responsabilidad de saber que si hacen un uso inapropiado de la confidencialidad de la información universitaria, puede negárseles el acceso futuro a la información y estarán sujetos a las sanciones disciplinarias establecidas.

DISPOSICIÓN FINAL. Aprobación y entrada en vigor

El presente documento ha sido revisado por la Comisión de seguridad TI de la UA con fecha 3 de noviembre de 2022, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la UA pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Entrará en vigor al día siguiente de su publicación en el BOUA, previa aprobación por el Consejo de Gobierno de la Universidad de Alicante. Esta Normativa es efectiva desde esta fecha de publicación y hasta que sea reemplazada por una nueva.