Medidas de protección aplicadas en la Universidad de Granada para el tratamiento de información con datos personales

Tabla de contenido

Oficina de Protección de Datos. Universidad de Granada. Complejo Administrativo Triunfo, Pabellón 7.
Avda. del Hospicio, s/n. 18071 GRANADA
Tfno. (+34) 958 24 0874. Correo electrónico protecciondedatos@ugr.es

1. INTRODUCIÓN

La Universidad de Granada, en razón de las competencias y funciones que le atribuye la normativa universitaria, presta una serie de servicios públicos, y para ello recaba y trata, de forma automatizada o no, datos de carácter personal de su estudiantado, profesorado, personal de administración y servicios o de la ciudadanía en general.

La protección de los derechos y libertades de las personas en relación con el tratamiento de sus datos personales que lleva a cabo la Universidad exige la adopción de medidas técnicas y organizativas con la finalidad de garantizar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos europeo (en adelante RGPD) y, en particular, una adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

El RGPD no establece unas medidas de seguridad o controles mínimos de obligado cumplimiento para garantizar la seguridad de los datos, sino que corresponderá al responsable determinar aquellas que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

No obstante, partiendo de que el *Esquema Nacional de Seguridad*, por lo que se refiere a las medidas de seguridad, es aplicable a cualquier información tratada por la Universidad de Granada como Administración Pública, sin distinción del soporte en el que se encuentre, este documento pretende contribuir a la difusión e implementación de las medidas de seguridad que, de acuerdo al Anexo II (Medidas de seguridad) del 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, se encuentran descritas en los documentos que conforman la Política de Seguridad de la Universidad de Granada publicada en la página web de Secretaría General (http://secretariageneral.ugr.es/pages/seindex), apartado seguridad de la información.

Básicamente se trata de establecer garantías de seguridad adecuadas (art. 5.1.f RGPD) que eviten, fundamentalmente, dos cosas:

- El tratamiento no autorizado o ilícito de datos personales.
- La pérdida de los datos personales, la destrucción o el daño accidental.

Para poder evitar ambos riesgos, se exige el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales, así como demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva). A título ejemplificativo, el RGPD señala las siguientes medidas:

- La pseudonimización y el cifrado de datos.
- Mecanismos que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes en los sistemas y servicios de tratamiento.
- Mecanismos que tengan la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en casos de incidente físico o técnico.
- Procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas de seguridad.

Se presentan, a continuación, una relación de medidas de protección, a modo de lista de verificación (*check list*), distinguiendo entre:

- Datos automatizados o informatizados los cuales, en la Universidad de Granada, pueden ser centralizados (gestionados por el CSIRC) o locales (gestionados de forma autónoma por usuarios externos al CSIRC), y
- Datos tratados en papel.

2. MEDIDAS PARA DATOS AUTOMATIZADOS

Conforme al Certificado de Conformidad con el Esquema Nacional de Seguridad (en adelante ENS), obtenido por la Universidad de Granada para sistemas de información de categoría media, se parten de las medias Organizativas, Operacionales y de Protección definidas en el 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, modificado por Real Decreto 951/2015.

Para datos automatizados conviene distinguir dos niveles de seguridad en la Universidad de Granada en función de la ubicación final de los datos, siendo, no obstante, aconsejable que todos los datos estén en nivel 1. Dichos niveles son:

- **Nivel 1:** medidas establecidas en el Anexo II del R.D. 3/2010. Se aplicarán sobre datos centralizados controlados por el CSIRC (Centro de Servicios de Informática y Redes de Comunicaciones) y en datos en el marco del ENS.

- **Nivel 2 o básico:** son las medidas descritas en los apartados siguientes que deben estar implementadas en los sistemas de información no controlados por el CSIRC que contengan datos personales. Al exponer cada una de ella, se añaden unas casillas en formato de *checklist*, a efectos de verificar su aplicación.

Las medidas de seguridad que deben cumplirse para datos automatizados no centralizados clasificadas según anexo II del R.D. 3/2010 son las siguientes:

A. **Marco Operacional:** está constituido por las medidas destinadas a proteger la operación del sistema.

a. ***Control de acceso:*** **s**e trata de medidas de identificación en los sistemas (ordenadores) consistentes en:

- No dejar ordenadores sin proteger, al menos protegerlos mediante clave.

No aplicada	
Aplicada	

- No dejar las claves escritas en *post-it* pegados en el equipo, ni a la vista. Si es posible utilizar alguna aplicación para móvil para gestión de claves, en el caso de tener muchas.

No aplicada	
Aplicada	

- Los usuarios creados en los ordenadores deben identificar a una sola persona.

No aplicada	
Aplicada	

- Cuando la persona que acceda al sistema tenga diferentes roles de manejo de la máquina debe crearse usuarios diferentes en dicha máquina/ordenador.

No aplicada	
Aplicada	

- Las cuentas deben tenerse durante el periodo necesario para atender necesidades de posible trazabilidad (que ha hecho el usuario), es lo que se llama periodo de retención.

No aplicada	
Aplicada	

- Los usuarios creados en la máquina deberán tener el mínimo número de privilegios sobre el equipo para trabajar. Se debe seguir una política de mínimos privilegios sobre los usuarios.

No aplicada	
Aplicada	

- Las credenciales de accesos al sistema (claves/*password*) estarán bajo el exclusivo control del usuario, no se deben ceder nunca.

No aplicada	
Aplicada	

- Se debe limitar el número de intentos de acceso, bloqueando el usuario una vez pasados 5 intentos fallidos.

No aplicada	
Aplicada	

- Se deben registrar los intentos con éxito y fallidos en la medida de lo posible. Esto se puede hacer activando la auditoría en *Windows.*

No aplicada	
Aplicada	

- Se debe informar al usuario una vez acceda cuando fue la última vez que accedió para su autocontrol.

No aplicada	
Aplicada	

- En el caso de acceso remoto al equipo, esto es, no estando sentados delante de él, se debe utilizar accesos mediante VPN.

No aplicada	
Aplicada	

b. ***Explotación:*** En este apartado se explicitan medias básicas para la gestión de los equipos que tengamos a nuestro cargo con datos personales.

- Mantener un inventario de ordenadores a nuestro nombre. Aunque el CSIRC tiene dicha lista, es conveniente revisarlo y tenerlo actualizado. Se deben incluir en una lista personal los equipos portátiles donde se trabajen con datos personales. Hay que incluir al menos número de serie, dirección MAC (*Media Access Control*, mirar glosario) de red del equipo, tipos de datos contenidos,

No aplicada	
Aplicada	

marca y modelo. En el caso de extravío se podrá utilizar este inventario para poner denuncia.

- Se deben eliminar las cuentas de usuario que trae por defecto el equipo, excepto la de administrador, pero la de "guest" o "invitado" se debe eliminar o bloquear dentro del apartado de administración de usuarios del ordenador.

No aplicada	
Aplicada	

- Hay que cambiar la clave por defecto, las que trae el ordenador una vez instalado el sistema, para el resto de cuentas, así se evitan accesos indebidos.

No aplicada	
Aplicada	

- Se deben cambiar las claves/*password* al menos una vez cada 6 meses.

No aplicada	
Aplicada	

- Se deben tener los sistemas actualizados para evitar vulnerabilidades. Aconsejable activar actualizaciones automáticas.

No aplicada	
Aplicada	

- Ante cualquier incidente de seguridad, o sospecha, debemos comunicarlo a Seguridad Informática del CSIRC a través del email seguridadinformatica@ugr.es .

No aplicada	
Aplicada	

- Debemos tener instalado un antivirus actualizado. La Universidad ofrece uno normalmente de forma gratuita, puede buscarlo en la página del CSIRC (csirc.ugr.es) apartado *software*.

No aplicada	
Aplicada	

- Debemos tener algún mecanismo de detección de intrusión en el equipo. Aconsejable tener un *firewall* configurado y activado controlando qué direcciones IP pueden acceder de forma remota al equipo.

No aplicada	
Aplicada	

B. Medidas de protección.

a. ***Instalaciones.*** Debemos tener especial cuidado con la ubicación física de los equipos. Se deben seguir las siguientes pautas:

- En el caso de tener los equipos fácilmente accesibles físicamente, para evitar robos se deberán tener en una caja cerrada con llave y ventilada. Esto se realizará para servidores que contengan datos personales de cualquier tipo.

No aplicada	
Aplicada	

- En caso de servidores es aconsejable tener protección de corriente mediante algún sistema de alimentación ininterrumpida, y aire acondicionado para evitar roturas por calentamiento.

No aplicada	
Aplicada	

- El acceso físico al ordenador debe estar controlado, los despachos deben quedar cerrados un vez se abandonen, bien al final de la jornada o a la salida para hacer alguna gestión.

No aplicada	
Aplicada	

- Se debe tener un control de entrada y salida de dispositivos, apuntando que persona lo realizó.

No aplicada	
Aplicada	

b. Protección de equipos:

- Se exigirá que los puestos de trabajo, mesas de escritorio, permanezcan despejados, sin más material encima que el requerido para la actividad que se está realizando en cada momento. El material no utilizado debe guardarse en lugar cerrado.

No aplicada	
Aplicada	

- El ordenador se bloqueará al cabo de un tiempo prudencial de inactividad de forma automática, requiriendo una nueva autenticación del usuario para reanudar la actividad, para ello hay que configurarlo en *Windows* las opciones de bloqueo de pantalla.

No aplicada	
Aplicada	

- Cuando abandone el ordenador debe dejarlo bloqueado. En *Windows* se hace con la tecla "Windows" + tecla L .

No aplicada	
Aplicada	

- Los equipos portátiles que se conecten remotamente a recursos de la Universidad deben hacerlo mediante VPN. Se aconseja igualmente que se active el cifrado del disco (en *Windows bitlocker*) y en el caso de pérdida del ordenador se deberá avisar. Para ello mirar protocolo de notificación brechas de seguridad de datos personales.

No aplicada	
Aplicada	

c. ***Protección de los soportes de información:*** en este apartado se describen medidas que se podrían aplicar a discos duros, dispositivos USB, cintas de copias de seguridad, etc. En lo relativo a tratamiento en información en papel, hay medidas que también se podrían aplicar a estos dispositivos. En cualquier caso, la pautas a seguir son:

- Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad que deben tener. En caso de ser información sensible pondríamos seguridad alta; en cualquier otro supuesto se pondría como seguridad normal. Los usuarios deben estar capacitados para entender las etiquetas, mediante una simple inspección o mediante consulta a un registro o repositorio.

No aplicada	
Aplicada	

- Se cifrará en la medida de lo posible, garantizando la confidencialidad y la integridad de la información contenida en los dispositivos removibles tales como DVD, CD, discos USB y otros similares. Si no se puede utilizar cifrado al menos los datos personales pueden ir en ficheros comprimidos con clave pudiéndose utilizar para ello la aplicación ***7zip*** de distribución gratuita o *veracrypt* aplicación de cifrado para discos y/o ficheros.

No aplicada	
Aplicada	

- Se aplicarán medidas de acceso a los soportes de información garantizando el control de acceso con medidas físicas (tenerlos en un armario bajo llave, por ejemplo, y anotar quien los coge) y tener en cuenta las garantías de conservación del fabricante (temperatura y humedad) para evitar el deterioro.

No aplicada	
Aplicada	

- Se garantizará que los dispositivos permanecen bajo control, de manera segura, en los desplazamientos. Se aconseja tener un registro de entrada/salida donde se indique que se saca de las dependencias, indicando el contenido y quien lo hace.

No aplicada	
Aplicada	

- Cuando se dejen de utilizar los soportes se deben borrar y/o destruir de forma segura. Si se recurre a una empresa externa deben darnos un certificado de dicha destrucción segura.

No aplicada	
Aplicada	

- En el caso de reutilización de cintas para copias de seguridad se deberán borrar previamente a grabar algo en ellas.

No aplicada	
Aplicada	

- Se realizarán copias de seguridad que permitan recuperar los datos perdidos, accidentalmente o intencionadamente con una antigüedad determinada. Es aconsejable hacer pruebas del estado de las copias, por si hubiese deterioro.

No aplicada	
Aplicada	

- En el caso de envío de documentos se retirará toda la información adicional contenida en campos ocultos, *meta-datos*, comentarios o revisiones anteriores, salvo cuando dicha información sea importante para el receptor del documento.

No aplicada
Aplicada

- Se revisará la información obsoleta publicada en las páginas web y se retirará una vez haya cumplido su cometido de informar.

No aplicada	
Aplicada	

3. MEDIDAS DE PROTECCIÓN PARA DATOS EN PAPEL

MEDIDAS A APLICAR	
• **Política de mesas limpias** (Custodia de la información). Se debe impedir el acceso a toda persona no autorizada. Se debe tener en la mesa solo lo necesario para el trabajo que se ha de realizar. Cuando termine la jornada, los documentos con datos personales deben quedarse bajo llave.	
• **Destructora de papel** (Destrucción de documentos). Evitar tirar documentos confidenciales y/o con datos personales a la papelera. Se debe eliminar en una destructora. Si hay gran volumen de documentos se puede llamar a una empresa para reciclaje a través de la UCA, Unidad de Calidad Ambiental, de la UGR. En este caso se debe hacer inventario de lo que se le entrega a la empresa y esta debe devolver un certificado de destrucción de la información suministrada.	
• **Datos bajo llave, acceso a la información controlada** (Custodia información). De forma general, los documentos confidenciales y con datos personales, al final de la jornada laboral, deben quedarse bajo llave (armarios, zonas cerradas con llave, despachos cerrados con llave). Cuando se trate de listas de comunicación **en tablones de anuncios** con datos personales estas deberán estar detrás de un cristal bajo llave para evitar hurtos.	
• **Datos sensibles** (salud, afiliación sindical, orientación sexual, etc.). Se ha de realizar un control de acceso mediante registro de las personas que acceden a esta información. Si hay una entrada/salida de soportes físicos que contengan este tipo de datos debe quedar convenientemente registrado.	
• **Traslado físico.** Se debe evitar la sustracción, pérdida o acceso indebido a la documentación. El traslado de los documentos se hará en carpetas, sobres cerrados o cajas cerradas etiquetados para saber su contenido. Cualquier salida de documentación fuera de las instalaciones de la UGR para fines de trabajo deberá estar debidamente autorizada.	
• **Etiquetado**. Etiquetar las carpetas que contengan documentación personal de forma operativa con el objeto de saber su contenido.	
• **Criterios de archivo**. Se debe garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas. Se ha de tener un inventario de los soportes.	

MEDIDAS A APLICAR	
• **Impresoras compartidas**. Establecer control de acceso a ellas. Una vez que enviemos datos a imprimir los documentos deben estar en la impresora el menor tiempo posible para evitar acceso a personal no autorizado. No es aconsejable que estén ubicadas en espacios que no estén dentro del ámbito de control visual del personal encargado.	
• **Copias de documentos**. Solo se harán copias en la medida que resulte estrictamente necesario para el desempeño de las funciones y tareas asignadas. En todo caso, serán destruidos cuando la finalidad para la que se realizaron se haya cumplido.	

4. MEDIDAS DE PROTECCIÓN PARA ALMACENAMIENTO DE DATOS PERSONALES EN LA NUBE

MEDIDAS A APLICAR	
• **Claves seguras y diferentes para cada uno de los servicios de la nube.** Como con el resto de medidas que se indican en este documento hay que tener en cuenta la utilización de claves que sean difíciles de descifrar con longitud mínima de 10 caracteres y que mezcle mayúsculas, minúsculas, números y caracteres especiales. Esta clave deberá cambiarse de forma periódica no superando periodos mas allá de un año. Se debe tener en cuenta que si tenemos varios servicios de almacenamiento deberemos tener diferentes claves. Y por supuesto no dársela a conocer a terceros.	
• **Cifrado de información sensible.** Para datos personales sensibles es aconsejable cifrarlos cuando se trate de nubes públicas. Se podrá utilizar ficheros comprimidos con clave utilizando por ejemplo la utilidad *7zip* o alguna aplicación como *boxcryptor*.	
• **Copias de Seguridad**. Para evitar la pérdida de información es necesario hacer copias de los contenidos en la nube, bien sean en nubes privadas propias de UGR, o públicas como Google drive.	

MEDIDAS A APLICAR	
• **Segundo factor de autenticación (2FA).** Se recomienda que en las nubes que se pueda utilizar un segundo factor de autenticación utilizarlo para una mayor seguridad en el acceso a los datos. El 2FA es un procedimiento donde aparte de la clave normal se utiliza una segunda clave suministrada por SMS, por correo o por aplicaciones como Authenticator de Google. Por supuesto Google lo permite.	
• **Trasferencia securizada.** Se debe verificar que la transferencia de información se realiza de forma securizada, en el caso de UGRDrive utilizamos https. Así para conectarnos vía web utilizamos la URL https://drive.ugr.es	
• **Exponer datos lo menos posible.** Borrar los datos cuando que ya no sean necesarios, sobre todo en nubes públicas. Por una parte para optimizar el espacio y por otra para evitar sobre explosión de información a posibles vulnerabilidades por accesos indebidos.	
• **Criterios de archivo**. Clasificar la información. Saber que información se sube a la nube, no subir de forma indiscriminada todos los datos personales si no es necesario que estén allí.	
• **Utilizar servicios propios de UGR. Nube privada.** UGRDrive (https://drive.ugr.es) es de uso exclusivo de investigadores. Documenta (https://documenta.ugr.es) para gestión universitaria, es un gestor documental basado en la aplicación Alfresco, se accede con usuario de correo electrónico y la clave de este.	
• **Localización de los datos.** Para saber que la información esté bajo el amparo de normativa europea debemos saber la ubicación física de la información en el caso de nubes públicas. Así por ejemplo Google Drive asegura en su política de privacidad indican que los datos de usuarios europeos se almacenaran en Irlanda a partir del 22 de enero del 2.019. Si se utiliza Google Drive aconsejamos hacerlo bajo el amparo del convenio firmado UGR-Google por el que se creo el dominio go.ugr.es (https://go.ugr.es)	
• **Tener contrato con el proveedor de la nube pública.** Si usa nube pública debe tener un contrato con el proveedor del servicio. En dicho contrato debe aparecer los servicios que suministra el proveedor así como ubicación física de servidores y medidas de seguridad aplicadas a los datos. Debe prestar especial atención al clausulado relativo a la responsabilidad y propiedad de los datos, algunos proveedores se adueñan de ellos como ya lo hizo dropbox en su día.	
• **Compartición de ficheros con datos personales**. Si se utiliza la nube (pública o privada) para compartir archivos se deberán compartir siempre indicándole una clave al recurso compartido para evitar que si cae la URL de compartición en malas manos se pueda hacer mal uso. Asegurarse que se comparte y evitar que se muestre más información de la debida.	

MEDIDAS A APLICAR	
En general, para cualquier servicio contratado en la nube, aparte de las medidas indicadas en esta tabla, debe prestarse especial atención a los siguientes aspectos: ○ Tiempos de respuesta de los servicios, para evitar, en la medida de lo posible, la interrupción de los servicios. ○ Ubicación de los equipos, se aplicará las normativa del país donde estén. ○ Contrastar si se nos ofrece acceso a l*ogs* de los sistemas para posibles auditorias que deseemos hacer. ○ Revisar de forma periódica, una vez al año, las condiciones del servicio, por sihan sido modificadas sin ser comunicadas. ○ Ante la duda en materia de condiciones contractuales, consultar con la Oficina de Protección de Datos.	

5. MEDIDAS DE PROTECCIÓN PARA ALMACENAMIENTO DE DATOS PERSONALES EN APP's .

Para app's para dispositivos móviles desarrolladas por la Universidad de Granada se deberán observar las medidas del apartado 4 de este documento, en la medida de lo posible.

GLOSARIO:

ARCO derechos: Derechos de Acceso, Rectificación, Cancelación u Oposición.

Cifrar: es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

Firewall*:** un **cortafuegos** (firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Logs: Es un registro de eventos ocurridos en el equipo/servidor, tales como registro de accesos, avisos de funcionamiento del sistema o el servicio, errores producidos, etc….

MAC (Dirección MAC de un dispositivo): es acrónimo de *Media Access Control*, o Control de Acceso al Medio. Es una dirección física que está asociada de forma inherente a la tarjeta de red que tiene el dispositivo. No confundir con la dirección IP, esta puede variar. La MAC no cambia. Se puede ver en los diferentes dispositivos viendo los parámetros de red; son números hexadecimales separados por ":". Ejemplo: AB:01:CD:55:EF

Metadatos**:** en general, un grupo de *metadatos* se refiere a un grupo de datos que describen el contenido informativo de un objeto al que se denomina "recurso". Por ejemplo en un fichero de fotografía se guardan datos de localización ,foco, paleta de color, persona que la ha editado, etc.

VPN (*Virtual Private Network*): mecanismo para establecer una conexión punto a punto de forma cifrada entre dos dispositivos en red. Puede información relativa a esto en vpn2.ugr.es. Para conectarse a UGR debe descargarse un software que se indica en la URL del CSIRC o de vpn2.ugr.es.