

**FRANCISCO ÁLVAREZ ARROYO, SECRETARIO GENERAL DE LA  
UNIVERSIDAD DE EXTREMADURA,**


**CERTIFICA:**

Que, en la sesión extraordinaria del Consejo de Gobierno de esta Universidad celebrada en la Sala de videoconferencia creada al efecto mediante medios telemáticos, el día 21 de febrero de 2024, en el punto, en el punto 5º Transformación Digital; 5.1: "Aprobación, si procede, de la normativa general de utilización de los recursos y los sistemas de información", se tomó el siguiente acuerdo:

**Aprobar la normativa general de utilización de los recursos y los sistemas de información,** conforme a la documentación suministrada que se adjunta como anexo al acta de la sesión.

*De conformidad con lo previsto en el artículo 19.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se hace constar que la presente certificación se expide con anterioridad a la aprobación del Acta de la citada sesión de Consejo de Gobierno.*

Y para que conste y surta efectos, extendiendo la presente, con el Vº Bº del Sr. Rector Magfco., en Badajoz a 21 de febrero de dos mil veinticuatro.

<b>Código Seguro De Verificación</b>	VZg1YqKErG1RZyXvg8V2gQ==	<b>Estado</b>	<b>Fecha y hora</b>	
<b>Firmado Por</b>	Francisco Álvarez Arroyo - Sede Secretario General	Firmado	02/05/2024 11:10:32	
<b>Observaciones</b>		<b>Página</b>	1/1	
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/VZg1YqKErG1RZyXvg8V2gQ==">https://uex09.unex.es/vfirma/code/VZg1YqKErG1RZyXvg8V2gQ==</a>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			



# NG.01 NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN

*Documento de uso interno*

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	1/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## ÍNDICE

<b>1</b>	<b>Objetivo</b> .....	<b>5</b>
<b>2</b>	<b>Ámbito de aplicación</b> .....	<b>6</b>
<b>3</b>	<b>Vigencia</b> .....	<b>6</b>
<b>4</b>	<b>Revisión y evaluación</b> .....	<b>6</b>
<b>5</b>	<b>Utilización del equipamiento informático y de comunicaciones</b> .....	<b>7</b>
5.1	Normas generales.....	7
5.2	Usos específicamente prohibidos.....	9
5.3	Normas específicas para el almacenamiento de información.....	10
5.4	Normas específicas para equipos portátiles y móviles.....	10
5.5	Normas específicas para memorias/lápices USB (pendrives).....	11
5.6	Grabación de CDs y DVDs.....	12
5.7	Copias de seguridad.....	12
5.8	Borrado y eliminación de soportes informáticos.....	13
5.9	Impresoras en red, fotocopiadoras y faxes.....	13
5.10	Digitalización de documentos.....	14
5.11	Cuidado y protección de la documentación impresa.....	14
5.12	Pizarras y flipcharts.....	14
5.13	Protección de la propiedad intelectual.....	14
5.14	Protección de la dignidad de las personas.....	15
<b>6</b>	<b>Uso eficiente de equipos y recursos informáticos</b> .....	<b>15</b>
<b>7</b>	<b>Instalación de software</b> .....	<b>15</b>
<b>8</b>	<b>Acceso a los sistemas de información y a los datos tratados</b> .....	<b>16</b>
<b>9</b>	<b>Identificación y autenticación</b> .....	<b>17</b>
<b>10</b>	<b>Acceso y permanencia de terceros en los edificios, instalaciones y dependencias</b> .....	<b>17</b>
10.1	Normas.....	17
10.2	Modelo de protocolo de firma.....	18
10.3	Modelo de autorizaciones y habilitaciones personales.....	18
<b>11</b>	<b>Confidencialidad de la información</b> .....	<b>19</b>
<b>12</b>	<b>Protección de datos de carácter personal y deber de secreto</b> .....	<b>20</b>
<b>13</b>	<b>Tratamiento de la información</b> .....	<b>20</b>
<b>14</b>	<b>Salidas de información</b> .....	<b>20</b>
<b>15</b>	<b>Copias de seguridad</b> .....	<b>21</b>
<b>16</b>	<b>Conexión de dispositivos a las redes de comunicaciones</b> .....	<b>21</b>

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	2/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





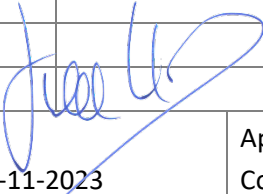
<b>17</b>	<b>Uso del correo electrónico corporativo .....</b>	<b>22</b>
<b>18</b>	<b>Acceso a internet y otras herramientas de colaboración.....</b>	<b>22</b>
18.1	Normas generales .....	22
18.2	Usos específicamente prohibidos .....	23
<b>19</b>	<b>Incidencias de seguridad.....</b>	<b>23</b>
<b>20</b>	<b>Compromisos de los usuarios .....</b>	<b>23</b>
<b>21</b>	<b>Control de actuaciones sobre las bases de datos de la UEx.....</b>	<b>24</b>
<b>22</b>	<b>Uso abusivo de los sistemas de información.....</b>	<b>24</b>
22.1	Uso abusivo del acceso a internet .....	25
22.2	Uso abusivo del correo electrónico .....	25
22.3	Uso abusivo de otros servicios y sistemas de la UEx .....	25
<b>23</b>	<b>Monitorización y aplicación de esta normativa .....</b>	<b>27</b>
<b>24</b>	<b>Incumplimiento de la normativa.....</b>	<b>28</b>
<b>25</b>	<b>Modelo de aceptación y compromiso de cumplimiento.....</b>	<b>28</b>
<b>26</b>	<b>Referencias .....</b>	<b>28</b>
<b>ANEXO I. Protocolo de firma.....</b>		<b>30</b>
<b>ANEXO II. Autorizaciones y habilitaciones.....</b>		<b>31</b>
<b>ANEXO III. Modelo de Aceptación y compromiso de cumplimiento .....</b>		<b>32</b>

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	3/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





### CONTROL DE VERSIONES

Revisión	Fecha	Motivo del Cambio
0.2	10/01/2024	Revisión Servicios jurídicos
Realizado y revisado Comité de Seguridad: 17-11-2023		Aprobado Consejo de Gobierno: 21-febrero-2024



<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	4/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





# 1 Objetivo

Conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo (que sustituye a los anteriores: Real Decreto 3/2010, de 8 de enero y Real Decreto 951/2015, de 23 de octubre), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), este documento contiene la **Normativa General de Utilización de los Recursos y Sistemas de Información de la Universidad de Extremadura**, gestionados o bajo la responsabilidad de la Universidad de Extremadura, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

La presente Normativa General de Utilización de los Recursos y Sistemas de Información de la Universidad de Extremadura 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 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a la Universidad de Extremadura (a partir de ahora, UEx), por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para la UEx:

- Facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión, y
- Proporcionar información completa, homogénea, actualizada y fiable.

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la UEx a determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

Por tanto, la presente Normativa General de Utilización de los Recursos y Sistemas de Información de la UEx tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

Este documento se considera de uso interno de la UEx y, por tanto, no podrá ser divulgado salvo autorización del Responsable de Seguridad/Comité de Seguridad.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	5/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 2 Ámbito de aplicación

Esta normativa general es de aplicación a todo el ámbito de actuación de la UEx, y sus contenidos traen causa de las directrices de carácter más general definidas en la **Política de Seguridad de la Información** de la Uex (aprobada en Consejo de Gobierno el 25 de mayo de 2023, publicada en el DOE de 8 de junio de 2023).

La presente Normativa General de Utilización de los Recursos y Sistemas de Información es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la UEx, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la UEx.

En el ámbito de la presente normativa, se entiende por **usuario** cualquier empleado público perteneciente o ajeno a la UEx así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la UEx y que utilice o posea acceso a los Sistemas de Información de la UEx.

## 3 Vigencia

La presente Normativa General de Utilización de los Recursos y Sistemas de Información ha sido aprobada por el Comité de Seguridad de la UEx, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la UEx 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.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la UEx.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa General.

## 4 Revisión y evaluación

La gestión de esta Normativa General corresponde al Comité de Seguridad que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	6/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa General, que se someterá, de haber modificaciones, a aprobación.

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

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

## 5 Utilización del equipamiento informático y de comunicaciones

La UEx facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la UEx pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos de la UEx, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados por la UEx para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

### 5.1 Normas generales

- La UEx dispone de dos redes virtuales diferenciadas y aisladas unas de otras: red de gestión, red de docencia e investigación.
- Actualmente, no existe una adquisición centralizada de los equipos informáticos conectados a la red de gestión. Sin embargo, con el objetivo de una mejor organización y aseguramiento del puesto de trabajo, y tras la aprobación de esta norma, los equipos informáticos conectados a la red de gestión serán asignados por el Servicio de Informática y Comunicaciones (SICUE).
- Existirá un inventario actualizado de los equipos informáticos de la red de gestión y docencia e investigación. El SICUE se encargará de gestionar dicho inventario.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	7/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		







- A cada usuario que necesite acceder a la red de gestión, el SICUE le facilitará acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales, creándole una cuenta de usuario dentro de los servicios de identificación y autenticación de la UEx (actualmente, se utiliza “*dominio activo*” de Microsoft).
- Para el alta de estos usuarios, se requerirá:
  - Nombre, apellidos y NIF.
  - Despacho/ubicación, teléfono y dirección de correo electrónico.
  - Área a la que se incorpora.
  - Servicios a los que requiere acceso.
  - Aplicaciones y perfiles.
  - Otros datos que, por la naturaleza del servicio que vaya a utilizarse, se requieran solicitar.
- Los ordenadores personales deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
- Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de la UEx. Cuando se precise instalar dispositivos no provistos por la UEx deberá solicitarse autorización previa al SICUE y Comunicaciones.
- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del SICUE. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
- Salvo autorización expresa del SICUE, los usuarios no tendrán privilegio de administración sobre los equipos.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
- Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable del Sistema que tomará las oportunas medidas correctoras y dará traslado de la incidencia
- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	8/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





a la correcta actualización, configuración y funcionamiento de los programas antivirus, cortafuegos o cualquier otro de índole similar.

- Los usuarios deberán notificar al Centro de Atención al Usuario (CAU) de la UEx, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Para ello, se seguirán las instrucciones indicadas en el apartado 19. Incidentes de Seguridad de esta norma.
- Salvo casos excepcionales y autorizados (por ejemplo, ordenadores instalados en las zonas comunes de acceso a Internet), cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su correcto uso.
- El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y notificando tales circunstancias.
- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de diferentes medios y mecanismos: disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico, instalación de programas descargados desde Internet, mensajes SMS, llamadas telefónicas, acceso a redes sociales, acceso a recursos externos compartidos en la nube. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.
- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al SICUE, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por la UEx estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

## 5.2 Usos específicamente prohibidos

Están terminantemente prohibidos los siguientes comportamientos:

- Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.)
- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	9/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la UEx, sin la previa autorización del SICUE.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por el SICUE
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa del SICUE.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

### 5.3 Normas específicas para el almacenamiento de información

- Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.
- La UEx puede poner a disposición de sus usuarios almacenamiento compartido en la nube para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que este almacenamiento es un recurso limitado y compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa del SICUE.

### 5.4 Normas específicas para equipos portátiles y móviles

- Los equipos portátiles corporativos que necesiten acceder a la red de gestión tendrán la misma consideración que los equipos de sobremesa y deberán ser asignados y configurados por el SICUE.
- Los móviles corporativos serán asignados exclusivamente por el SICUE.
- Existirá un inventario actualizado de los equipos portátiles y móviles.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del SICUE. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del SICUE para la adopción de las medidas que correspondan y a efectos de baja en el inventario.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	10/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de la UEx.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la UEx o no autorizadas para ello.
- En general, los equipos portátiles no deberán conectarse directamente a redes externas (incluyendo la red o el acceso a Internet del usuario en su domicilio). La UEx puede proporcionar accesos remotos autorizados y configurados por la SICUE a través de tarjetas móviles. Cuando este sea el caso, deberán realizar de forma obligatoria dicha conexión cuando requieran el acceso a Internet desde dichos equipos. En casos debidamente justificados y previamente autorizados por la SICUE se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente Normativa General que resulten de aplicación.
- Los usuarios de equipos portátiles deberán realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por el SICUE, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad. En su defecto, los equipos portátiles serán entregados al SICUE para la actualización de tal software.
- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).
- Como norma general, los equipos portátiles se configurarán por defecto con todos los canales, puertos y sistemas de comunicaciones de salida de información bloqueados (wifi, bluetooth, USB's, CD, DVD, tarjetas de red, etc.). Por petición justificada dirigida al SICUE, se podrán habilitar algunas o todas las funciones de salida de información.
- Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá al SICUE llevar a cabo estas modificaciones.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) Que originaron la entrega de un recurso informático móvil, el usuario lo devolverá al SICUE, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

## 5.5 Normas específicas para memorias/lápices USB (pendrives)

Con carácter general, el uso de memorias USB en la UEx no está autorizado. En su caso, la autorización deberá proporcionarla el SICUE.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	11/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y el SICUE.

En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por la UEx, que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario de la UEx, no debiendo ser usados fuera de éstos.

Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. El SICUE podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas de la UEx unidades de almacenamiento en red, que podrán usarse para tal propósito.

La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del SICUE, de forma inmediata.

## 5.6 Grabación de CDs y DVDs

Con carácter general, el uso de equipos grabadores de CDs y DVDs en la UEx no está autorizado. En su caso, la autorización deberá proporcionarla el SICUE.

Por razones de seguridad, los equipos grabadores de CDs y DVDs de los puestos de trabajo estarán deshabilitados. En el caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y por el SICUE.

## 5.7 Copias de seguridad

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 en la nube corporativa de la UEx.

De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de estos repositorios. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse al CAU del SICUE.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	12/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 5.8 Borrado y eliminación de soportes informáticos

Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información. En este sentido, el usuario deberá:

- Asegurarse del contenido de cualquier soporte antes de su eliminación.
- Cuando contenga información sensible, confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por la UEx.

Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por el SICUE, previa petición del jefe de la unidad. Esta petición deberá dirigirse a través de la apertura de una incidencia, que será responsable de la destrucción o almacenamiento de los medios informáticos obsoletos.

## 5.9 Impresoras en red, fotocopiadoras y faxes

Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la UEx y, en su consecuencia, estén debidamente inventariados.

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. Si se encontrase documentación sensible, confidencial o protegida 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 del SICUE.

Los faxes se consideran equipos obsoletos y por tanto deben retirarse de la red corporativa en el plazo máximo de un año, salvo autorización expresa de la Gerencia de la UEx. Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización precisa.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	13/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 5.10 Digitalización de documentos

Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.

Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, 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 del SICUE.

## 5.11 Cuidado y protección de la documentación impresa

La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.

Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de la UEX, de forma que no sea recuperable la información que pudieran contener.

Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.

Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

## 5.12 Pizarras y flipcharts

Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiaran adecuadamente las pizarras, flipcharts o cualquier otro dispositivo utilizado en las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

## 5.13 Protección de la propiedad intelectual

Está estrictamente prohibida la ejecución de programas informáticos en los sistemas de información de la UEX sin la correspondiente licencia de uso.

Los programas informáticos propiedad de la UEX o licenciados a la UEX están protegidos por la vigente legislación sobre propiedad intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa del SICUE.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	14/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		







Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de propiedad intelectual, sin la debida autorización del SICUE.

## 5.14 Protección de la dignidad de las personas

Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

## 6 Uso eficiente de equipos y recursos informáticos

Dentro de las medidas de austeridad y reducción del gasto de la UEx, se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios.

- Apagar el equipo (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética. Esta norma es de obligado cumplimiento para todos los equipos conectados a la red de gestión de la UEx, salvo autorización expresa del SICUE.
- Imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color.
- Se optará por usar las impresoras en red antes que las locales.
- Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.

## 7 Instalación de software

Únicamente el personal de soporte técnico autorizado por el SICUE podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios conectados a la red de gestión.

En el caso que un usuario necesite utilizar una aplicación o herramienta de uso común perteneciente al catálogo disponible en la UEx de este tipo de aplicaciones, no instalada previamente, deberá solicitarla al SICUE, que procederá a analizar la conveniencia de la instalación y la realizará eventualmente.

Todo usuario podrá solicitar la inclusión de una aplicación en dicho catálogo de aplicaciones autorizadas para su estudio por parte del SICUE

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora	
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37	
Observaciones		Página	15/32	
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			





No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de propiedad intelectual.

Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la UEx de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el SICUE, especialmente aquellas relacionadas con la seguridad.

## 8 Acceso a los sistemas de información y a los datos tratados

Los datos gestionados por la UEx y tratados por cualquier sistema de información de la UEx deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

El alta de los usuarios será comunicada al SICUE. Para acceder a los recursos informáticos es necesario tener asignada previamente una cuenta de usuario y estar dado de alta en los servidores de dominio. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por el SICUE en caso de mala utilización.

Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

Cuando un usuario deje de atender un equipo durante un cierto tiempo, es necesario bloquear la sesión de usuario, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlos. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el pc de un usuario se bloqueará automáticamente tras un periodo de inactividad de 15 minutos.

La baja de los usuarios será comunicada al SICUE, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	16/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 9 Identificación y autenticación

Los usuarios dispondrán de un código de usuario y una contraseña o bien una tarjeta criptográfica con certificado digital, para el acceso a los sistemas de información de la UEx, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del pc o terminal desde el que se realiza el acceso.

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

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

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

Los usuarios deben utilizar contraseñas seguras: las contraseñas han de tener una longitud mínima de 8 caracteres, incluyendo letras mayúsculas y minúsculas, caracteres especiales (del tipo @, #, +, etc.) y dígitos numéricos. Las contraseñas no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables al usuario (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.). Las contraseñas deberán cambiarse periódicamente, como máximo cada 365 días.

Si, en un momento dado, un usuario recibiera una llamada telefónica (o un mensaje de cualquier tipo) solicitándole su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar el incidente de forma inmediata.

Dada la importancia de la gestión de contraseñas, se va a desarrollar una norma específica: **NP.40 Normas de Creación y uso de contraseñas.**

## 10 Acceso y permanencia de terceros en los edificios, instalaciones y dependencias

### 10.1 Normas

Los terceros ajenos a la UEx que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias con equipamiento del SICUE, deberán observar las siguientes normas:

- El personal ajeno a la UEx que temporalmente deba acceder a los sistemas de información de la UEx, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de la UEx (enlace) y previa autorización del SICUE.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	17/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





- Cualquier incidencia que surja antes o en el transcurso del acceso a la UEx deberá ponerlo en conocimiento de su enlace. La función del enlace será dar asesoramiento, atender consultas o necesidades, transmitir instrucciones, ponerle al corriente de sus cometidos, objetivos, etc.
- Para los accesos de terceros a los sistemas de información de la UEx, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en la UEx. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.
- Tales personas, en lo que les sea de aplicación, deberán cumplir puntualmente la presente normativa general, así como el resto de normativa de seguridad de la UEx, especialmente en lo referente a los apartados de salida y confidencialidad de la información.
- Para acceder a los edificios, instalaciones o dependencias de la UEx deberá estar en posesión de la correspondiente documentación de identificación personal admitida en derecho (DNI., pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que pertenezca. La primera vez que acceda físicamente deberá identificarse al personal de control de acceso y solicitar la presencia de la persona responsable de la UEx, que constituirá su enlace durante su estancia en él.
- La acreditación personal que se le proporcione en el control de acceso deberá portarse en lugar visible en todo momento, debiendo ser entregada a la salida.
- Una vez en el interior de los edificios, dependencias o instalaciones de la UEx, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común (aseos, comedor, zona de máquinas de cafetería, etc.).
- Asimismo, deberán tener autorización del enlace cuando tengan necesidad de realizar desplazamientos entre distintos departamentos de la UEx.
- Los terceros atenderán siempre los requerimientos que le hiciera el personal de control y seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

## 10.2 Modelo de protocolo de firma

Se propone el uso del documento definido en el Anexo I. Protocolo de firma de esta norma, para la identificación y autorización del acceso de terceros a las instalaciones de la UEx.

## 10.3 Modelo de autorizaciones y habilitaciones personales

Aquellas áreas o dependencias requisitos concretos de seguridad, podrá disponer de su propio Modelo de Autorizaciones y Habilitaciones personales. Se propone el uso del documento definido en el Anexo II. Autorizaciones y habilitaciones.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	18/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 11 Confidencialidad de la información

Como medida de protección de la información propia, confiada o tratada por la UEx, está absolutamente prohibido el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiere sido previamente autorizada por el SICUE.

Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por la UEx (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

En el caso de entrar en conocimiento de información que no sea de libre difusión, en cualquier tipo de soporte, deberá entenderse que dicho conocimiento es estrictamente temporal mientras dure la función encomendada, con la obligación de secreto o reserva indefinidas y sin que ello le confiera derecho alguno de posesión, titularidad o copia del mismo. Asimismo, se deberán devolver los soportes de información utilizados inmediatamente después de la finalización de las tareas que hubieren originado su uso.

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.

Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de mínimo privilegio posible y necesidad de conocer.

La información contenida en los Sistemas de Información de la UEx es propiedad de la UEx, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa del SICUE.

Los soportes de información que vayan a ser reutilizados o causen baja deberán ser previamente tratados para eliminar permanentemente la información que pudieran contener, de manera que resulte imposible su recuperación. Estos soportes deberán entregarse al SICUE.

Se evitará almacenar información sensible, confidencial o protegida en medios desatendidos (tales como CDs, DVDs, memorias USB, listados, etc.) o dejar visible tal información en la misma pantalla del ordenador.

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	19/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 12 Protección de datos de carácter personal y deber de secreto

La información contenida en las bases de datos de la UEx que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos. Los Ficheros o Tratamientos de datos de carácter personal gestionados por la UEX han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

Todo usuario (de la UEx 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 o profesional con la UEx.

## 13 Tratamiento de la información

Toda la información contenida en los Sistemas de Información de la UEx o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a la UEx y a su personal.

Cualquier tratamiento en los Sistemas de Información de la UEx deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos.

Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia de la UEx en servidores externos a la UEx salvo autorización expresa del SICUE, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la UEx y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

## 14 Salidas de información

La salida de información de la UEx (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado por el SICUE, autorización que contemplará igualmente a la propia información que sale.

La salida de datos sensibles, confidenciales o protegidos requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la normativa vigente en materia de Protección de Datos.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	20/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





Los usuarios se abstendrán de sacar al exterior cualquier información de la UEx en cualquier dispositivo (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

## 15 Copias de seguridad

Si un usuario está autorizado para almacenar información en forma local (por ejemplo, en el disco duro del PC asignado), deberá tener en cuenta que es responsable de realizar las copias de seguridad de dicha información. Por este motivo, se recomienda que los usuarios almacenen sus ficheros de trabajo en las carpetas de red habilitadas al efecto.

Por parte del SICUE se realizarán copias de seguridad de los ficheros del sistema de almacenamiento en red (carpetas de los servidores) y del resto de sistemas corporativos.

Si algún usuario desea recuperar algún fichero borrado del sistema de almacenamiento en red, lo participará al SICUE.

## 16 Conexión de dispositivos a las redes de comunicaciones

El acceso a la red de comunicaciones de la Universidad estará restringido a los usuarios a los que se hace referencia en el ámbito de esta Normativa.

Las normas que a continuación se detallan serán de aplicación a la utilización de los elementos que conforman la red de comunicaciones, bien desde dependencias dentro de la propia Universidad, o bien desde cualquier otra ubicación que haga uso de la red de comunicaciones de la UEx y esté contemplada por la relación contractual del usuario con la Universidad, convenio de colaboración o proyecto o actividad institucional autorizado:

- Solo se podrán conectar a la red de comunicaciones cableada los ordenadores, estaciones de trabajo, servidores, periféricos y demás equipos de comunicaciones asignados para las funciones académicas o adquiridos con fondos finalistas para investigación, innovación y formación permanente, lo que se hará siguiendo los procedimientos establecidos por el SICUE.
- Se podrán conectar a la red de comunicaciones inalámbrica los equipos anteriormente citados, así como los ordenadores y dispositivos móviles de uso personal, quedando el usuario obligado a un uso responsable que no perjudique su correcto funcionamiento o modifique su configuración.
- Todos los usuarios de la red de comunicaciones tienen la obligación de cooperar activamente con el SICUE en las tareas de diagnóstico y resolución de las incidencias técnicas y de seguridad que se puedan producir.
- Todos los usuarios de la red de comunicaciones de la Universidad deberán cumplir también las

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	21/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





políticas de seguridad de la red de comunicaciones y todas las normas de uso de los servicios de la red de comunicaciones.

## 17 Uso del correo electrónico corporativo

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la UEx, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

Dada la importancia y uso de este recurso compartido, se ha desarrollado una norma específica para su uso: **NG02. Normas de uso del correo electrónico.**

## 18 Acceso a internet y otras herramientas de colaboración

El acceso corporativo a Internet es un recurso centralizado que la UEx pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

La UEx velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

### 18.1 Normas generales

- El acceso a Internet deberá ser autorizado por el SICUE, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.
- Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
- Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por la UEx en los puestos de usuario. No podrá alterarse la configuración del mismo, ni utilizar un navegador alternativo, sin la debida autorización del SICUE.
- Deberá notificarse al SICUE 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.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	22/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## 18.2 Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.
- La descarga de programas informáticos sin la autorización previa del SICUE 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.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- 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 SICUE.

## 19 Incidencias de seguridad

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la UEx o su imagen, deberá informar inmediatamente al SICUE, a través del CAU, que lo registrará debidamente y elevará, en su caso. Para la notificación del incidente se abrirá una incidencia en el **Centro de Atención al Usuario** de la UEx (<https://cau.unex.es>).

Si no fuese posible crear la incidencia en el CAU, se notificará en el teléfono de atención al usuario: 924 28 93 18 (extensión 89318).

## 20 Compromisos de los usuarios

Es responsabilidad directa del usuario:

- a) Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore el SICUE, para garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido
- b) En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa de la UEx establezca al respecto.
- c) Garantizar la disponibilidad de toda la información importante para la UEx alojada en el equipo del usuario -si no residiera en los servidores corporativos-, mediante la realización de

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	23/32
Url De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		







copias de seguridad periódicas.

Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de la UEx para desarrollar actividades que persigan o tengan como consecuencia:

- El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
- La degradación de los servicios.
- La destrucción o modificación no autorizada de la información, de manera premeditada.
- La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
- El deterioro intencionado del trabajo de otras personas.
- El uso de los sistemas de información para fines ajenos a los de la UEx, salvo aquellas excepciones que contempla la presente Normativa.
- Dañar intencionadamente los recursos informáticos de la UEx o de otras instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

## 21 Control de actuaciones sobre las bases de datos de la UEx

La UEx podrá habilitar Sistemas de Información cuyo acceso y/o modificación de la información contenida quedarán registrados en una Base de Datos, lo que permitirá su ulterior auditoría.

Las modificaciones de los datos deben realizarse sólo por parte de los usuarios autorizados y deberán estar siempre respaldadas por un expediente administrativo que justifique los cambios o la carga de ficheros de información suministrados y debidamente registrados en los registros de entrada/salida, de acuerdo con los procedimientos establecidos.

Se prohíbe realizar cualquier tipo de actualización en Bases de Datos corporativas, masiva o puntual, desde fuera de las aplicaciones de la UEx sin la autorización previa del SICUE.

## 22 Uso abusivo de los sistemas de información

El uso de Internet, del correo electrónico y el acceso al resto de los servicios y sistemas de la UEx estará debidamente controlado para todos los usuarios. Si se hiciese un uso abusivo o inapropiado de estos servicios, la UEx podrá adoptar las medidas disciplinarias que considere oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	24/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





Con carácter general, se enumeran seguidamente un conjunto de acciones que se consideran uso abusivo de los sistemas de información de la UEx:

## 22.1 Uso abusivo del acceso a internet

- Acceso a otras redes, con el propósito de violar su integridad o seguridad.
- Acceso a contenidos no relacionados con los cometidos profesionales del usuario, tales como:
  - Acceder, recuperar o visualizar textos o gráficos que excedan los límites de la ética.
  - Almacenar en la estación de trabajo del usuario o en los servidores de la UEx archivos personales (salvo autorización previa del SICUE).
  - Utilizar el acceso a Internet para el uso de mensajería instantánea (Messenger, Skype, etc.).
  - Transferencia de ficheros no relativa a las actividades profesionales del usuario (tales como juegos, ficheros de sonido, fotos, videos o películas, etc.).
  - Realizar cualquier actividad de promoción de intereses personales.
- Publicación o envío de información no solicitada.
- Publicación o envío de información sensible, confidencial, protegida o propiedad de la UEx, a personas, empresas o sistemas de información externos no autorizados. En este sentido, los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.
- Publicación o envío de mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del servicio de Internet de manera ilegal o infringiendo cualquier norma interna que pudiera resultar de aplicación.
- Empleo de utilidades de intercambio de información en Internet (tales como redes P2P).
- Uso de Internet para propósitos que puedan influir negativamente en la imagen de la UEx, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

## 22.2 Uso abusivo del correo electrónico

Estos aspectos se definen en la norma: **NG02. Normas de uso del correo electrónico.**

## 22.3 Uso abusivo de otros servicios y sistemas de la UEx

- Acceso a servicios y/o contenidos de la UEx con el propósito de violar su integridad o

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	25/32
Url De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





seguridad.

- De forma general, realizar actividades no relacionadas con las tareas profesionales del usuario, tales como:
  - Acceder, recuperar, o visualizar textos o gráficos que excedan los límites de la ética.
  - Almacenar archivos personales en la estación de trabajo o en los servidores de la UEx.
  - El uso de mensajería instantánea (Messenger, Skype, etc.).
  - Transferencia de ficheros entre usuarios de la UEx no relativa a las actividades profesionales.
  - Realizar cualquier actividad de promoción de intereses personales.
- Uso de cualquier servicio de la UEx para:
  - La publicación o envío de información no solicitada.
  - La publicación o envío de información confidencial, propiedad de la UEx, a personas, empresas o sistemas de información externos no autorizados. Los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.
  - El uso de los servicios de la UEx para propósitos que puedan influir negativamente en la imagen de la misma, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.
  - 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.
- Comunicación a terceros del contenido de cualquier dato reservado o confidencial propiedad de la UEx o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.

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

La UEx implantará los sistemas de protección de acceso a los sistemas que considere necesario, para evitar que se produzcan incidentes relacionados con el abuso de estos servicios.

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>	
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37	
<b>Observaciones</b>		<b>Página</b>	26/32	
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			



## 23 Monitorización y aplicación de esta normativa

La UEx, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente<sup>1</sup>:

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

La UEx llevará a cabo esta actividad de monitorización<sup>2</sup> de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El SICUE, con la colaboración de las restantes unidades de la UEx, velará por el cumplimiento de la presente Normativa General e informará al SICUE sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema

<sup>1</sup> En este sentido, el Artículo 24. Registro de actividad y detección de código dañino, del ENS (RD 311/2022, de 3 de mayo), señala: "Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa."

<sup>2</sup> Las actividades de monitorización a las que se refiere este apartado son puramente técnicas y se realizarán a nivel de los sistemas, y siempre cumpliendo con todas las normativas, reglamentos y recomendaciones oficiales relativas a la protección de los datos y en ningún caso se realizará ninguna actividad de acceso, intromisión o recopilación de información de carácter personal o privado.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	27/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar al SICUE sobre usos prolongados e indebidos del servicio.

## 24 Incumplimiento de la normativa

**Todos los usuarios de la UEx están obligados a cumplir lo prescrito en la presente Normativa General de Utilización de los Recursos y Sistemas de Información.**

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa General, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

## 25 Modelo de aceptación y compromiso de cumplimiento

Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la UEx deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa General de Utilización de los Recursos y Sistemas de Información, debiendo suscribirla.

Se propone el modelo que se recoge en el **Anexo III. Modelo de Aceptación y compromiso de cumplimiento; la presentación, recogida y almacenamiento de la aceptación y el compromiso de cumplimiento se implementará por medios electrónicos.**

## 26 Referencias

Esta Norma se apoya y se ve complementada por las siguientes referencias:

### Internas:

- PO.01 Política de Seguridad de la Información de la Universidad de Extremadura.
- NP.02 Normas De Uso Del Correo Electrónico.
- NP.40 Normas de Creación y uso de contraseñas.
- Otras por definir.

### Externas:

- [Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica \(ENS\).](#)
- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.

Código Seguro De Verificación	d4YDCpbzJbZJANjnAkiJ6Q==	Estado	Fecha y hora
Firmado Por	Juan María Hernández Núñez - Sede Vicerrector de Transformación Digital	Firmado	02/05/2024 12:46:37
Observaciones		Página	28/32
Uri De Verificación	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- [Guía de seguridad de las TIC CCN-STIC 821 Anexo I: Normativa General De Utilización De Los Recursos Y Sistemas De Información De La Entidad NG00.](#)

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	29/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





## ANEXO I. Protocolo de firma



### Anexo I. Protocolo de firma

He leído y comprendido las presentes Normas de Acceso y Permanencia en la universidad de Extremadura y acepto íntegramente su contenido, en los términos expresados, comprometiéndome a su cumplimiento.

En \_\_\_\_\_, a \_\_\_\_ de \_\_\_\_ de 20\_\_

<b>Empresa:</b>	
<b>Trabajador (Nombre y Apellidos):</b>	
<b>DNI:</b>	
<b>Firmado:</b>	

Enlace de la UEx: \_\_\_\_\_

DNI: \_\_\_\_\_

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	30/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		






## ANEXO II. Autorizaciones y habilitaciones

		Normativa General de Utilización de los Recursos y Sistemas de Información		
<b>Anexo II. Autorizaciones y Habilitaciones</b>				
<b>Horario de trabajo:</b>				
<b>Ubicación del puesto de trabajo:</b>				
Áreas con acceso físico autorizado				
		SI	NO	Observaciones
Planta 0	Zona 1			
	Zona 2			
	Zona 3			
Planta 1	Zona 1			
	Zona 2			
	Zona 3			
<b>Uso de teléfono:</b>				
<b>Uso del puesto de trabajo:</b>				
<b>Uso de ordenador portátil:</b>				
<b>Conexión a la red corporativa:</b>				
<b>Acceso a internet:</b>				
Servidores con acceso autorizado	Tipo 1			
	Tipo 2			
	Tipo 3			
<b>Acceso a control de versiones:</b>				
<b>Acceso a gestor documental:</b>				
<b>Acceso a carpetas de red:</b>				
<b>Otras:</b>				


<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	31/32
<b>Url De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		





	<p>Normativa General de Utilización de los Recursos y Sistemas de Información</p>	<p>Versión: 0.2  Código: NG.01  Fecha: 10/01/2024  Página 32 de 32</p>
---	---	--

## ANEXO III. Modelo de Aceptación y compromiso de cumplimiento

	<p>Normativa General de Utilización de los Recursos y Sistemas de Información</p> <p><b>Anexo III. Modelo de Aceptación y compromiso de cumplimiento</b></p>
<p>Mediante la cumplimentación de la siguiente declaración, el abajo firmante, personal de la UEx, como usuario de recursos informáticos y sistemas de información de la UEx, declara haber leído y comprendido la Normativa General de Utilización de los Recursos y Sistemas de Información de la UEx (versión 1) y se compromete, bajo su responsabilidad, a su cumplimiento.</p> <p>En _____, a ____ de ____ de 20__</p>	
<b>Organismo:</b>	
<b>Trabajador (Nombre y Apellidos):</b>	
<b>DNI:</b>	
<b>Número de registro de Personal:</b>	
<b>Firmado:</b>	
<p>Por la UEx: Nombre y apellidos: _____</p> <p>DNI: _____</p> <p>Número de Registro de Personal: _____</p>	

<b>Código Seguro De Verificación</b>	d4YDCpbzJbZJANjnAkiJ6Q==	<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Juan María Hernández Núñez - Sede Vicerrector de Transformacion Digital	Firmado	02/05/2024 12:46:37
<b>Observaciones</b>		<b>Página</b>	32/32
<b>Uri De Verificación</b>	<a href="https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==">https://uex09.unex.es/vfirma/code/d4YDCpbzJbZJANjnAkiJ6Q==</a>		
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

