UNIVERSIDAD DE ALMERÍA
Secretaría General

Fecha: 03 de junio de 2019

Unidad Origen: Secretaría General

Asunto: *Petición de inclusión de asunto en el orden del día del Consejo de Gobierno*

Unidades de destino: Secretaría General de la UAL

Por orden del Sr. Rector se procede a incluir en el orden del día del próximo Consejo de Gobierno un punto con el siguiente enunciado:

Aprobación, si procede, de las Normas de Uso de los Sistemas de Información de la Universidad, de acuerdo al ENS, al RGPD y a la LOPDyGDD, aprobadas por la Comisión de Seguridad Informática y Protección de Datos de la UAL, para su elevación al Consejo de Gobierno.

y cuya propuesta de acuerdo sería:

Se aprueban las Normas de Uso de los Sistemas de Información de la Universidad, de acuerdo al ENS, al RGPD y a la LOPDyGDD, aprobadas por la Comisión de Seguridad Informática y Protección de Datos de la UAL, para su elevación al Consejo de Gobierno.

[Firmado Digitalmente]

Universidad de Almería
Carretera Sacramento s/n
04120, La Cañada de San Urbano, Almería
www.ual.es

Secretaría General
Edificio de Gobierno y Paraninfo
Planta Tercera, Despacho 3.170

UNIVERSIDAD DE ALMERÍA

COMISIÓN DE SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS

Normas de uso de los sistemas de información de la UAL

Autor	Comisión de Seguridad Informática y Protección de Datos
Destinatario	Usuarios de los sistemas de información de la UAL
Fecha creación	
Fecha última modificación	
Fecha aprobación	
Aprobado por	Comisión de Seguridad Informática y Protección de Datos

Registro de ediciones

Versión	Fecha	Partes que cambian	Descripción de los cambios
1.0	21/06/2010		Documento inicial
1.1	14/02/2019		Adaptación a nuevos servicios y a la nueva legislación sobre protección de datos personales
1.2	21/02/2019	Organización índice	Mejor clarificación de la normativa
1.3	01/03/2019		Se incorporan los comentarios de Govertis y se incluyen las formas de contacto con el STIC y con la Comisión de Seguridad.
1.4	04/03/2019		Algunos errores y mejoras.
1.5	07/03/2019		Se incorpora comentario sobre correo electrónico y mejora a realizar, dentro del apartado 5.1 Correo Electrónico
1.6	31/05/2019		Aprobado Comisión Seguridad para elevar CG

Índice

1. Introducción

El marco normativo en protección de datos y seguridad informática actualmente está regulado por:

- 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 (en adelante RGPD)

- Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantías de Derechos Digitales (en adelante LOPDyGDD)

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica para las Administraciones Públicas (en adelante ENS)

- Real Decreto 951/2015, de 23 de octubre, de modificación del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

- Documentos de la Administración en Materia de Seguridad Electrónica: Criterios de Seguridad, Normalización y Conservación.

- Instrucciones Técnicas (Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad).

- Las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones.

Este amplio marco normativo pretende fortalecer al administrado frente a la Administración, a la vez que obliga a ésta, a jugar un papel activo y actualizado en materias como la protección de datos de carácter personal, así como garantizar y consagrar unos servicios públicos seguros, garantizando la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos que permitan a ambos sujetos, el ejercicio de derechos y el cumplimiento de deberes.

El ENS persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con sistemas de información del sector privado. De esta manera la seguridad debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse

efectivamente para evitar “tierras de nadie” y fracturas que pudieran dañar a la información o los servicios que presta la Administración.

A su vez, el RGPD y la reciente LOPDyGDD, además de empoderar al administrado frente a la Administración, han venido a cambiar el paradigma en la protección de datos y la seguridad, obligando a ésta, a mantener una responsabilidad proactiva. Este principio de accountability o de responsabilidad proactiva es un nuevo concepto fundamental, que deben comprender las administraciones públicas y transmitir a todos los niveles.

Además, las administraciones públicas deben cumplir con el conjunto de obligaciones establecidas en el RGPD y ser capaces de demostrar que se está cumpliendo. Para ello, el responsable del tratamiento, deberá aplicar las medidas técnicas y organizativas apropiadas para poder garantizar y demostrar que los tratamientos que realiza son conformes con el RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas.

Para fundamentar la confianza en los sistemas de información, además de cumplir con la responsabilidad proactiva que se nos está demandando, están las auditorías sobre los distintos sistemas de información, que nos van a permitir profundizar en los detalles del sistema y evidenciar las fortalezas y debilidades del mismo, utilizando los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a las auditorías de sistemas de información.

Según la Política de Seguridad de la Universidad de Almería, aprobada en fecha 18/06/2018 por el Consejo de Gobierno, las funciones que según el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero) corresponden al “Comité de Gestión del ENS” son asumidas en la UAL por la Comisión de Seguridad Informática y Protección de Datos, en adelante Comisión de Seguridad.

Una de las funciones que asume por tanto la Comisión de Seguridad es la “Aprobación de la normativa de seguridad de la Organización”. La Comisión de Seguridad procede aprobar esta Política de Uso de Los Sistemas de Información cuyo objetivo, alineado con la legislación anteriormente descrita, se define seguidamente.

2. Objetivos del documento

La seguridad siempre ha sido un concepto presente en todos los sistemas de gestión de la información. Su implementación no es sencilla, porque abarca todos los eslabones de la cadena de gestión de la información y requiere de un gran conjunto de medidas organizativas y tecnológicas.

El éxito de su implantación depende además de que exista en todos los niveles de la Administración una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el Usuario final del sistema (informático y papel).

El Usuario final necesita, por tanto, ser concienciado en materia de seguridad de la información y al mismo tiempo debe disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos a su alcance, así como soportes o documentos en papel. Y, con especial relevancia, en cuanto a preservar la confidencialidad de la información de carácter personal que esté siendo tratada, como son los datos personales proporcionados por los promotores de quejas o de los que dirigen consultas a la institución.

El presente documento establece así, las normas de uso del ordenador asignado al puesto de trabajo, de la red corporativa, de equipos portátiles, de las aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, a nivel informático y en papel.

Es fundamental que todos los usuarios de la Universidad de Almería que utilizan equipamiento informático y accedan o traten información de carácter personal para la realización de sus funciones y tareas sean conocedores y acepten estas normas de uso.

La Comisión de Seguridad podrá aprobar normas de uso específicas para algunos servicios TIC, si así lo estima conveniente.

3. Normas generales y de uso de los dispositivos

En ningún caso se podrá acceder a los recursos informáticos y telemáticos con las siguientes finalidades:

- Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
- Difundir contenidos contrarios a los principios enunciados en los Estatutos de la Universidad de Almería.
- Dañar los sistemas físicos y lógicos de la Universidad de Almería, de sus proveedores o de terceras personas.
- Introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar los daños.
- Usar cuentas de usuario sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta.
- Usar la red u ordenadores de la Universidad de Almería para conseguir acceso no autorizado a cualquier ordenador.
- Realizar con conocimiento de causa cualquier acto que interfiera en el correcto funcionamiento de los ordenadores, servicios, red de comunicaciones, etc.
- Intentar sobrepasar protecciones de datos o sistemas de seguridad informática.
- Violar la privacidad de los datos y el trabajo de otros usuarios.
- Queda prohibido terminantemente la apropiación de archivos o ficheros titularidad de la Universidad de Almería, para uso particular y/o de terceros.

3.1. De los ordenadores personales

La Universidad de Almería facilita a los Usuarios (profesores, alumnos y personal de administración y servicios) el equipamiento informático (conexión a servicios, ordenadores y red de comunicaciones) necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Este equipamiento es propiedad de la Universidad de Almería y no está destinado a un uso personal. El usuario se compromete a utilizar los recursos informáticos de la Universidad de Almería exclusivamente para usos relacionados con su actividad de docencia, estudio, investigación o gestión de la Universidad.

El Servicio TIC será el responsable de definir la configuración básica hardware y software de los puestos de trabajo y administrar los accesos a la red corporativa. Cualquier necesidad de

modificación del puesto será solicitada por la persona responsable de la dirección o unidad que lo solicita.

Los Usuarios deben cumplir las siguientes medidas de seguridad establecidas por la Universidad de Almería para el uso de los ordenadores personales:

- No está permitido alterar la configuración física de los equipos ni conectar otros dispositivos a iniciativa del Usuario, así como variar su ubicación.
- No está permitido alterar la configuración software de los equipos, desinstalar o instalar programas o cualquier otro tipo de software distinto a la configuración lógica predefinida.
- La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad del Servicio TIC. Nunca se almacenará en el dispositivo local información importante para el desarrollo del trabajo. Se utilizarán los espacios en servidores que proporcionará el Servicio TIC. Cada Usuario será responsable de la integridad y copia de seguridad de la información almacenada en el ordenador que tenga asignado.
- El Usuario deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario deberá comunicarlo al Servicio TIC para que tome las medidas oportunas.
- El usuario deberá cumplir con las instrucciones del Servicio TIC en relación a la protección del equipo de trabajo (uso de antivirus, congelación de equipos, etc)

3.2. De los dispositivos y soportes móviles

Los ordenadores portátiles tienen la misma consideración de puestos de trabajo y se rigen por las mismas normas anteriores. El uso al que están destinados y la posibilidad de que estos equipos se utilicen fuera del entorno de seguridad de la red corporativa de la Universidad de Almería hace necesarios procedimientos de seguridad específicos en relación con la actualización de los sistemas antivirus y del software instalado.

- Los equipos portátiles, así como los dispositivos o soportes informáticos, única y exclusivamente están puestos a disposición con la finalidad de permitir el desempeño de las funciones y tareas laborales encomendadas, estando prohibido el uso para otras finalidades de carácter personal.
- En caso de salida de dispositivos y soportes informáticos fuera del despacho con datos de carácter personal o sensibles deberá el usuario de adoptar medidas técnicas de cifrado de datos para evitar sean accesibles en caso de pérdida o robo.

Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el Usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.

4. Uso de la red corporativa

La red corporativa es un recurso compartido y limitado. Este recurso sirve no sólo para el acceso de los Usuarios internos de la Universidad de Almería a la intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

La información que circula por la red de la Universidad de Almería es propiedad de la Universidad de Almería.

El STIC proporcionará a los empleados y alumnos un servicio de conexión remota al sistema de información de la UAL, para cuando estos se encuentren fuera de la Universidad de Almería. Esta conexión será segura y cifrada.

Se recomienda que cualquier conexión que se realice desde el exterior a equipos dentro de la UAL sea segura y cifrada. Si la conexión puede llevar información de carácter personal, sensible o privilegiada, deja de ser una recomendación para ser una obligación.

Los Usuarios deben cumplir una serie de normas establecidas por la Universidad de Almería para el uso de la red corporativa:

- Las acciones sobre la red corporativa que intencionadamente rompan, retarden, pongan en peligro o accedan al trabajo de otros usuarios, sin autorización específica, están prohibidas, son éticamente reprobables y serán perseguidas con las normas internas, y judicialmente si fuera preciso.
- Está prohibido instalar o ejecutar en cualquier punto de la red informática programas que deterioren o incrementen en exceso la carga en cualquier punto de la misma, hasta el límite de llegar a perjudicar a otros usuarios o al rendimiento de la propia red. Esto incluye cualquier tipo de ensayo, experimento o actividad que incluso pudiendo ser considerada legítima perjudique el buen funcionamiento de la red.
- La utilización de Internet por parte de los Usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como personal de la Universidad de Almería, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de Usuario, y que no produzcan a una mejora en la calidad del trabajo desarrollado.
- Queda prohibido cualquier uso comercial y/o privado no autorizado de la red corporativa de la Universidad de Almería.
- Está prohibido el uso de programas de compartición de contenidos en red, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.
- Está prohibido instalar o ejecutar en cualquier punto de la red informática programas que traten de descubrir información distinta de la del propio usuario. Esto incluye los “sniffer”, escáner de puertos, etc.
- La conexión a la red fija de comunicaciones de un nuevo equipo informático tiene que ser autorizada por el STIC quien proporcionará a dicho equipo una dirección IP. Queda prohibido el uso de una dirección IP no proporcionadas por el STIC o el intercambio de ellas.
- Cualquier cambio de ubicación del dispositivo conectado a la red fija de comunicaciones debe ser comunicado al STIC.
- Queda prohibida la instalación de servidores DHCP conectados a la red de comunicaciones.
- La Universidad de Almería, a través del STIC, gestionará los rangos de direcciones IP que le han sido asignados por RedIRIS en base a criterios técnicos, de ahorro y eficacia.
- Cualquier acción sobre el cableado de la red de datos solo puede ser realizada por el Servicio TIC, o bien por un tercero bajo su supervisión y aprobación.
- La red inalámbrica de la Universidad de Almería usa para su funcionamiento las bandas liberadas de frecuencia 2.400-2.483 Ghz y 5725-5850 Ghz. La Universidad de Almería gestionará de estas bandas de frecuencias en sus instalaciones y con el objeto de evitar interferencias con su red inalámbrica prohíbe expresamente la instalación de cualquier punto de acceso de red inalámbrica que trabaje en las mencionadas bandas de frecuencia sin la autorización previa del Servicio TIC.

5. Acceso a aplicaciones y servicios

Gran parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde ordenadores personales a aplicaciones que residen en servidores conectados a la red corporativa.

La Universidad de Almería asignará a sus empleados y alumnos una cuenta de usuario institucional única que permitirá identificar unívocamente al usuario.

Los Usuarios deben cumplir las siguientes medidas de seguridad establecidas por la Universidad de Almería para el uso de aplicaciones y servicios corporativos:

- Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante Usuario y contraseña, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
- La custodia de la contraseña, certificado digital u otro medio de autenticación es responsabilidad del Usuario. Nunca debe utilizarse la cuenta de Usuario asignada a otra persona.
- El Servicio TIC establecerá normas de obligado cumplimiento respecto a las contraseñas: vigencia, calidad de las mismas, etc.
- Las contraseñas no deben anotarse, deben recordarse.
- Las contraseñas deben cambiarse periódicamente. Los Usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.
- Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable correspondiente.
- Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones y bloquear la pantalla con contraseña.

Dentro del ENS, en su Anexo II Medidas de Seguridad, Apartado 4. Marco operacional [op], Subapartado 4.2.1. Identificación [op.acc.1], en relación a la identificación de los usuarios del sistema, nos indica que:

> *"4. Las cuentas de usuario se gestionarán de la siguiente forma:*
>
> *a) Cada cuenta de usuario estará asociada a un identificador único."*

Se limita en la UAL por tanto el uso de cuentas de usuario genéricas (no directamente asociadas a una persona) solo a los casos y para los usos estrictamente necesarios (ej: correo electrónico de un servicio o departamento). No se permitirá el uso de las mismas para el acceso a los sistemas de información de la UAL.

En el mismo apartado anterior del ENS podemos leer:

> *"b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario."*

La Universidad creará las instrucciones técnicas necesarias para garantizar el correcto flujo de información que permita inhabilitar las cuentas de usuario cuando proceda o modificar los permisos de acceso asociados a las mismas.

5.1. Correo electrónico

Se considera el correo electrónico institucional como un instrumento básico de trabajo. El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones.
En relación con la dirección de correo electrónico institucional, la Agencia Española de Protección de Datos indica que se trata de un dato personal cuando la dirección de correo electrónico incorpora datos relacionados con la persona titular de la cuenta o cuando, aunque no los incorpore, otros datos

(como el dominio o el domicilio o el nombre y apellidos) permitan identificar a un usuario sin un esfuerzo desproporcionado, aunque la exposición pública del correo electrónico institucional en la web de la Universidad se haga con fines estrictamente profesionales.

Sobre este aspecto, la Universidad creará las Reglas Técnicas de uso del Correo Electrónico que pondrá a disposición de todos los trabajadores, al objeto de que se eviten los envíos masivos de información, o lo correos que se destinen a gran número de usuarios que serán solo los estrictamente necesarios para no provocar un colapso del sistema de correo y para corregir malas prácticas.

6. Acceso y tratamiento de datos personales a nivel informático y en papel

Las instrucciones descritas en este documento serán de aplicación en la observancia del cumplimiento de una normativa de especial importancia, el Real Decreto 951/2015, de 23 de octubre, de modificación del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el Reglamento UE 2016/676 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo referente al tratamiento de datos personales y a la libre circulación de datos, y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. Dado que esta legislación trata de salvaguardar un derecho fundamental, mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el Usuario, que accede y trata información de carácter personal en el desempeño de las funciones y tareas, deberá atender a las siguientes obligaciones.

- Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal, conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la Universidad de Almería.

Dato personal = Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

6.1. Ficheros informáticos

En particular, respecto a la información de carácter personal contenida en ficheros informáticos, deberá cumplir, en consonancia con lo expuesto en anteriores apartados, las siguientes diligencias:

- Claves de acceso al sistema informático.- Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Queda prohibido, asimismo, emplear identificadores y contraseñas de otros Usuarios para acceder al sistema informático. En caso de que fuera necesario acceder al sistema, en ausencia de un compañero, se solicitará al Responsable de Seguridad que se habilite el acceso eventual. Una vez finalizada la/s tarea/s que motivaron el acceso, deberá ser comunicado, de nuevo, al Responsable de Seguridad.

- Bloqueo o apagado del equipo informático.- Bloquear la sesión del Usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público.

- Almacenamiento de archivos o ficheros en la red informática.- Guardar todos los ficheros de carácter personal empleados por el Usuario, en el espacio de la red informática habilitado por la Universidad de Almería, en concreto por el Servicio de Tecnologías de la Información y las Comunicaciones, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.

- Manipulación de los archivos o ficheros informáticos.- Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros. Los permisos de acceso de los Usuarios a los diferentes ficheros son concedidos por la Universidad de Almería, en concreto por el Responsable de Seguridad. En el caso de que cualquier Usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del citado departamento.

- Generación de ficheros de carácter temporal.- Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. Estos ficheros deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática. Si transcurrido un mes el Usuario detecta la necesidad de continuar utilizando la información almacenada en el fichero, deberá comunicárselo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.

- No uso del correo electrónico para envíos de información de carácter personal sensible.- No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros. De modo que, se pondrá en conocimiento del Responsable de Seguridad para que implemente el cifrado, encriptado u otro mecanismo que salvaguarde la integridad y privacidad de la información.

- Comunicación de incidencias y en su caso, violaciones de seguridad que afecten a la seguridad de datos de carácter personal.- Comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales a la Comisión de Seguridad y Protección de Datos de la UAL.

Entre otros, tienen la consideración de incidencia de seguridad que afecta a los ficheros informáticos, los sucesos siguientes:

- Pérdida de contraseñas de acceso a los Sistemas de Información.
- Uso indebido de contraseñas.
- Acceso no autorizado de usuarios a ficheros excediendo sus perfiles.
- Pérdida de soportes informáticos con datos de carácter personal.
- Pérdida de datos por mal uso de las aplicaciones.
- Ataques a la red.
- Infección de los sistemas de información por virus u otros elementos dañinos.
- Fallo o caída de los Sistemas de Información, etc.

6.2. Ficheros en papel

En relación con los ficheros en soporte o documento papel, el Usuario deberá cumplir con las siguientes diligencias:

- Custodia de llaves de acceso a archivadores o dependencias.- Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal.

- Cierre de despachos o dependencias.- En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

- Almacenamiento de soportes o documentos en papel.- Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada laboral. Cuando estos soportes o documentos, no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.

- No dejar en fotocopiadoras, faxes o impresoras papeles con datos de carácter personal.- Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes.

- Documentos no visibles en los escritorios, mostradores u otro mobiliario.- Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario; especialmente en las zonas de atención al público, guardando así una adecuada política de prevención de mesas limpias.

- Desechado y destrucción de soportes o documentos en papel con datos personales.- No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. A estos efectos, deberá ser siempre desechada o destruida mediante las destructoras de papel de las que dispone la Universidad de Almería. Se prohíbe terminantemente echar en papeleras, contenedores de cartón o papel, soportes o documentos, donde se contengan datos personales.

- Archivo de soportes o documentos.- Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de la Universidad de Almería. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información. Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos. No podrá acceder o utilizar los archivos pertenecientes a otros Departamentos, que compartan la sala o dependencia habilitada a archivo.

- Traslado de soportes o documentos en papel con datos de carácter personal.- En los procesos de traslado de soportes o documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubieren datos de carácter personal.

- Traslado de dependencias.- En caso de cambiar de dependencia, en el proceso de traslado de los soportes o documentos en papel, se deberá realizar con el debido orden. Asimismo,

se procurará mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal.

- Envío de datos personales sensibles en sobre cerrado.- Si se envían a terceros ajenos a la Universidad de Almería, datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte o documento papel, se debe realizar, en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.

- Comunicación de incidencias y en su caso, violaciones de seguridad que afecten a la seguridad de datos de carácter personal.- Comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales a la Comisión de Seguridad y Protección de Datos de la UAL.

Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel, los sucesos siguientes:

- Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal.
- Uso indebido de las llaves de acceso.
- Acceso no autorizado de usuarios a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal.
- Pérdida o sustracción de soportes o documentos en papel, con datos de carácter personal.
- Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal

7. Sobre la Gestión de Incidentes de Seguridad

La Universidad de Almería cuenta con un Procedimiento de Gestión de Incidentes y brechas o violaciones de Seguridad que define y establece los procedimientos mediante los cuales se deben identificar, catalogar, resolver y/o escalar todas aquellas entradas con eventos de seguridad.

De conformidad con el art. 4.12 RGPD entendemos por violación de seguridad, aquel incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Por tanto, toda violación de seguridad tendrá la consideración de incidente pero no todo incidente supondrá una violación de seguridad, sino únicamente aquellos que afecten a datos de carácter personal.

Por tanto, teniendo en cuenta los aspectos destacados a los que aluden los apartados anteriores, 6.1 Ficheros Informáticos y 6.2 Ficheros en Papel, relacionados como brechas de seguridad en los que se vean implicados “datos personales”, será de obligado cumplimiento para todo el personal de la Universidad de Almería, informar en el plazo máximo de 2 horas a la Comisión de Seguridad Informática y Protección de Datos, sobre cualquier hecho detectado para que se evalúe y se revise de la forma adecuada.

Vía de comunicación de incidencias con la Comisión de Seguridad:

- a través del email consulta.comision.seguridad@ual.es
- a través del formulario de notificación de incidencias de la página web de la Comisión de Seguridad http://seguridad.ual.es

Cualquier otro tipo de incidencia de seguridad TIC se comunicará al STIC a través de su Centro de Atención a Usuarios:

- Teléfono 950 015999
- http://caustic.ual.es

8. Medidas sancionadoras

La Universidad de Almería podrá suspender el uso de estos recursos a aquellos usuarios que contravengan la presente normativa y en los casos en los que cualquier circunstancia sobrevenida lo aconseje.

Si el posible trastorno causado a otros usuarios o al servicio, por un usuario, se entiende que no afecta de forma inmediata al buen funcionamiento del servicio, se le notificará su mal proceder mediante correo electrónico u ordinario. Si, por el contrario, se entendiera que el trastorno producido altera el buen funcionamiento del servicio, el STIC tendrá la facultad de tomar las medidas necesarias para restaurar de forma inmediata el correcto servicio. Entre otras medidas de aplicar, se contemplan las siguientes:

- Deshabilitar las cuentas de usuario.
- Inhabilitar el acceso a la red de los dispositivos que estén generando el mal funcionamiento.
- Inhabilitar los servicios del usuario que estén generando el mal funcionamiento (por ejemplo una página web).