REGLAMENTO SOBRE UTILIZACIÓN DE LOS RECURSOS DIGITALES Y SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD INTERNACIONAL DE ANDALUCÍA

I. Conforme a lo establecido en el artículo 15 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS en adelante), el significado y alcance del uso seguro de los sistemas de información deberá concretarse en unas normas de seguridad aprobadas por la dirección o el órgano superior correspondiente.
En el marco de la progresiva implantación de este modelo, y de la Política de Seguridad y Privacidad de la Información aprobada por el Acuerdo del Consejo de Gobierno de la UNIA 37/2023, de 26 de mayo (BOUNIA núm. 11/2023, de 1 de junio), el presente Reglamento viene a sintetizar los principios recogidos en los correspondientes documentos técnicos de política y normativa, como medio para facilitar la necesaria información y formación del personal, propio y ajeno, y del resto de usuarios, en relación con sus deberes, obligaciones y responsabilidades en materia de seguridad y correcta utilización de los sistemas, recursos digitales e información de los que sea titular o responsable la UNIA.

Por lo tanto, el presente Reglamento debe considerarse desarrollado y completado por los demás documentos e instrumentos que los órganos competentes de la UNIA desplieguen y aprueben en el marco del Anexo II del ENS.

II. Este Reglamento, que incorpora materialmente un código de conducta de los usuarios, consta de cinco capítulos, doce artículos, cinco disposiciones adicionales, una derogatoria y otra final. En el primero de estos capítulos se abordan el objeto y finalidad de la misma, las definiciones y su ámbito de aplicación. En el segundo se analizan la conservación y la utilización de los equipos informáticos y de telecomunicaciones, prestando una especial atención al uso del correo electrónico y de Internet. Se parte de su uso exclusivamente profesional para aportar reglas, principios de actuación y ejemplos de comportamientos especialmente prohibidos. El capítulo tercero se dedica a los sistemas de identificación, prestando una especial atención al certificado de empleado público como base para su posterior implantación en la UNIA. Finalmente, los dos últimos capítulos aportan nociones básicas sobre los deberes de los usuarios en relación con la gestión y protección de la información y la protección de datos en la UNIA, así como los posibles procedimientos de auditoría y control de estas reglas.

III. En la elaboración y tramitación de este documento se han cumplido los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas. Igualmente, y de acuerdo con lo establecido en el artículo 87 de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, este Reglamento ha sido objeto de consulta y participación con los representantes de los trabajadores, ha sido previamente informado favorablemente por el Comité de Seguridad y Privacidad de la

Información y sometido a exposición pública. En las disposiciones adicionales se prevén mecanismos de evaluación, actualización y de formación e información de los usuarios en especial, de los empleados públicos.

CAPÍTULO PRIMERO. NORMAS GENERALES

Artículo 1. Objeto y finalidad de este Reglamento

1. El presente Reglamento tiene como objeto establecer los principios básicos de seguridad en el uso de los recursos digitales, de los sistemas y de la información de la que es o pueda ser titular o responsable la UNIA.

2. Lo establecido en este Reglamento deberá ser interpretado en el marco de los documentos técnicos y de las políticas específicas que los órganos competentes de la UNIA establezcan para la completa implantación del ENS en esta institución.

3. La finalidad de este Reglamento es que todos los usuarios, tanto internos como externos, que accedan o utilicen los recursos, los sistemas o la información de la que sea titular o responsable esta universidad hagan un uso seguro y eficiente de los mismos.

Artículo 2. Definiciones

1. A los efectos previstos en este Reglamento, las definiciones, palabras, expresiones, y términos deben ser entendidos en el sentido indicado en la normativa de protección de datos personales, en la normativa en materia de procedimiento administrativo común y en la normativa de seguridad de las tecnologías de la información y la comunicación.

2. Específicamente, y a los efectos del presente Reglamento se entiende por:
   a. “Usuario”: cualquier persona que posea, acceda o utilice, de cualquier forma o en cualquier momento, los equipos, recursos, sistemas o la información de la que sea titular o responsable la UNIA.
   b.“Equipamiento informático o de telecomunicaciones”: cualquier dispositivo o instrumento tecnológico capaz de transmitir o retener información incluyendo, a mero título orientativo ordenadores, teclados, ratones, paneles o pantallas táctiles o no, escáneres, impresoras, altavoces, auriculares, micrófonos, tabletas, teléfonos y líneas telefónicas y de datos, soportes digitales o de almacenamiento, dispositivos de geolocalización, gafas, relojes inteligentes o “wareables” y, en general, elementos periféricos similares.

A estos efectos se equiparan a los mismos los programas informáticos que la UNIA incorpore a estos terminales bajo licencia.

c. "Correo electrónico corporativo": herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la UNIA, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.
d. "Uso para fines profesionales": la utilización de recursos, sistemas o información conectada y necesaria para el desarrollo y correcto cumplimiento de cuantas lícitas y justificadas necesidades conlleve su actividad como empleado público o usuario.
e. "Certificado electrónico o digital": fichero digital que permite identificar a su titular de forma inequívoca.
f. "Información o documentación sensible": es toda información clasificada como interna, confidencial o secreta, según el procedimiento de protección de la información de la UNIA.

Artículo 3. Ámbito de aplicación.

1. Este Reglamento será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, bajo régimen funcionarial, laboral u otra forma o modalidad contractual, preste sus servicios indefinidos o temporales, a tiempo completo o a tiempo parcial, para la UNIA.
Estas normas se aplicarán tanto cuando la actividad laboral se desarrolle en cualquiera de las sedes o dependencia de la UNIA como cuando esta se realice a distancia, especialmente en los supuestos de teletrabajo.

2. Igualmente será obligatorio para todos aquellos otros usuarios que utilicen cualquiera de los equipos, recursos, sistemas o información de la UNIA, ya sea como alumnos, docentes, cargos u órganos unipersonales, directores o subdirectores de cátedras o aulas universitarias, becarios, colaboradores u otros posibles perfiles de usuarios.

3. El respeto de estas normas deberá exigirse a cuantas empresas o personas contraten o se relacionen con la UNIA y/o tengan acceso a recursos, sistemas o información de la que sea titular esta Universidad.

CAPÍTULO SEGUNDO. DE LA CONSERVACIÓN Y UTILIZACIÓN DEL EQUIPO INFORMÁTICO Y DE LOS SISTEMAS DE TELECOMUNICACIONES

Artículo 4. Principios generales

1. La UNIA conservará la titularidad de cualquier equipamiento informático o de telecomunicaciones que ponga a disposición de cualquier usuario.

2. Los usuarios deberán custodiar estos equipos y conservarlos en perfectas condiciones, permitiendo en su caso el acceso a los mismos del personal de soporte técnico que será el único autorizado para la instalación de software.
Todo usuario deberá comunicar inmediatamente al responsable de seguridad cualquier deterioro o pérdida, así como cualquier anomalía o posible uso incorrecto o ilegal realizado por un tercero.

En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el Área de Gestión de las TIC y relacionadas con la seguridad.

3. Está prohibido alterar cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, así como distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.

4. Los dispositivos, programas y servicios informáticos que la UNIA ponga a disposición de los usuarios deberán utilizarse exclusivamente para el desarrollo de fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

5. A la finalización de tales funciones, y con independencia de los procedimientos internos establecidos en la UNIA, deberán proceder a la devolución de estos recursos o equipos en el plazo más breve posible, que nunca excederá de un mes.

Artículo 5. Actividades y usos prohibidos

1. Queda prohibido todo uso para fines particulares de los equipos informáticos y de telecomunicaciones aportados por la UNIA. El personal deberá utilizar sus propios medios tecnológicos para tales fines.
Ello supone la expresa aceptación por los usuarios de la inexistencia de cualquier dato personal, no profesional, del usuario en los medios proporcionados por la UNIA.
Por tanto, la hipotética violación de esta regla no impedirá, junto a otras posibles consecuencias, la posible y lícita auditoria y análisis de estos y de su utilización por parte del personal técnico de la UNIA.

2. Partiendo de la premisa anterior, está terminantemente prohibida la utilización de tales equipos para el desarrollo de actividades ilícitas o ilegales, que infrinjan los derechos de

la organización, de cualquier miembro de la comunidad universitaria o de terceros, o que puedan atentar contra la seguridad, la legislación vigente o la normativa aplicable.
A modo de ejemplo, quedan terminantemente prohibidos, pudiendo ser objeto en su caso, y entre otras, de sanción disciplinaria:

a. Su utilización para almacenar, transmitir o distribuir cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.
b. La incorporación o uso de cualquier software dañino o la introducción de código malicioso, dispositivo o físico o cualquier secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos o de interceptar, acceder, copiar, extraer o transmitir sin autorización información confidencial o de carácter personal.
c. La instalación, el uso, reproducción, cesión, transformación o comunicación pública y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. En este sentido, se prohíben la reproducción, modificación, cesión, transformación o comunicación de programas informáticos, salvo en los términos en los que la licencia lo permita y con autorización previa del Área TIC.
d. Intentar alterar, modificar, eliminar, distorsionar o falsear los sistemas de seguridad, incluidos los registros de los sistemas de información o intentar destruir, alterar, inutilizar o realizar cualquier otra forma de dañar los datos, programas o documentos electrónicos de la empresa. En este sentido, se prohíbe el uso de programas de utilidades que puedan ser capaces de invalidar los controles del sistema y de las aplicaciones o la protección de la información o que, por su naturaleza, hagan un uso abusivo de la red.
e. Instalar o utilizar, sin autorización del responsable de seguridad de la información, sistemas de escucha, grabación de audio y/o vídeo o de interceptación de comunicaciones en las dependencias de la UNIA o, en general, durante la jornada laboral, para espiar o interceptar las comunicaciones, informaciones, conversaciones o reuniones de carácter interno o con clientes y proveedores.

Artículo 6. Del uso del correo electrónico corporativo

1. Tanto la dirección del correo corporativo como la propia herramienta de comunicación sólo podrán ser utilizadas con fines estrictamente profesionales. El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo. Por tanto, en el mismo no deberá haber datos personales que no sean estrictamente profesionales y a los que, por tanto, no pueda acceder la UNIA.

2. En el uso del correo deberán seguirse las reglas elementales de prudencia y protección de datos. Así, y por mencionar algunas:

a. No deberán abrirse ni ejecutarse ficheros de fuentes no fiables.
b. Se deben revisar las barras de direcciones antes de enviar un mensaje para evitar suplantaciones o el envío de correos a destinatarios incorrectos. Esta cautela debe

incrementarse cuando se envíe o adjunte información sensible.
c. En el caso de reenvío de mensajes, o de cadenas de ellos, debe revisarse el contenido de los anteriores. Igualmente deberán revisarse los destinatarios cuando se opte por contestar a todos.
d. Si por necesidad urgente se ha de enviar un correo a un conjunto de destinatarios, se deberá colocar la lista de direcciones en el campo de Copia Oculta (CCO o BCC), evitando su visibilidad a todos los receptores del mensaje.

3. Está terminantemente prohibido, entro otros usos inadecuados o ilegales:

a. El envío de correos masivos o que por el volumen de sus adjuntos pueda suponer dificultades técnicas para el servicio.
b. La suplantación o utilización del correo de otro usuario o el acceso a buzones de correo electrónico y el envío de correos electrónicos desde usuarios/perfiles distintos de los asignados por la UNIA.
c. El envío de mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo cualquier norma que pudiera resultar de aplicación.
d. El uso de los servicios de la UNIA para fines comerciales o para propósitos que puedan influir negativamente en la imagen de la UNIA, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

4. Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son responsabilidad de su titular.

5. Al cesar en sus funciones deberá procederse a la cancelación de la cuenta. Si se tratase de una cuenta ligada a una función o puesto, se comunicará al responsable con un plazo razonable la necesidad de revisar la información en ella contemplada, transmitiéndose con posterioridad las credenciales y la responsabilidad de la misma al siguiente titular del órgano o puesto.

Artículo 7. Del acceso y uso de Internet corporativo

1. Las conexiones que se realicen al Internet corporativo de la UNIA deberán obedecer a fines profesionales o estrictamente ligados a la concreta finalidad que motivó su otorgamiento por esta Universidad.

2. El acceso a Internet para fines personales debe realizarse prioritariamente por los medios y conexiones privadas. De ser absolutamente necesario, el uso de la red corporativa sólo debe desarrollarse excepcionalmente, por el tiempo mínimo, sin que interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos y exclusivamente en páginas seguras y confiables.

3. Sólo se podrá acceder a Internet mediante el navegador facilitado y configurado por la

UNIA en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del Área de Gestión de las TIC.

4. Quedan terminantemente prohibidas las siguientes actuaciones:

a. La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa del Área de Gestión de la TIC.
b. La descarga de programas informáticos sin la autorización previa del Área de Gestión de las TIC o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso, debe asegurarse que el sitio Web visitado es confiable.
c. El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
d. La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por el Área de Gestión de las TIC.
e. La descarga y utilización de aplicaciones portables.

5. Deberá notificarse al Administrador de la Seguridad cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

CAPÍTULO III. DE LOS SISTEMAS DE IDENTIFICACIÓN, CERTIFICADOS Y CREDENCIALES

Artículo 8. Obligaciones con respectos a los sistemas de identificación, certificados digitales u otro tipo de credenciales o sistemas de identificación

1. Los usuarios deberán acceder a los equipos, sistemas y redes de comunicación de la UNIA utilizando los sistemas de identificación establecidos en cada caso por esta universidad.

2. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso, certificado digital, o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

3. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

4. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Administrador de la Seguridad la correspondiente incidencia de seguridad.

5. Los usuarios deben utilizar claves seguras, siguiendo las recomendaciones recogidas en la normativa POS.03 Procedimiento de Control de Acceso Lógico.

6. Si, en un momento dado, un usuario recibiera una notificación (verbal o escrita) solicitándole su identificador de usuario y/o clave, nunca facilitará dichos datos y procederá a comunicar este hecho al Administrador de la Seguridad, de forma inmediata.

Artículo 9. Sobre el certificado de empleado público

1. Los Certificados de Empleado Público tendrán, a todos los efectos, la consideración de instrumentos de uso profesional, tanto en el ejercicio de las competencias como de las funciones o tareas asignadas por el empleo público o cargo desempeñado legalmente.

2. Todos los usuarios a quienes se expida certificado de empleado público tendrán respecto a los mismos los siguientes derechos y obligaciones:

a. Colaborar en el procedimiento de expedición del mismo, mediante, en su caso, su personación ante el órgano competente. Por ello, estos empleados deberán recibir y aceptar expresamente el certificado y sus claves, así como cualesquiera elementos de seguridad que sean necesarios para su uso adecuado.
b. Proteger los elementos de seguridad entregados para el uso del sistema, en especial de las claves para la activación. El uso de este certificado está restringido únicamente a su titular. Su uso o cesión a terceros no podrá ser nunca autorizado ni admitido.
c. Utilizarlos únicamente mientras dure la relación para la cual se realizó su expedición y para los trámites y actuaciones que realicen por razón de su condición de Cargo Académico o Empleado Público.
d. Deberán solicitar su revocación cuando alguno de los datos referidos al cargo o empleo público sea inexacto o incorrecto y, en particular, a partir del momento en que cese en su relación de empleo o funcionarial con la UNIA. En caso de proseguir con su relación con la UNIA, deberán solicitar la emisión de un nuevo Certificado que subsane todos los datos inexactos previamente detectados.
e. Comunicar, de manera fehaciente, con la mayor rapidez posible al responsable de la Oficina de Registro o a la Secretaría General, la pérdida, extravío, o sospecha de acceso o de uso inadecuado del Certificado del que es usuario y custodio, con el fin de iniciar, en su caso, los trámites de su revocación. Igualmente deberá comunicar a la mayor brevedad posible cualquier incidencia de uso o de seguridad que pueda afectar al sistema de identificación o firma electrónica.
f. Los Empleados Públicos y Cargos Académicos de la UNIA se comprometen a no utilizar el Certificado cuando alguno de los datos referidos al cargo o empleo público sea inexacto o incorrecto. En especial, no podrá ser utilizado a partir del momento en que cese en su relación de empleo o funcionarial con la UNIA.

3. El incumplimiento por los empleados públicos de las obligaciones aquí recogidas podrá

ser objeto de sanción de conformidad con el régimen jurídico disciplinario que resulte de aplicación a los mismos.

4. Si un usuario o personal de la UNIA detectase cualquier anomalía que indicase una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Seguridad de la Información, quien tomará las oportunas medidas correctoras y dará traslado de la incidencia al Área competente.

5. A todos los efectos, el uso de certificado digital de usuario para persona física (certificado personal) tendrá la misma validez que el certificado de empleado público.

CAPÍTULO IV. DE LA GESTIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Artículo 10: Respeto a la normativa de protección de datos y de seguridad de la información

1. Todos los usuarios de la UNIA están obligados a respetar la normativa general en materia de protección de datos y de seguridad de la información, acatando las políticas y normas que en este campo elabore y aplique la UNIA.

2. Los usuarios sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.

3. En el tratamiento de los datos personales deberá respetarse en todo caso los principios de:

a. Licitud, lealtad y transparencia en relación con el interesado. Por tanto, el tratamiento, que incluye la recogida de los datos, solo será lícito si existe consentimiento expreso del interesado para uno o varios fines específicos; si es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; si es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; para proteger intereses vitales del interesado o de otra persona física; para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, o, en general, cuando el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.
b. Limitación de la finalidad. De acuerdo con este principio, estos datos solo serán

recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

c. Minimización de datos. En virtud de este principio solo se recogerán y se tratarán ulteriormente aquellos datos adecuados, pertinentes y limitados a lo necesario en relación con los fines necesariamente lícitos y determinados para los que son tratados.

d. Exactitud y actualización. Se adoptarán, por tanto, todas las medidas razonables para que se supriman o se rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan o se trataron.

e. Limitación del plazo de conservación. Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo, salvo excepciones normativamente previstas, del necesario para los fines del tratamiento de los datos personales.

f. Integridad y confidencialidad. En virtud de este principio debe garantizarse una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

g. Responsabilidad proactiva. De acuerdo con este principio, el responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas y que permitan garantizar y poder demostrar que el tratamiento es conforme al marco normativo en cada momento vigente.

4. Todo usuario (de la UNIA o de terceras organizaciones) que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral, profesional o de cualquier tipo, que mantenga con la UNIA.

5. En el desempeño de sus funciones y siempre que estén en relación con información o datos personales de la UNIA, los usuarios deberán adoptar las medidas de seguridad de información previstas por la UNIA, y, en especial:

a. Política de despachos cerrados, mesas limpias de documentos e información, especialmente sensible, pizarras borradas. Nunca deben mantenerse sobre las mesas documentos con información relevante de manera que puedan ser leídos por otras personas.

b. La información sensible, tanto en papel como en soportes de almacenamiento electrónico, debe estar guardada (en una caja fuerte, armario u otro tipo de mueble de seguridad), cuando no se necesite, especialmente cuando la oficina está vacía.

c. Mantener copias de seguridad es una cautela esencial de protección de la información. Los datos generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, vinculado a la cuenta institucional del usuario o en unidades de red compartidas alojadas en los servicios Cloud de la universidad. Se debe evitar el almacenamiento de documentos en los equipos locales, salvo aquellos archivos que sean de uso temporal.

d. No transferirá al exterior información no necesaria y justificada, prestando especial cuidado a posibles errores de comunicación o envío, por ejemplo, a través de correo electrónico.

e. Cuando se imprima documentación, deberá permanecer el menor tiempo posible en

las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma. Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia y borrar el archivo escaneado una vez remitido a nuestra dirección. Si se encontrase documentación sensible abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de Gerencia.

f. Los usuarios bloquearán y apagarán el PC (incluido el monitor y la impresora local, en su caso) cuando se deje de atender durante un cierto tiempo el equipamiento informático y, en todo caso, al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.

g. En cualquier caso, las copias de seguridad y la información personal que haya sido objeto de tratamiento será eliminada de los soportes temporales cuando haya finalizado el procedimiento para el que se requirió este.

6. Las obligaciones y condiciones contenidas en este Reglamento referentes a la confidencialidad, reserva, no divulgación y secreto continuarán vigentes tras la finalización de las actividades, la relación, las funciones y las responsabilidades que se le hubieran asignado o desarrolle el usuario para la UNIA. Asimismo, se deberán devolver los soportes de información utilizados inmediatamente después de la finalización de las tareas que hubieren originado su uso.

En este sentido, los datos, documentos, archivos, programas, análisis o cualquier otra información que hayan generado, utilizado o conocido por su relación con la UNIA no pueden ser destruidos, borrados o alterados y deberán ser entregados al finalizar la relación, salvo que exista un pacto previo entre las partes, o que una normativa interna o la legislación vigente establezcan otra cosa al respecto.

Cuando finalice la relación entre el usuario y la UNIA, el personal autorizado por esta última podrá revisar los sistemas que habían sido puestos a disposición del usuario para su evaluación, mantenimiento y reutilización.

CAPÍTULO V. DEL CONTROL Y LAS POSIBLES EXCEPCIONES A LAS REGLAS GENERALES ESTABLECIDAS EN ESTE REGLAMENTO

Artículo 11. Procesos para la autorización y control del cumplimiento

Para todos aquellos aspectos relativos al uso o la operación con los sistemas que constituyan una excepción respecto a lo establecido con carácter general, tanto en la presente normativa como en el resto de procedimientos operativos del sistema de gestión de la Seguridad y Privacidad de la Información, se seguirá un proceso de autorización que se iniciará con una solicitud del responsable del departamento o unidad pertinente, la cual será registrada y tratada en el sistema de gestión de peticiones de servicio. Se seguirá lo indicado en el Procedimiento de gestión de autorizaciones accesible a través del

correspondiente apartado de la web.

Artículo 12. Control y monitorización

1. La UNIA, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

a. Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
b. Monitorizará los accesos a la información contenida en sus sistemas.
c. Auditará la seguridad de las credenciales y aplicaciones.
d. Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

2. La UNIA llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegítimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

3. Cuando existan indicios de uso ilícito o abusivo por parte de un empleado, la UNIA realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoría en el ordenador utilizado por el empleado o en los sistemas que ofrecen el servicio. Los resultados podrán ser puestos en conocimiento de las autoridades administrativas o judiciales pertinentes. Respecto a la normativa de aplicación se aplicará el Estatuto de los Trabajadores (ET), la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD y GDD) y demás normativa de aplicación.

4. Si se demostrase un uso abusivo o inapropiado de estos servicios, la UNIA podrá adoptar las medidas disciplinarias que considere oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar.

Disposición adicional primera. Formación e información a los usuarios

La UNIA proporcionará información y formación suficiente y contextualizada sobre el contenido de este Reglamento a todos los posibles usuarios.
El contenido de este Reglamento estará disponible permanentemente en la página web de la UNIA y formará parte de los temarios de oposiciones y pruebas de acceso del personal a esta universidad.

Disposición adicional segunda. Incorporación a pliegos, convenios y demás instrumentos similares

Cuando como consecuencia de su actividad, la UNIA prevea que otras empresas, personas o instituciones puedan acceder o utilizar los instrumentos, recursos, servicios o informaciones a los que hace referencia este Reglamento, exigirá a tales empresas, personas o servicios que declaren conocer y respetar en las mismas las reglas y deberes establecidos en la correspondiente normativa.

Disposición adicional tercera. Evaluación y revisión de este Reglamento

En el marco de las evaluaciones anuales realizadas por los órganos competentes en materia de seguridad de la UNIA se analizará en este mismo lapso temporal la necesidad o conveniencia de su posible revisión.
En su caso, las propuestas de modificación serán transmitidas a la Secretaría General de esta Universidad y al órgano competente en materia de personal que, previo cumplimiento de las obligaciones legales o reglamentarias de participación de los empleados públicos, y de los órganos competentes en materia de seguridad de la información, podrá proponer las correspondientes mejoras al Consejo de Gobierno de esta Universidad.

Caso de aprobarse, se elaborará un texto consolidado de este Reglamento del que serán informados y formados los empleados públicos.

Disposición adicional cuarta. No afectación

Este Reglamento en ningún caso modifica ni altera el procedimiento establecido en la Instrucción conjunta 1/2023 de la Secretaría General y de la Gerencia de la Universidad Internacional de Andalucía mediante la que se articula el procedimiento para la comunicación de los nombramientos de cargos a las distintas universidades andaluzas interesadas.

Disposición adicional quinta. Cita en género femenino de los preceptos de estas normas.

Todos los preceptos de este texto refundido que utilizan la forma del masculino genérico se entenderán aplicables a cualquier persona con independencia de su sexo.

Disposición derogatoria

Quedan derogadas, en cuanto entren en contradicción con lo aquí establecido, tanto la Normativa de uso de los Recursos Informáticos y de Comunicaciones de la Universidad Internacional de Andalucía, aprobada en Consejo de Gobierno de 22 de octubre 2014 y modificada por el mismo órgano el 18 de noviembre de 2014, como la Normativa de Seguridad de la Información de la Universidad Internacional de Andalucía, aprobada en Consejo de Gobierno el 5 de febrero de 2019 y modificado en Consejo de Gobierno el 28 de enero de 2022.

Disposición final

Este Reglamento entrará en vigor a los quince días de su publicación en el Boletín Oficial de la Universidad Internacional de Andalucía.