III.- OTRAS DISPOSICIONES Y ACTOS

Universidad de Castilla-La Mancha

Resolución de 04/05/2018, de la Universidad de Castilla-La Mancha, por la que se publica la normativa de seguridad sobre la utilización de los sistemas de información y recursos informáticos de la Universidad de Castilla-La Mancha. [2018/5546]

El Consejo de Gobierno de la Universidad de Castilla-La Mancha, en su reunión del día 03 de mayo de 2018, aprobó la Normativa de Seguridad sobre la utilización de los sistemas de información y recursos informáticos de la Universidad de Castilla-La Mancha.

En su virtud,

Este Rectorado ha resuelto proceder a la publicación en el Diario Oficial de Castilla-La Mancha de la Normativa de Seguridad sobre la utilización de los sistemas de información y recursos informáticos de la Universidad de Castilla-La Mancha que figura en el Anexo.

Ciudad Real, 4 de mayo de 2018

El Rector
MIGUEL ÁNGEL COLLADO YURRITA

Anexo

Normativa de Seguridad sobre la utilización de los sistemas de información y recursos informáticos de la Universidad de Castilla-La Mancha.

ÍNDICE

Preámbulo

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece en su artículo 156.2 que el Esquema Nacional de Seguridad (ENS) tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de esta Ley, estando este constituido por los principios básicos y requisitos mínimos que permitan garantizar una adecuada protección de la información. Por tanto, la finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos.

Específicamente, en el artículo 1.2 del R.D. 3/2010, de 8 de enero, por el que se regula el ENS, se indica que este "será aplicado por las administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias". Así, en cumplimiento de lo establecido en el ENS, la Universidad de Castilla-La Mancha (UCLM) se dotaba en abril de 2015 de una *Política de Seguridad* que define un marco organizativo y operacional para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios prestados a través de medios electrónicos, creando las condiciones de confianza necesarias para que los miembros de la comunidad universitaria y los ciudadanos en general puedan ejercer sus derechos y cumplir sus deberes a través de estos medios.

En desarrollo de la mencionada Política, y conforme a lo dispuesto en el ENS, el presente documento constituye la *Normativa de Seguridad sobre la utilización de los sistemas de información y recursos informáticos de la Universidad de Castilla-La Mancha* mediante la que se establecen directrices generales y procedimientos para la protección y seguridad de los sistemas de información y recursos informáticos, y se señalan, asimismo, los compromisos que adquieren los usuarios respecto a la seguridad y buen uso de tales sistemas y recursos.

La UCLM considera que sus sistemas de información son un activo estratégico y elemento esencial para el cumplimiento de su misión académica y el ejercicio de los valores y principios que la inspiran, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las diferentes 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. Por un lado, servir de instrumento para alcanzar los objetivos que se marca la Universidad en la docencia, la investigación, la innovación y el resto de misiones universitarias. Por otro, facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión. Y todo ello proporcionando información completa, homogénea, actualizada, fiable y en el tiempo requerido.

Por ello, estos medios y recursos se ponen a disposición del personal docente e investigador (PDI), del personal investigador (PI), del personal de administración y servicios (PAS) y de nuestros estudiantes como instrumentos de trabajo para el desempeño de su actividad docente, investigadora, profesional y educativa, razón por la cual es necesario establecer las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

Así, en el Título I se recogen las disposiciones generales en materia de seguridad de los recursos informáticos y sistemas de información, fijando el ámbito objetivo y subjetivo de aplicación de esta normativa y las obligaciones y responsabilidades de los usuarios.

En el Título II se establecen las normas generales de uso de los recursos y sistemas de información de la UCLM y se especifican los usos concretos que se consideran no permitidos. Este Título se divide en cuatro capítulos que establecen normas específicas de uso del equipamiento para el puesto de trabajo, la red de comunicaciones, la mensajería electrónica corporativa y el acceso a internet.

El Título III está dividido en 4 capítulos. En el capítulo I se establecen una serie de normas, procedimientos y mecanismos encaminados a proteger la información, tanto en su forma electrónica como en su versión impresa, regulándose las autorizaciones que deben tener los usuarios para acceder a la información y la forma de proceder para la salida de información fuera de la Universidad. En el capítulo II, se protegen los derechos de las personas, tanto los relativos a los datos de carácter personal y la dignidad personal como el derecho de propiedad intelectual. El capítulo III está referido a la identificación de los usuarios para acceder a los sistemas de información y los recursos informáticos de la Universidad. Y, finalmente, el capítulo VI trata la aplicación y desarrollo de esta normativa y el procedimiento de comunicación de las incidencias y anomalías de seguridad que puedan comprometer el buen uso y funcionamiento de los sistemas de información de la Universidad o su imagen.

El texto contiene en su parte final un *Glosario de términos* para facilitar la comprensión del articulado.

Título I. Disposiciones generales

Capítulo I. Objeto y ámbito de aplicación

Artículo 1. Objeto

Esta normativa tiene por objeto la protección de los sistemas de información de la UCLM y los recursos informáticos que les dan soporte, garantizando la seguridad de los sistemas, los datos, las informaciones, las comunicaciones y los servicios prestados a los ciudadanos y a la comunidad universitaria.

Artículo 2. Ámbito objetivo de aplicación

La presente normativa es de aplicación a todas las actuaciones en materia de seguridad de la información y de los sistemas de información y de protección de datos personales en la UCLM, y su contenido se basa en las directrices de carácter general definidas en la *Política de Seguridad de la Información de la Universidad de Castilla-La Mancha*.

Artículo 3. Ámbito subjetivo de aplicación

Esta normativa es de aplicación a todos los miembros de la comunidad universitaria: estudiantes y empleados públicos, tanto PDI y PI como PAS. Asimismo, es de aplicación a los proveedores externos de servicios y a su personal, y a otras organizaciones públicas o privadas, entidades colaboradoras o entidades con algún tipo de vinculación con la UCLM cuando utilicen o tengan acceso a los sistemas de información de la Universidad.

Artículo 4. Conceptos y definiciones

A los efectos previstos en esta normativa, los conceptos y términos se han de entender en el sentido en que han sido definidos en el anexo I *Glosario de términos*.

Capítulo II. Responsabilidades de los usuarios

Artículo 5. Obligaciones y responsabilidades de los usuarios de los sistemas de información

1. Todo usuario que acceda a los servicios y sistemas de información de la UCLM estará obligado a:

a) Custodiar las **credenciales** que se le proporcionen y seguir todas las recomendaciones de seguridad que se elaboren, para garantizar que aquellas no puedan ser utilizadas por terceros.

b) Cerrar la **sesión** al terminar de usar su cuenta o bloquear el equipo cuando lo deje desatendido.

c) En el caso de que en su equipamiento almacene **información** clasificada o sensible, se deberán cumplir los requisitos legales aplicables y las medidas de protección que la normativa establezca al respecto, al menos el cifrado de la información y la activación de los registros de actividad.

2. Asimismo, no se podrán utilizar los recursos informáticos de la Universidad para el desarrollo de actividades que persigan o tengan como consecuencia:

a) El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones para usos no relacionados con la actividad académica o de gestión relacionada con el puesto de trabajo.

b) La degradación de los servicios.

c) La destrucción o modificación no autorizada de la información, de manera premeditada.

d) La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.

e) La vulneración de los derechos de propiedad intelectual.

f) El deterioro intencionado del trabajo de otras personas.

g) El uso de los sistemas de información para fines ajenos a los de la Universidad, salvo aquellas excepciones que contemple la presente Normativa.

h) Dañar intencionadamente los recursos informáticos de la Universidad o de otras instituciones.

i) Difundir contenidos contrarios a los principios enunciados en los Estatutos de la Universidad de Castilla-La Mancha.

j) Incurrir en cualquier otra actividad ilícita, del tipo que sea y, particularmente, difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatoria contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, el honor, la propia imagen o contra la dignidad de las personas.

3. Todos los usuarios están obligados a cumplir la presente normativa. En el supuesto de que un usuario no lo hiciera, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en

su caso, las responsabilidades legales correspondientes, el órgano de gobierno unipersonal con competencias en materia de seguridad o en tecnologías de la información y las comunicaciones (en adelante, el órgano competente), según corresponda, podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tuviera asignados.

Título II. Normas de uso de los recursos informáticos y usos específicamente no permitidos

Capítulo I. Uso del equipamiento informático

Artículo 6. Equipamiento para el puesto de trabajo utilizado por los empleados de la Universidad

1. La UCLM facilitará a sus profesores, investigadores y PAS el equipamiento para el puesto de trabajo y dispositivos de comunicaciones, tanto fijos como móviles, que necesiten para el desarrollo de su actividad profesional, de acuerdo a los programas y disponibilidades presupuestarias. Dicho equipamiento, así como los programas, aplicaciones, datos, dispositivos y demás recursos informáticos que tenga instalado, deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las funciones y competencias profesionales que tenga asignadas cada usuario.

2. Estos equipos informáticos se suministrarán debidamente configurados y con acceso a los servicios y aplicaciones corporativos necesarios para el desempeño de sus funciones y competencias profesionales, siendo los usuarios responsables de los usos que hagan de ellos.

3. Cuando finalice la relación que une al usuario con la Universidad o cambien las circunstancias profesionales que originaron la entrega del equipamiento, el usuario deberá devolverlo al Área de Tecnología y Comunicaciones (en adelante, A.TIC) o comunicar esta circunstancia de manera inmediata a través del Centro de Atención al Usuario para que el equipamiento sea retirado, al objeto de borrar de forma segura la información almacenada en él y restaurarlo a su estado original, y reutilizarlo, en su caso.

4. Las altas, bajas o modificaciones en el inventario de este equipamiento y la asignación de responsables se deberán incluir en el inventario de activos de la UCLM. Así mismo, se deberá actualizar el inventario patrimonial cuando así lo disponga la Normativa de Patrimonio.

Artículo 7. Normas generales de instalación, configuración y uso de este equipamiento

Las normas generales de instalación, configuración y uso son las siguientes:

a) Los equipos informáticos proporcionados por la Universidad serán instalados y configurados siguiendo los procedimientos establecidos por el A.TIC en aplicación de las políticas y medidas de seguridad que correspondan.

b) Los equipos informáticos serán asignados por la Gerencia o el órgano competente, en su caso. Existirá, además del inventario patrimonial gestionado por la Gerencia, un catálogo o inventario actualizado del equipamiento que será gestionado por el A.TIC.

c) Salvo aquellos ordenadores instalados en aulas de informática de libre uso, laboratorios de prácticas, salas de consulta de la Biblioteca, préstamos de equipos portátiles a estudiantes, puntos de información y los utilizados en las aulas como apoyo a la docencia o

conectados a equipos de video proyección, cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios serán responsables de su correcto uso, de acuerdo a lo establecido en los artículos siguientes.

d) Como norma general, los usuarios de equipos no destinados a tareas docentes o de investigación no tendrán privilegios de administración sobre los equipos, no pudiendo realizar modificaciones en el hardware o el software de los mismos.

e) Los equipos se configurarán por defecto con los mínimos privilegios que sean necesarios para el desarrollo de las funciones encomendadas a cada usuario, aplicándose las políticas o directivas de grupo del perfil de usuario al que este pertenezca.

Artículo 8. Usos no permitidos del equipamiento para el puesto de trabajo

No se permitirán los siguientes comportamientos:

a) Utilizar cualquier tipo de software dañino.

b) Utilizar programas que, por su naturaleza, hagan un uso abusivo de la red, esto es, que utilicen de manera intensiva los canales de comunicación para usos no profesionales, no justificados o que limiten el uso de otros usuarios.

c) Instalar software del que no se disponga de la licencia correspondiente o utilizar contenido que vulnere la legislación vigente en materia de propiedad intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas y legales aplicables.

d) Eliminar o deshabilitar las aplicaciones informáticas corporativas relacionadas con la seguridad instaladas en los equipos informáticos de la Universidad.

e) Alterar cualquiera de los componentes hardware o software de los equipos informáticos y dispositivos de comunicación referidos en el artículo 6. En todo caso, estas operaciones sólo podrán realizarse siguiendo los procedimientos establecidos por el A.TIC.

Artículo 9. Normas específicas para equipos portátiles y dispositivos móviles

1. Los equipos portátiles deberán almacenar la información cifrada y tener activado el registro de eventos del sistema. Lo mismo será aplicable al resto de dispositivos móviles, siempre que sea posible.

2. Estos equipos estarán bajo la custodia del usuario que los utilice, quien deberá adoptar las medidas necesarias para evitar daños o su sustracción, responsabilizándose del acceso a ellos o de su utilización por parte de personas ajenas a la Universidad o no autorizadas.

3. Quienes utilicen el equipamiento de la UCLM durante largos periodos fuera de la Universidad deberán realizar conexiones frecuentes a la red corporativa a través de una conexión de red privada virtual[1] (VPN), según las instrucciones proporcionadas por el A.TIC, para permitir la actualización de las aplicaciones, el sistema operativo, las firmas de virus y otras medidas de seguridad.

[1] Se pueden consultar las condiciones de uso del servicio de red privada virtual en el sitio https://area.tic.uclm.es/servicios/vpn.

4. En el supuesto de que un equipo sea sustraído, el incidente se habrá de poner inmediatamente en conocimiento del A.TIC a través del Centro de Atención al Usuario para la adopción de las medidas que correspondan, acompañando la correspondiente denuncia, en su caso.

Artículo 10. Instalación de software y hardware en el equipamiento para el puesto de trabajo

1. Para distribuir, instalar o desinstalar software y hardware o modificar la configuración del equipamiento del puesto de trabajo que gestione o maneje datos o sistemas de información de la Universidad se seguirán los procedimientos establecidos por el A.TIC.

2. En caso del equipamiento adquirido con fondos finalistas para investigación, innovación y formación permanente se deberá seguir también los procedimientos establecidos por el A.TIC en aquellos aspectos que puedan repercutir en la seguridad. No obstante, se podrán realizar otras configuraciones sobre dicho equipamiento siempre que se apliquen las medidas de seguridad mínimas equivalentes a las de dichos procedimientos, siendo sus usuarios responsables de la aplicación y eficacia de las mismas.

3. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para las tareas de instalación, mantenimiento o reparación. Este acceso se limitará únicamente a las acciones necesarias para llevar a cabo estas tareas y finalizará una vez terminadas.

4. El equipamiento para el puesto de trabajo deberá tener instaladas las actualizaciones de seguridad que los fabricantes de software vayan publicando para el sistema operativo y el resto de programas. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.

5. Los usuarios deberán notificar a través del Centro de Atención al Usuario cualquier incidencia que pueda afectar al funcionamiento del equipamiento que tengan asignado, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Los virus y programas maliciosos pueden propagarse con rapidez a través de dispositivos de almacenamiento portátil o de mensajes de correo electrónico, por lo que una rápida intervención del personal de soporte técnico puede evitar un incidente de mayor gravedad.

Capítulo II. Uso de la red de comunicaciones

Artículo 11. Normas generales de uso de la red de comunicaciones

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

2. 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 UCLM y esté contemplada por la relación contractual del usuario con la Universidad, convenio de colaboración o proyecto o actividad institucional autorizado:

a) 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 A.TIC.

b) 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.

c) Los usuarios de la red de comunicaciones tienen la obligación de cooperar activamente con el A.TIC en las tareas de diagnóstico y resolución de las incidencias técnicas y de seguridad que se puedan producir.

d) Los usuarios de la red de comunicaciones de la Universidad deberán cumplir también las políticas de seguridad de la red de comunicaciones y el resto de normas y condiciones de uso de los servicios de la red de comunicaciones.

Artículo 12. Usos no permitidos de la red de comunicaciones

Las siguientes actuaciones no serán permitidas:

a) Realizar actividades que pongan en peligro la disponibilidad, integridad o seguridad de la información que circula por la red de comunicaciones o se encuentre almacenada en bases de datos.

b) Conectar a la red de comunicaciones cualquier equipo o dispositivo no autorizado o inventariado en la Universidad, salvo que sean expresamente autorizados por el órgano competente.

c) Conectar aquellos equipos o dispositivos que modifiquen el diseño físico de la red o que interfieran en su correcto funcionamiento, tales como enrutadores, pasarelas, conmutadores de red o puntos de acceso inalámbrico, salvo que sean expresamente autorizados por el órgano competente.

d) Conectar a la red de comunicaciones equipos con direcciones IP no asignadas automáticamente por los servidores de asignación dinámica (DHCP), salvo autorización expresa del órgano competente.

e) Utilizar protocolos o puertos de red no permitidos por el A.TIC, salvo que se tenga previamente autorización para ser utilizados por el órgano competente.

f) Utilizar vulnerabilidades de la red de comunicaciones o de los sistemas de información de la Universidad que comprometan su seguridad, la disponibilidad de sus servicios o que permitan realizar cualquier ataque sobre estos servicios o los de otros organismos, instituciones o empresas.

g) Instalar, distribuir o ejecutar programas que permitan realizar cualquier ataque sobre la red de comunicaciones o los sistemas de información de la Universidad, o los de otros organismos, instituciones o empresas.

Capítulo III. Uso de la mensajería electrónica corporativa

Artículo 13. Normas generales de uso de la mensajería electrónica corporativa

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

2. Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos. Por ello, se dictan las siguientes normas generales de uso:

a) Todos los usuarios dispondrán de una cuenta de mensajería electrónica para el desempeño de su actividad de docencia, investigación, gestión o estudiantil que les permitirá el envío y recepción de mensajes. Las acciones realizadas desde esta cuenta son responsabilidad de su titular.

b) La instalación y configuración de las herramientas y programas de mensajería electrónica será realizada siguiendo los procedimientos establecidos por el A.TIC .

c) Los buzones de las cuentas de mensajería electrónica se configurarán con un tamaño para almacenamiento limitado, tamaño especificado en las condiciones de uso del servicio[2]. El sistema indicará cuándo se encuentra al límite de su capacidad, tras lo cual no se permitirá enviar ni recibir mensajes.

d) Se deberá notificar a través del Centro de Atención al Usuario cualquier tipo de anomalía detectada en relación a este servicio a fin de poner en marcha o configurar las medidas de seguridad oportunas.

e) Se deberá prestar especial atención a los ficheros adjuntos en los mensajes recibidos, no debiendo abrirse ni ejecutarse ficheros procedentes de emisores no fiables puesto que podrían contener virus o código malicioso.

f) Se deberá evitar responder a mensajes de los que se tengan sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.

g) Para la verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

Artículo 14. Usos no permitidos de la mensajería corporativa

Las siguientes actuaciones no estarán permitidas:

a) Enviar mensajes con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad o discapacidad o que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal.

b) Enviar mensajes que contengan programas informáticos sin licencia o ficheros adjuntos que vulneren los derechos de propiedad intelectual, con alerta de virus falsos o difusión de virus reales y código malicioso o, en general, la utilización de la mensajería electrónica infringiendo cualquier norma que pudiera resultar de aplicación.

c) Utilizar la mensajería electrónica para propósitos que puedan influir negativamente en la imagen de la Universidad, de sus representantes o de los organismos públicos o privados con los que esta mantiene relación.

d) Enviar información clasificada o sensible propiedad de la UCLM sin tener autorización del responsable de la información o de terceros, salvo que tal actuación fuera realizada en

[2] Se pueden consultar las condiciones de uso del servicio de correo en https://on.Universidad.es/condiciones.aspx.

cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.

e) Enviar mensajes que puedan provocar un mal funcionamiento o el colapso del sistema de mensajería electrónica o supongan un uso abusivo de los recursos. El envío de mensajes a un gran número de destinatarios se realizará a través de las listas de distribución de correo o herramientas de comunicación corporativas habilitadas a tal fin.

f) Acceder a un buzón de correo electrónico distinto del propio o del que no se esté autorizado para ello, así como suplantar la identidad de un usuario de mensajería electrónica o de cualquier otra herramienta colaborativa.

g) Utilizar el correo electrónico corporativo como medio de intercambio de ficheros especialmente voluminosos. El sistema evitará el intercambio de correos con ficheros adjuntos de tamaño superior al especificado en las condiciones de uso del servicio[3].

h) Utilizar el correo electrónico corporativo para trasladar publicidad o hacer llegar información no relacionada con la actividad profesional de forma masiva.

Artículo 15. Usos recomendados de la mensajería corporativa

La Universidad fomentará buenas prácticas en materia de mensajería corporativa con el fin de contribuir a la seguridad. En este caso, se considerarán buenas prácticas en el uso de la mensajería corporativa las siguientes:

a) Asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

b) Evitar, en la medida de lo posible, el uso ineficiente del servicio, agrupando los envíos a múltiples destinatarios en un solo mensaje y, en general, los envíos innecesarios.

c) No abrir ficheros adjuntos a los mensajes de correo de los que no se conozca su procedencia o que puedan considerarse sospechosos.

d) Transmitir ficheros muy voluminosos que, alternativamente, podrían compartirse a través de los espacios electrónicos institucionales.

Capítulo IV. Uso del acceso a internet

Artículo 16. Normas generales de uso del acceso a internet

1. El acceso a internet es un recurso corporativo que la UCLM pone a disposición de sus usuarios como herramienta para el desempeño de su actividad docente, investigadora, de gestión o estudiantil.

2. La Universidad velará por el buen funcionamiento de este recurso, tanto desde el punto de vista de la eficiencia como desde los riesgos de seguridad asociados a su uso. Por ello, se dictan las siguientes normas generales de uso:

[3] Se pueden consultar las condiciones de uso del servicio de correo en https://on.Universidad.es/condiciones.aspx.

a) Las conexiones que se realicen a internet deben obedecer a fines legítimos y para el desempeño de las tareas que cada usuario tenga asignadas.

b) Cualquier anomalía detectada en el uso del acceso a internet deberá notificarse a través del Centro de Atención al Usuario, así como la sospecha de posibles problemas o incidencias de seguridad relacionados con dicho acceso.

Artículo 17. Usos no permitidos en el acceso a internet

No se permitirán las siguientes actuaciones:

a) La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para los sistemas de información de la Universidad.

b) El acceso a recursos y páginas web o la descarga de programas o contenidos que vulneren la legislación en materia de propiedad intelectual.

c) El uso de internet para violar la integridad y seguridad de la red y los servicios y sistemas de información de la Universidad o el de instituciones, empresas o particulares.

d) El uso de internet para fines personales relacionados con la descarga de archivos y la ejecución de programas en línea que utilicen recursos de red de forma abusiva o cuando de dicho uso se pueda producir un perjuicio para el correcto funcionamiento de los servicios.

e) El uso de internet para propósitos que puedan influir negativamente en la imagen de la Universidad, de sus representantes o de los organismos públicos o privados con los que se mantiene relación y, en general, infringiendo cualquier norma que pudiera resultar de aplicación.

Artículo 18. Uso abusivo del acceso a internet y de los servicios y sistemas de la Universidad

1. La Universidad controlará el uso abusivo del acceso a internet y a sus servicios y sistemas. Si se hiciese un uso abusivo de estos, se adoptarán las medidas disciplinarias y administrativas que se consideren oportunas, sin perjuicio de las acciones legales a las que hubiere lugar.

2. La Universidad implantará los sistemas de protección de acceso a los sistemas que considere necesarios para evitar que se produzcan incidentes relacionados con el abuso de sus servicios y sistemas de información.

Título III. Protección y seguridad de la información

Capítulo I. Protección de la información

Artículo 19. Acceso a los sistemas de información y a los datos

1. Los datos gestionados por la Universidad y tratados en cualquier sistema de información deben tener asignado un responsable que será el encargado de conceder, modificar o anular la autorización de acceso a dichos datos por los usuarios, de acuerdo a la normativa en materia de protección de datos, en su caso.

2. El responsable funcional o el responsable del sistema de información autorizará a través del Centro de Atención al Usuario o de la aplicación correspondiente el alta de los usuarios que deban acceder al sistema de información. La autorización de acceso establecerá el perfil con el que se materializan las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos. Así, los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones.

3. La baja de los usuarios será comunicada a través del Centro de Atención al Usuario o se realizará utilizando la aplicación correspondiente por su responsable funcional o por el responsable del sistema de información al que tuviera acceso, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

4. Cuando un usuario deje de atender el ordenador durante un cierto tiempo, será necesario bloquear la sesión de usuario para evitar que otra persona no autorizada pueda acceder al sistema de información y a los datos. Así, y en general, los ordenadores de los usuarios que deban acceder a los sistemas de información de la Universidad se bloquearán automáticamente tras un periodo de inactividad de 10 minutos.

5. Así mismo, los usuarios deberán adoptar las medidas de seguridad necesarias para salvaguardar la información clasificada o sensible almacenada en soportes de información o dispositivos de almacenamiento extraíble frente a posibles revelaciones o accesos no autorizados de terceros.

Artículo 20. Control de las actuaciones sobre la información y los datos

1. La Universidad podrá habilitar mecanismos para registrar el acceso o modificación de la información contenida en los sistemas de información, lo que permitirá su ulterior auditoría.

2. Se prohíbe realizar cualquier tipo de actualización en la información contenida en los sistemas de información, de forma masiva o puntual, desde fuera de las aplicaciones corporativas sin la autorización previa de su responsable.

3. Las modificaciones de los datos que se hagan fuera de las aplicaciones corporativas deben realizarse solo por parte de los usuarios autorizados y deberán estar siempre autorizadas por el responsable de la información o de la base de datos cuyos datos vayan a ser modificados, y se realizará de acuerdo con los procedimientos establecidos.

Artículo 21. Confidencialidad de la información

1. La información propiedad de la Universidad y contenida en sus sistemas de información es considerada como confidencial, por lo que los usuarios deben abstenerse de comunicarla, divulgarla, distribuirla o ponerla en conocimiento por cualquier medio de terceras personas no autorizadas, ya sean usuarios internos o externos. Como medida de protección de la información propia, y de la que sea propiedad de terceros y que haya sido confiada o sea tratada por la Universidad, solo podrá ser enviada al exterior a través de las redes de comunicaciones, en soportes informáticos o en soporte papel, si su salida ha sido previamente autorizada por el responsable de la misma.

2. Todo el personal que por razón de su actividad profesional tenga acceso a información gestionada por la Universidad deberán mantener sobre ella el debido secreto profesional por tiempo indefinido, salvo que dicha información sea de libre acceso.

3. El personal ajeno a la Universidad que, como consecuencia de la prestación de un servicio, deba tener acceso a información en cualquier tipo de soporte, será estrictamente por el tiempo necesario para la prestación del servicio encomendado, con la obligación de mantener secreto profesional indefinido sobre la información a la que haya accedido, salvo que dicha información sea de libre acceso. En el supuesto de que hubiera sido necesario la utilización de soportes de información, se deberán devolver inmediatamente después de la finalización de las tareas que hubieren originado su uso.

4. 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.

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

6. 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.

7. Se evitará almacenar información clasificada o sensible en medios desatendidos tales como CDs, DVDs, memorias USB, listados impresos o dejar visible tal información en la pantalla del ordenador.

8. Los datos personales tratados en la UCLM tendrán específicamente el carácter de datos protegidos y sobre ellos, además de lo indicado en los párrafos anteriores, se deberán observar las normas y procedimientos de seguridad que se establecen en esta Normativa, en el *Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha*[4] y en el *Documento de seguridad para ficheros con datos de carácter personal en la Universidad de Castilla-La Mancha*.

Artículo 22. Tratamiento de la información

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

2. Cualquier tratamiento en los sistemas de información deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la de protección de datos.

3. No se podrá comunicar o ceder información clasificada o sensible a personas, empresas o sistemas de información externos no autorizados, ni la comunicación o cesión de datos de carácter personal a terceros, salvo que tal actuación fuera realizada con la previa autorización del responsable del fichero y con el previo consentimiento de los interesados, cuando así fuera necesario.

4. Queda prohibido, asimismo, transmitir o alojar información clasificada o sensible propia de la Universidad en servidores externos salvo autorización expresa del responsable de la información, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la Universidad y la empresa responsable de la prestación del servicio, incluyendo los

[4] Ambos documentos están disponibles en la intranet: http://intranet.uclm.es/psi/

acuerdos de nivel de servicio que procedan, el correspondiente acuerdo de confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

Artículo 23. Salidas de información

1. La salida de información relacionada con los procesos de gestión de la Universidad, en cualquier soporte o por cualquier medio de comunicación, deberá ser realizada exclusivamente por personal autorizado, autorización que contemplará igualmente a la propia información que sale.

2. La salida de datos clasificados o sensibles 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 y en el Código de conducta y Documento de seguridad de la Universidad.

3. Los usuarios se abstendrán de sacar al exterior cualquier información en cualquier dispositivo: CDs, DVDs, memorias USB, ordenadores u otros dispositivos portátiles, salvo lo indicado en los dos párrafos anteriores.

Artículo 24. Copias de seguridad

1. La información y los datos deben ser protegidos de posibles daños o pérdidas, por lo que realizar copias de seguridad es una medida esencial para su protección. En este caso, se recomienda a los usuarios guardar las copias de seguridad que puedan realizar alejadas de los datos originales.

2. Los datos tratados y generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en los espacios compartidos de trabajo, lo que permitirá que sean protegidos por las medidas y mecanismos de seguridad institucionales.

3. Los servicios TIC de la Universidad en ningún caso realizarán copias de seguridad de la información almacenada de forma local en el puesto de trabajo del usuario, quien podrá hacer uso para ello del almacenamiento personal en la nube que proporciona la UCLM.

4. La información almacenada en las copias de seguridad institucionales y de una antigüedad no superior a 12 meses podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de solicitarlo a través del Centro de Atención al Usuario.

Artículo 25. Tratamiento de la documentación en papel en impresoras, fotocopiadoras y escáneres

1. La impresión de documentos con información clasificada o sensible se realizará a través del sistema de impresión corporativo, que garantiza que los documentos solo estarán accesibles para quién los envió a imprimir, dado que el sistema requiere de la previa identificación del usuario.

2. En la impresión de documentos en impresoras compartidas se deberá asegurar que se han recogido todas las hojas impresas y que estas no quedan en las bandejas de la impresora, para evitar que terceras personas puedan acceder a la misma. De igual modo, se deberá recoger y no dejar olvidado el documento original que se haya fotocopiado o digitalizado, una vez finalizado el proceso de copia o digitalización.

3. Si se encontrase documentación clasificada o sensible abandonada en una impresora, fotocopiadora o escáner, salvo que el usuario conozca y pueda localizar a su propietario para

avisarle de que la recoja, pondrá este hecho inmediatamente en conocimiento a través del Centro de Atención al Usuario.

Artículo 26. Cuidado y protección de las copias impresas

1. Las copias impresas que contengan datos clasificados o sensibles deben ser especialmente resguardadas, de forma que solo tenga acceso a ellas el personal autorizado, y custodiada en armarios bajo llave, impidiendo que puedan quedar accesibles a personas no autorizadas.

2. Cuando concluya la vida útil de las copias impresas con información clasificada o sensible, deberán ser eliminadas en las máquinas destructoras, de forma que no sea recuperable la información que pudieran contener.

Capítulo II. Protección de los derechos relativos a las personas

Artículo 27. Protección de datos de carácter personal

1. La información contenida en los sistemas de información de la Universidad que comprenda datos de carácter personal estará protegida conforme a la normativa vigente en esta materia, en especial por lo establecido en el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como por las normas de la Universidad en esta materia.

2. Sobre los ficheros o tratamientos de datos de carácter personal gestionados por la Universidad se adoptarán las medidas técnicas y organizativas que garanticen su seguridad.

3. Todo usuario de la Universidad 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 Universidad.

Artículo 28. 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 el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Artículo 29. Protección de la propiedad intelectual

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

2. Los programas informáticos propiedad de la Universidad o licenciados a la Universidad 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 se tenga la autorización previa del órgano competente.

3. 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.

Capítulo III. Identificación y acceso a los sistemas de información

Artículo 30. Identificación y acceso de los usuarios de la universidad a los sistemas de información

1. La UCLM facilitará a su personal y sus estudiantes, para el acceso a los sistemas de información y los recursos informáticos para los que estén autorizados y precisen para el desarrollo de sus actividades de docencia, investigación, gestión y estudiantil, unas credenciales de usuario, formadas por un identificador de usuario y una contraseña, que serán intransferibles y únicas para cada persona en la organización. El usuario será responsable de su custodia y de toda actividad relacionada con su uso y con los accesos que se realicen con ella a los sistemas de información de la Universidad. Una utilización de las credenciales de usuario contraria a lo establecido en esta Normativa supondrá la desactivación de las mismas.

2. La creación de las credenciales para los nuevos usuarios requerirá que estos proporcionen la siguiente información:

a) Nombre, apellidos y NIF (o documento de identidad equivalente).

b) Nº de teléfono móvil y dirección alternativa a la de la Universidad de correo electrónico, que serán utilizados para la recuperación de las credenciales en caso necesario.

c) Colectivo de usuario al que pertenece: PDI, PI, PAS, Personal de Investigador en Formación, Estudiante, etc.

d) Campus universitario y centro al que pertenece.

e) Servicios y aplicaciones a los que necesita acceder.

3. Los usuarios no deberán revelar o ceder, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. Si un usuario tuviera sospechas de que sus credenciales están siendo utilizadas por otra persona, deberá comunicar inmediatamente esta incidencia de seguridad a través del Centro de Atención al Usuario. Los usuarios no utilizarán nunca las credenciales de otra persona, aunque dispongan de su consentimiento.

4. La Universidad podrá habilitar la autenticación en sus sistemas de información mediante el uso de un certificado digital o del DNI electrónico. A los certificados digitales se les aplicarán las mismas prevenciones que a las contraseñas sobre su custodia y no revelación de información relativa a las claves que protegen su utilización.

5. Las normas sobre las contraseñas y sus recomendaciones de uso estarán incluidas en la **Política de contraseñas**[5] de la Universidad, validada por la *Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad de la Información* y aprobada por el Consejo de Dirección.

[5] Disponible en la intranet: https://intranet.uclm.es/psi/

Artículo 31. Identificación y acceso de terceros a los sistemas de información de la Universidad

Los terceros ajenos a la Universidad que, eventualmente, tengan que acceder a los sistemas de información, deberán observar las siguientes normas:

a) El personal ajeno que temporalmente deba acceder a los sistemas de información de la Universidad deberá hacerlo siempre bajo la supervisión de algún miembro acreditado del A.TIC, que actuará como su interlocutor dándole asesoramiento, atendiendo sus consultas o necesidades, transmitiéndole instrucciones y poniéndole al corriente de sus cometidos.

b) Para los accesos de terceros a los sistemas de información, siempre que sea posible, se crearán usuarios temporales que serán eliminados una vez concluido su trabajo en la Universidad. 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.

c) Cualquier incidencia que surja antes o en el transcurso del acceso deberán ponerla en conocimiento del miembro del A.TIC responsable de la coordinación o supervisión y que hace de interlocutor.

d) Tales personas, en lo que les sea de aplicación, deberán cumplir la presente Normativa, así como el resto de normativa de la Universidad, especialmente en lo referente a los apartados de salida y confidencialidad de la información.

Capítulo IV. Aplicación y desarrollo de esta normativa

Artículo 32. Aplicación de esta normativa y seguimiento de su aplicación

1. La UCLM, 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. Se 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. 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 a criterio del órgano competente, sin perjuicio del derecho del usuario a realizar las alegaciones que a su derecho convengan y en plazo que, a ese efecto, se habilite en la notificación de esa medida cautelar. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El A.TIC velará por el cumplimiento de la presente Normativa e informará al Comité de Seguridad y

al órgano competente sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

4. El sistema que proporciona el servicio de mensajería electrónica 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 o de las condiciones de uso del servicio. 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 mensajes.

5. El sistema que proporciona el servicio de acceso a internet podrá contar con filtros que bloqueen el acceso a páginas web potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema 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.

Artículo 33. Incidencias de seguridad

1. 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 Universidad o su imagen, deberá informar inmediatamente de estas circunstancias a través del Centro de Atención al Usuario, donde la incidencia quedará debidamente registrada.

2. Entre otros sucesos, tendrán la consideración de incidencias de seguridad:

a) Pérdida de la contraseña de acceso a los sistemas de información o uso indebido de la misma.

b) Acceso no autorizado a información o datos excediendo los perfiles de usuario.

c) Pérdida de soportes informáticos con datos de carácter personal o información clasificada, o que dicha perdida pueda afectar a la seguridad de los sistemas de información.

d) Pérdida de datos por mal uso de las aplicaciones.

e) Ataques a la red, fallo o caída de los sistemas de información.

f) Infección de los sistemas de información por virus u otros elementos dañinos.

Artículo 34. Desarrollo de la Normativa

Para la implementación de la Normativa de Seguridad, la UCLM, a través del *Comité de Seguridad* y con el informe de la *Comisión de Tecnologías de la Información, Comunicaciones y Seguridad Informática* y la asesoría del A.TIC, desarrollará y dictará las normas técnicas necesarias, entre las que se encontrarán, al menos, las siguientes:

- Política de contraseñas
- Uso de la red de comunicaciones
- Normas sobre la gestión de las copias de seguridad
- Normas de clasificación de la información

Disposiciones adicionales

Disposición adicional primera. Consideraciones lingüísticas

Todas las denominaciones contenidas en este Reglamento referidas a órganos unipersonales de gobierno y representación y miembros de estos se entenderán realizadas y se utilizarán indistintamente en género masculino y femenino, según el sexo del titular que los desempeñe.

Disposición adicional segunda. Habilitación interpretativa

Se habilita al órgano colegiado unipersonal con competencias en materia de seguridad para la interpretación y resolución de cuantas cuestiones se planteen en la aplicación de esta Normativa.

Disposición final

Disposición final única. Entrada en vigor

Esta normativa se publicará en el Boletín Oficial de la Universidad y en el Diario Oficial de Castilla-La Mancha, y entrará en vigor al día siguiente de su publicación en el DOCLM.

Anexo I. Glosario de términos

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Amenaza. Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Antivirus. Programa o aplicación informática capaz de detectar y eliminar virus y demás códigos o programas maliciosos, también conocido como como malware.

Aplicación informática. Programa informático diseñado como herramienta para permitir a un usuario realizar una o varias funciones o tareas.

Auditoría de seguridad. Revisión y examen de los registros de eventos y actividades del sistema para verificar la idoneidad de los controles de seguridad del sistema y para identificar, enumerar y describir las diversas vulnerabilidades que pudieran detectarse.

Autenticación. Procedimiento de comprobación de la identidad del usuario.

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que provienen los datos.

Cifrar información. Proceso por el que se transforma una información legible en otra ininteligible usando un procedimiento y una clave determinados, y que solo quien conozca dicho procedimiento y clave puede acceder a la información original.

Código malicioso. Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. También conocido como código dañino o malware.

Comité de Seguridad de la Información. Es el órgano responsable de impulsar y revisar la política de seguridad y sus normas de desarrollo en el marco del ENS.

Comisión de Tecnologías de la Información y las Comunicaciones y de Seguridad Informática. Es una comisión dependiente del Consejo de Gobierno que asesora en materia de seguridad informática, de objetivos estratégicos en TIC y de divulgación en estos ámbitos.

Confidencialidad. Propiedad o característica consistente en que la información se mantiene inaccesible y no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Conmutador de red. Dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local.

Contraseña. Información confidencial, a menudo compuesta de una cadena de caracteres, que puede ser usada en la autenticación de un usuario, entidad o recurso.

Copia de seguridad. Copia duplicada de datos que se realiza con el fin de archivarlos o protegerlos de daños o pérdidas, y que permite recuperarlos en caso necesario.

Cortafuegos. Dispositivo físico o lógico que permite inspeccionar las comunicaciones entre redes de datos y en función de un conjunto de reglas permitir o denegar el tráfico de datos.

Credencial de usuario. Combinación del identificador de usuario y del factor o factores utilizados para autenticar al usuario, generalmente una contraseña.

Cuenta de usuario. Conjunto de los permisos y configuraciones que tiene el usuario para acceder a un equipo informático (cuenta de equipo), un sistema de información (cuenta de aplicación), una red de comunicaciones (cuenta de red), etc.

Dato de carácter personal. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Degradación del servicio. Pérdida de calidad o rendimiento de un servicio que se presta al usuario, pudiendo llegar a no ser posible su prestación.

DHCP. *Dynamic Host Configuration Protocol* o protocolo de configuración dinámica de *host*. Es un servidor que posee una lista de direcciones IP dinámicas y las va asignando a los clientes (equipos) conforme éstas van quedando libres, conociéndose en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Dimensiones de seguridad. Cada uno de los aspectos de seguridad de la información que debe ser protegido y que pueden verse afectado por un incidente de seguridad. El Esquema Nacional de Seguridad establece cinco dimensiones de seguridad: disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

Dirección IP. Número que identifica de manera lógica y jerárquica a una conexión de red de un dispositivo (ordenador, tableta, portátil, teléfono inteligente, etc.) que utilice el protocolo IP (*Internet Protocol* o Protocolo de Internet).

Disponibilidad. Propiedad o característica de los componentes o funcionalidades de un sistema de información consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Dato. Valor o representación simbólica dispuesta de manera adecuada para su tratamiento por un ordenador. Un dato por sí mismo no constituye información, es el procesamiento de los datos lo que proporciona la información.

Enrutador. También conocido como *router* o encaminador, es un dispositivo cuya función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de ordenadores con direcciones IP del mismo rango que se pueden comunicar sin la intervención de un enrutador, sino mediante un conmutador de red.

Estación de trabajo. Ordenador de altas prestaciones destinado para trabajo técnico o científico.

Fichero con datos personales. Conjunto organizado de datos de carácter personal, cualquiera que sea su forma o modalidad de creación, almacenamiento, organización y acceso.

Firma de virus. Pequeña muestra o parte de un virus que lo identifica y define de forma inequívoca, y que es utilizada por el programa antivirus para detectar software malicioso. Para que el antivirus pueda detectar un virus es necesario que la base de datos del antivirus esté actualizada con la firma del virus, esto es, que se conozca su firma.

Hardware. Componentes físicos de un equipo informático.

Identificación. Procedimiento de reconocimiento de la identidad de un usuario.

Identificador de usuario. Generalmente es una cadena de caracteres que identifica a un usuario de manera única y singular, distinguiéndolo del resto de usuarios.

Incidencia de seguridad. Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

Incidente de seguridad. Acceso, uso, divulgación, modificación o destrucción no autorizada de información; suceso que impide el normal funcionamiento de las redes, los sistemas o los recursos informáticos.

Información. Elemento de conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

Información clasificada. Cualquier información que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad. En España, la información puede estar clasificada como *secreta*, *reservada*, *confidencial* y de *difusión limitada* en función del perjuicio que puede ocasionar su difusión no autorizada.

Información sensible. Información, en especial la de carácter personal, que no debe ser puesta a disposición ni revela a individuos, entidades o procesos no autorizados.

Integridad. Propiedad o característica consistente en mantener la información como fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Lista de distribución de correo. Herramienta de difusión de información basada en el correo electrónico, mediante la que se envía de forma simultánea un mensaje de correo electrónico a varios usuarios a la vez, en lugar de enviar un mensaje individual a cada uno de ellos. En una lista de distribución de correo, el mensaje se envía a la dirección de la lista, y es esta quien se encarga de hacerlo llegar a la dirección de todas las personas inscritas en ella.

Mensajería electrónica. Sistema de intercambio de mensajes de manera electrónica entre ordenadores. Forman parte de la mensajería electrónica el correo electrónico y la mensajería instantánea o comunicación en tiempo real a través de mensajes de texto.

Pasarela. En una red, el punto de acceso a otra red. Interfaz que conecta dos o más redes que tienen funciones similares, pero implementaciones diferentes.

Política de Seguridad de la Información de la UCLM. Marco organizativo y operacional orientado a facilitar y garantizar la seguridad de los sistemas, los datos y los servicios prestados a través de

medios electrónicos y a crear las condiciones de confianza necesarias para el ejercicio de los derechos y deberes de los miembros de la comunidad universitaria mediante dichos medios.

Punto de acceso inalámbrico o *wifi*. Dispositivo de interconexión utilizado para conectar a una red física equipos de forma inalámbrica.

Programa informático. Secuencia de instrucciones y comandos escritos en código para realizar una tarea concreta en un ordenador.

Programa malicioso. Virus, software dañino o *malware*.

Propiedad intelectual. Derechos de carácter personal y patrimonial que tiene el autor de una obra literaria, artística o científica y que le atribuyen su plena disposición y el derecho exclusivo a su explotación, sin más limitaciones que las establecidas en la Ley.

Protocolo de red. Conjunto de reglas que rigen el intercambio de información a través de una red de ordenadores.

Puerto de red. interfaz a través de la cual se comunican los programas informáticos en una red.

Red de comunicaciones. Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Red privada virtual. También conocida por sus siglas VPN (*Virtual Private Network*), es una clase de red que se configura dentro de una red pública como mecanismo para establecer una comunicación segura entre los extremos. La integridad y confidencialidad de la información que circula por esta red privada virtual se garantiza mediante su cifrado.

Registro de eventos del sistema. Registro de la actividad del sistema, las aplicaciones y los accesos de los usuarios. Se registra información sobre quién, qué, cuándo, dónde y por qué ocurre un evento, el tiempo de conexión de los usuarios, los servicios utilizados, los datos accedidos, etc. También se utiliza el término inglés *System Logs* para referirse al registro de eventos del sistema.

Responsable del fichero con datos de carácter personal. Persona que toma la decisión sobre la finalidad, el uso y el contenido del tratamiento que se da a los datos de carácter personal y autoriza el acceso de los usuarios al fichero y las cesiones o comunicaciones de los datos.

Responsable de la información. Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable del sistema de información. Persona que toma la decisión sobre la explotación del sistema de información y concede, modifica o anula la autorización de acceso a los usuarios.

Responsable funcional. Persona que autoriza, modifica y revoca los permisos de acceso a una aplicación en un ámbito funcional determinado.

Riesgo de seguridad. Posibilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización.

Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición de personas, presentar o transmitir.

Software. Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Software dañino. Virus, código malicioso o *malware*.

Soporte de información. Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Tratamiento de datos. Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Virus. Programa que está diseñado para replicarse a sí mismo con la intención de infectar a otros programas o ficheros.

Vulnerabilidad. Debilidad de seguridad de un sistema que le hace susceptible de poder ser dañado al ser aprovechada por una amenaza. Es decir, es un defecto de diseño, fallo de configuración, error de programación, etc. que puede permitir a un atacante tener acceso no autorizado a la red de comunicaciones de una organización y a sus sistemas de información.