I. DISPOSICIONES Y ACUERDOS GENERALES

I.3. Rector

Resolución Rectoral de 19 de julio 2017 por la que se aprueba el Documento de Seguridad como normativa de desarrollo de la Política de Seguridad de la Información de la Universidad de Sevilla.

Mediante Acuerdo del Consejo de Gobierno de 26 de febrero de 2014, se aprobó la Política de Seguridad de la Información de la Universidad de Sevilla, que dispone, en su artículo 9, que citada Política "será revisada anualmente por la Comisión de Seguridad de la Información y será aprobada por Resolución Rectoral".

La Comisión de Seguridad de la Información en sesión de 17 de julio de 2017 acordó proponer al Rector de la Universidad de Sevilla la aprobación del Documento de Seguridad, para su aprobación por Resolución Rectoral.

Por Resolución Rectoral de 17 de julio de 2017 se aprobó el Texto integrado del Documento de Seguridad de la Universidad de Sevilla conforme a la propuesta por la Comisión de Seguridad de la Información.

El Artículo 5.1 de la Política de Seguridad de la Información dispone que entre las funciones y responsabilidades propias de la Comisión de Seguridad de la Información se encuentra proponer al Rector la aprobación de las normativas y reglamentos de seguridad relacionados con la aplicación del Esquema Nacional de Seguridad.

En la citada sesión de 17 de julio de 2017 la Comisión de Seguridad de la Información acordó proponer al Rector la aprobación de la normativa que describe el Documento de Seguridad en relación a la protección de datos de carácter personal en la Universidad de Sevilla, cuyo texto se incorpora al acta de la sesión.

En su virtud, mediante la presente Resolución acuerdo:

1. Aprobar la siguiente Normativa de la Universidad de Sevilla, que se incluye como Anexo a la misma:
   - Documento de Seguridad de la Universidad de Sevilla.

2. La citada normativa entrará en vigor desde el día de la fecha, no obstante será publicada en el Boletín Oficial de la Universidad de Sevilla.

EL RECTOR,
Miguel Ángel Castro Arroyo.

ANEXO

NORMATIVAS DE SEGURIDAD
DOCUMENTO DE SEGURIDAD DE LA UNIVERSIDAD DE SEVILLA

Índice

INTRODUCCIÓN

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 1720/2007 de 13 de Diciembre), recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este Documento se mantendrá permanentemente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

El contenido principal de este Documento queda estructurado como sigue:

I. Ámbito de aplicación del documento.

II. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

III. Procedimiento general de información al personal.

IV. Funciones y obligaciones del personal.

V. Procedimiento de notificación, gestión y respuestas ante las incidencias.

VI. Procedimientos de revisión.

VII. Consecuencias del incumplimiento del Documento de Seguridad.

A continuación se detallan los anexos a este Documento de Seguridad (DS) con sus correspondientes contenidos:

Anexo I. Nombramientos.

Con el fin de establecer la identificación de los Responsables Propietarios de los ficheros y de los Responsables de Seguridad se recoge en este Anexo.

Anexo II. Formatos de Documentos.

En este Anexo se presentan los formatos de documentos para llevar a cabo las actividades en materia de seguridad que desarrolla el Reglamento.

VIGENCIA

El presente documento ha sido aprobado por la Comisión de Seguridad de la US con fecha 17 de julio de 2017, estableciendo de esta forma las directrices generales para aplicar la regulación relativa a la protección de datos personales en la Universidad de Sevilla.

Este documento entrará en vigor inmediatamente después de su publicación y difusión por parte de la US. Las versiones anteriores quedan anuladas por la última versión de este documento.

CAPÍTULO I. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de la Universidad de Sevilla, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

- Nivel básico: Se aplicarán a los ficheros con datos de carácter personal.
- Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, (en estos dos casos, deberán ser de titularidad pública), servicios financieros y los que se rijan por el Art. 29 de la LOPD (prestación de servicios de solvencia y crédito).
- Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual o los recabados para fines policiales sin consentimiento (en este último caso, también deberán ser de titularidad pública).

Todas las personas que tengan acceso a los datos de estos ficheros, bien a través del sistema informático habilitado para acceder al mismo, o bien a través de cualquier otro medio de acceso, se encuentran

obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

Recursos protegidos.

La protección de los datos de los anteriores ficheros frente a accesos no autorizados se deberá realizar mediante el control de todas las vías por las que se pueda tener acceso a dicha información. Los recursos que, por servir de medio directo o indirecto para acceder al Fichero, deberán ser controlados por esta normativa son:

- Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan.
- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero.
- Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero.
- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.

Los recursos hardware y software para el tratamiento de los ficheros de datos de carácter personal vienen recogidos en el "Anexo II. Formatos de Documentos" con el número 02-010-00 para el inventario de hardware y con el número 02-020-00 para el inventario de software

Todos estos recursos se encuentran asignados a los servicios, departamentos y secciones que figuran en el Anexo I.

CAPÍTULO II. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

II.1. Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales.

El responsable del fichero según el Art. 11 del Reglamento se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al Sistema de Información y a la documentación correspondiente en los ficheros mixtos. Para ello, se ha delegado la función de crear y mantener actualizada dicha relación en los Responsables Propietarios de nivel Tecnológico y de nivel Funcional, en sus respectivas atribuciones.

El procedimiento de identificación y autenticación garantizará la confidencialidad e integridad de las contraseñas en la forma de asignación, distribución y almacenamiento de las mismas. Todo ello de acuerdo con el Art. 93.4 del Reglamento 1720/2007 que indica que "*el documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con lo que tienen que ser cambiadas las contraseñas que, mientras estén vigentes se almacenarán de forma ininteligible*" y el Art. 93.3 del Reglamento que indica que "*Existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad*".

El usuario de los ficheros de datos personales debe tener en cuenta lo siguiente:

- El usuario deberá modificar las claves que le entregue el administrador de manera inmediata a su recepción.

- Los usuarios no pueden compartir sus claves bajo ningún concepto con otras personas, aunque sean de su mismo entorno.
- Guardar la información de claves en un lugar seguro pero accesible.
- Los usuarios deberán cambiar sus contraseñas al menos una vez cada año.

Respecto a asignación de contraseñas, éstas deberán ser conformes a la Política de Contraseñas de la Universidad de Sevilla.

Los administradores de los sistemas deberán tener en cuenta los siguientes puntos:

- Cambiar periódicamente la contraseña, sobre todo si hay cambios (bajas, traslados) entre el grupo de personas que la conocen.
- El código de usuario y la contraseña se comunicarán al usuario por vías seguras, y preferentemente por vías diferentes o no al mismo tiempo. Los envíos no tendrán indicación externa de su contenido ni podrán leerse al trasluz, ni abrir los sobres sin detectarse". Cuando se envíen a través de redes inseguras deberían comunicarse mediante protocolos seguros.

En los ficheros de datos personales la identificación de los usuarios se deberá realizar de forma inequívoca, unívoca y personalizada, verificando su autorización. Asimismo, en los ficheros de nivel medio y alto de se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema información.

II.2. Medidas y normas relativas al Control de acceso.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. La exigencia que se materializa en la inclusión del documento formato 03-060-020 que se incluye en el Anexo II de acuerdo con el Art. 91 Control de acceso que indica que:

- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
- El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

Los estándares del control de acceso para los sistemas de información deben establecerse intentando satisfacer la necesidad de balancear las restricciones para prevenir accesos no autorizados frente a la necesidad de proporcionar acceso sin obstáculos en los procesos habituales de la Universidad de Sevilla.

Se tendrán en cuenta en el control de accesos lo siguiente:

- El nivel de sensibilidad de los datos que se procesan y su nivel de control de acceso.
- La diseminación y circulación de la información almacenada por los sistemas.
- La consistencia de los perfiles de usuario a través de las aplicaciones y los sistemas operativos subyacentes
- Los requerimientos para el cumplimiento de controles legales y de reglamentos.

En el documento 03-060-30 del Anexo II, se incluye el documento formato para la relación de personal que administra los accesos a los sistemas de información, incluyendo el tipo de acceso que se autoriza para cada uno de los usuarios. Este documento se actualizará cuando existan altas, bajas o modificaciones en los usuarios de cada uno de los sistemas.

Exclusivamente las personas que figuran en este documento están autorizadas para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos. El procedimiento para solicitar el alta,

modificación y baja de las autorizaciones de acceso a los datos se hará mediante un documento en formato papel o electrónico firmado por dicho personal administrador de accesos dirigido a la persona administradora del sistema. Todo ello de acuerdo con el Art. 91.4 que dice:

"Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero."

II.3. Medidas y normas relativas a la Gestión del acceso de usuarios.

Las aplicaciones que acceden a los ficheros de datos personales deberán solamente presentar detalles del sistema una vez que el usuario se haya conectado con éxito.

Donde sea posible los login con éxito deberían proporcionar la siguiente información para verificación por el usuario:

- Fecha y hora del login anterior.
- Detalles de los intentos fallidos.
- Mostrar mensajes de advertencia de accesos no autorizados antes del login con éxito.

Los procedimientos de gestión de acceso deberán incluir lo siguiente:

- Mecanismos del control de cambios para el usuario que cambie de puesto o deje la institución.
- Mecanismos para evitar las cuentas redundantes y eliminarlas si procede.
- Procesos de autorización formales para asignar una cuenta a cada usuario.
- Mecanismos de control de cambios para autorización rápida de cambio de derechos.
- Gestión de privilegios para asegurar que un usuario está en el rango que le corresponde.
- Identificar la categoría de los usuarios que deberían tener acceso a cuentas privilegiadas.

Ciertas funciones, como la reestructuración de bases de datos, no deben estar asignadas a los operadores de manera continua. Estas funciones deben ser revocadas cuando se terminen los trabajos asociados. Se deben otorgar privilegios a las aplicaciones de red y de software según lo necesiten. El nombre de cuenta no debe mostrar sus privilegios asociados.

II.4. Medidas y normas de Control de acceso físico.

Exclusivamente el personal (nombres o puestos de trabajos) que se indica en el documento 03- 060-040 que se incluye en el Anexo II, podrá tener acceso físico a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal. Todo ello de acuerdo con el Art. 99 del Reglamento para ficheros de datos personales de nivel medio y alto.

El acceso por el personal de mantenimiento, limpieza y seguridad se hará siempre que se haya firmado las correspondientes cláusulas de prohibición de acceso a los datos. La entrada en los locales siempre se hará con la correspondiente identificación de estas personas para las tareas que se le han asignado.

Otro punto importante es el control de entradas/salidas: quienes estén autorizados a entrar no deberían poder sacar sin autorización equipos o información y habrá que controlar las entradas/salidas de las personas que porten ordenadores portátiles o dispositivos de almacenamiento y verificar el contenido de dichos dispositivos, pues podría ser una forma de fuga no autorizada de información si el usuario ha tenido ocasión de obtener copias.

II.5. Medidas y normas para el Registro de accesos.

En los accesos a los datos de los ficheros de datos personales de nivel alto, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si

ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

Los datos del registro de accesos se conservaran durante al menos dos años, de acuerdo al Art. 103.4 del Reglamento.

El responsable de seguridad revisará periódicamente la información de control registrada y elaborará un informe mensual sobre dichos registros.

II.6. Medidas y normas para la Gestión de soportes.

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, con el fin de ser inventariados y almacenados en un lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan en el documento 03- 070-20.

Los soportes informáticos se almacenarán de acuerdo a las normas contempladas en el documento 03-070-00.

Los soportes se almacenarán en un local con llave estando el acceso al mismo limitado al responsable propietario del fichero, y a las personas que expresamente éste autorice.

Los soportes no podrán salir de los locales en que están ubicados, salvo autorización del Responsable Propietario o la persona que hubiera delegado de acuerdo al siguiente procedimiento:

Se recibirá una solicitud en formato papel o formato electrónico firmada por el Responsable Propietario del Fichero, autorizando a la persona en cuestión para la entrada/salida de dicho soporte indicándose en el registro de entrada y salida de soportes la correspondiente actividad.

El registro de entrada y salida de soportes se gestionará mediante un libro de Inventario de Soportes, que podrá ser electrónico, donde se anotarán consecutivamente, para cada copia realizada, la información que figura en la etiqueta de los soportes añadiendo, en su caso, la fecha y el motivo de la baja ya sea por destrucción o reutilización y en el que deberán constar en el caso del registro de entrada de soportes los campos siguientes:

- Tipo de soporte.
- Fecha y hora.
- Emisor.
- Número de soportes.
- Tipo de información que contienen.
- Forma de envío.
- Persona responsable de la recepción que deberá estar debidamente autorizada.

Para el caso del sistema de registro de salida de soportes informáticos debe permitir conocer de forma directa o indirecta la siguiente información:

- Tipo de soporte.
- Fecha y hora.
- Destinatario.
- Número de soportes.
- Tipo de información que contienen.
- Forma de envío.

La persona responsable de la entrega deberá estar debidamente autorizada.

Los soportes correspondientes a los ficheros de nivel alto, que vayan a ser desechados o reutilizados, deberán ser previamente tratados, como se detalla a continuación, en función del tipo de soporte de forma que no sea posible recuperar la información almacenada en ellos:

- En caso de que sea un equipo que contenga uno o varios soportes: un servidor, un PC de sobremesa e incluso un equipo portátil, se debe aplicar un borrado profundo, dándole formato nuevo (la opción que físicamente lo borre, no que sólo elimine la entrada en el directorio), o bien sobrescribiendo datos aleatorios en varias pasadas, para que el contenido anterior no resulte accesible ni con mecanismos o dispositivos sofisticados.
- Si los soportes no forman parte de un equipo o son extraíbles, se pueden desmagnetizar si se trata de soportes magnéticos, o incinerar, triturar o destruir en cualquier caso.
- Si son ópticos y no regrabables se pueden triturar en equipos adecuados, o destruir.
- En todo caso, si se entregan a una entidad para mantenimiento y no ha sido posible borrarlos, o bien se intenta la recuperación o es para su destrucción, y en especial si no existe un contrato, se deben exigir cláusulas de confidencialidad, y en el caso de destrucción, la confirmación escrita.
- Hasta que se proceda al tratamiento, borrado o destrucción, los soportes estarán protegidos frente al acceso no autorizado.
- Finalmente se podrá dar de baja en el inventario, anotando el método utilizado: incinerado, entregado una empresa para destrucción, etc.

II.7. Distribución cifrada de soportes.

La distribución de soportes que contengan datos de carácter personal de los ficheros de nivel alto, se realizará teniendo en cuenta lo siguiente:

- Emplear preferentemente cifrado con claves que de acuerdo con las tecnologías del momento nos permitan mantener la más alta confidencialidad posible.
- Almacenar o eliminar la información de manera segura una vez que la información ha sido cifrada, transmitida a su destino y descifrada.
- Buscar consejo legal, cuando sea necesario, para confirmar que las técnicas de cifrado elegidas pueden usarse sin problemas legales, puesto que la legislación de algunos países no permite la utilización de ciertos tipos de codificaciones ni su exportación a otros países.

II.8. Medidas y normas relativas a los Ficheros temporales.

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

II.9. Medidas y normas relativas a las Copias de seguridad.

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el documento 03-120-00 del Anexo II se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Las recuperaciones de datos de los ficheros de nivel alto deberán ser autorizadas por escrito por el responsable propietario del fichero.

En los ficheros de nivel alto se conservará obligatoriamente una copia de respaldo en lugar distinto en donde se encuentra el sistema y el fichero de datos en producción.

II.10. Medidas y normas para la realización de Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado. En el documento 03-140-00 del Anexo II se describe el procedimiento para realización de pruebas.

II.11. Acceso y transmisión de datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el Responsable Propietario del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- Cualquier ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero.
- Deberá garantizarse el nivel de seguridad correspondiente al fichero tratado.
- La seguridad abarcará tanto los extremos, ubicación del fichero, como terminales o dispositivos desde los que se accede o donde aparecen resultados visuales o impresos, así como en los procesos de transmisión, para lo que se aplicarán otros apartados del Documento de Seguridad que puedan ser aplicables.
- En el caso de encargados de tratamiento existirán contratos que cumplan el Art. 12 de la LOPD y se especificarán las medidas de seguridad a cumplir.
- En otros casos que no entren en la categoría anterior, existirán también medidas de seguridad adecuadas en cuanto accesos y autenticación, y salvaguardas en su caso, así como compromisos de confidencialidad, y también respecto a la devolución/destrucción de datos una vez finalizado el trabajo o según las condiciones que se determinen y de no realización de copias no autorizadas, o no modificación de datos sin autorización, según los casos.

La transmisión de datos de carácter personal de los ficheros de nivel alto, se realizará teniendo en cuenta lo siguiente:

- Emplear cifrado a gran escala siempre que sea posible ya que la falta de capacidad de procesamiento de los sistemas podría suponer una limitación.
- Almacenar o eliminar la información de manera segura una vez que la información ha sido cifrada, transmitida a su destino y descifrada.
- Buscar consejo legal, cuando sea necesario, para confirmar que las técnicas de cifrado elegidas pueden usarse sin problemas legales, puesto que la legislación de algunos países no permite la utilización de ciertos tipos de codificaciones ni su exportación a otros países.

CAPÍTULO III. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

El personal afectado además del Responsable Propietario del Fichero según la normativa se clasifica en tres categorías:

- Administradores del sistema, encargados de administrar o mantener el entorno operativo del Fichero. Este personal deberá estar explícitamente relacionado en el correspondiente documento,

ya que por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos saltándose las barreras de acceso de la Aplicación.
- Usuarios Autorizado del Puesto de Trabajo (UAPT), o personal que usualmente utiliza el sistema informático y la documentación en papel correspondiente al Fichero, y que también deben estar explícitamente relacionados en el correspondiente documento.
- Responsable de Seguridad.

Cualquier otro perfil de personal que se determine por los Responsables Propietarios de los ficheros de datos personales de la Universidad de Sevilla, debe recogerse las funciones y obligaciones de los mismos en el Documento de Seguridad.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en los correspondientes Anexos para cada fichero.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

- Se determinará las personas autorizadas para enviar la información sobre seguridad tales como circulares, recordatorios, nuevas normas leyes, etc…
- En función del perfil del personal de la Universidad de Sevilla las personas autorizadas enviarán en formato papel o electrónico aquella información de seguridad que le concierna. Es de interés establecer mecanismos de acuse de recibo de esta información.
- En función del perfil del personal de la Universidad de Sevilla el personal autorizado enviará las normas nuevas que se establezcan en materia de seguridad en datos personales y las consecuencias de su incumplimiento. Es de interés establecer mecanismos de acuse de recibo de esta información.
- Se establecerán sesiones de concienciación del personal para dar a conocer la necesidad de cumplir tanto los requerimientos legales, la Política de Seguridad Corporativa y la Política de Uso Aceptable.

CAPÍTULO IV. FUNCIONES Y OBLIGACIONES DEL PERSONAL

IV.1. Funciones y obligaciones de carácter general.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla. Constituye una obligación del personal notificar al responsable del fichero o de seguridad en su caso las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Capítulo V. Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Según el Art. 91.2 del Reglamento será preciso relacionar todos aquellos puestos de trabajo cuyos titulares tengan acceso a los ficheros que contengan datos de carácter personal con el nombre de la persona que ocupa el puesto.

En el caso de que una misma función sea desarrollada por varias personas, la función se describirá una sola vez apareciendo al lado el nombre de todas aquellas personas que la realicen. La relación nominativa se puede realizar al no ser numerosa la parte de la plantilla que tiene acceso a estos ficheros y la poca movilidad de ésta. En otro caso habría que dar un código a cada una de las funciones y

asignar éste a cada persona que le corresponda.

A continuación se pasa a detallar cada una de las funciones y obligaciones de los diferentes actores que participan en la seguridad de los ficheros de datos de carácter personal.

IV.2. Funciones y obligaciones de los Responsables de ficheros automatizados.

El responsable del fichero o la persona en quien estén delegadas sus funciones tendrá las siguientes competencias y obligaciones respecto a las medidas de seguridad en relación con los ficheros de nivel básico:

- Deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal en los términos establecidos en el Reglamento.
- Autorizar la ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero.
- Elaborará el Documento de Seguridad.
- Adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias a que daría lugar su incumplimiento.
- Se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al Sistema de Información.
- Establecerá los procedimientos de identificación y autenticación para dicho acceso.
- Establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Será quien únicamente pueda autorizar la salida fuera de los locales en que esté ubicado el fichero de soportes informáticos y documentos que contengan datos de carácter personal.
- Verificará la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

Para los ficheros declarados de nivel medio y alto de medidas de seguridad deberá además de:

- Designar uno o varios responsables de seguridad.
- Adoptará las medidas correctoras necesarias en función de lo que se exponga en el informe de auditoria.
- Establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al Sistema de Información y la verificación de que esté autorizado.
- Autorizar por escrito la ejecución de los procedimientos de recuperación.

IV.3. Funciones y obligaciones de los Responsables de Seguridad.

- Pueden ser uno o varios (tecnológico y funcional).
- Coordinará y controlará las medidas definidas en el Documento de Seguridad.
- No tiene delegada la responsabilidad que le corresponde al responsable del fichero.
- Analizará los informes de auditoria.
- Elevará las conclusiones del análisis al responsable del fichero.
- Controlará los mecanismos que permiten el registro de accesos.
- Revisará periódicamente la información de control registrada.
- Una vez al mes elaborará un informe de las revisiones realizadas en el registro de accesos.

IV.4. Funciones y Obligaciones de los Responsables Propietarios de Ficheros.

Los Responsables Propietarios de los ficheros asumen todas y cada una de las funciones y obligaciones que tienen los Responsables de ficheros automatizados reflejadas en la sección IV.2

A) Responsables Propietarios de Ficheros de Nivel Bajo. Funcional.

Inscripción/Modificación del fichero.

Deberá rellenar los formularios de declaración/modificación del fichero de datos personales para su publicación en el BOJA y ante la Agencia de Protección de Datos. Indicando finalidad, contenido y usos del tratamiento.

Recogida de datos personales.

Deberá tener en cuenta la calidad de los datos.

Informar a los interesados (a quienes se le solicitan datos) de modo expreso, preciso e inequívoco:

- De la existencia del fichero de datos personales, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a preguntas planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Todos los impresos y formularios Web de recogida de datos deben contener una leyenda donde se informe a los afectados acerca de los extremos exigidos por el Art. 5.1 de la LOPD para los supuestos de recogida de datos personales del propio afectado.

Acceso Físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los puestos de trabajo desde los que se acceden a los sistemas de información con datos de carácter personal.

Cancelación de Datos.

Los datos de carácter personal serán cancelados (no conservados) cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Acceso a Datos Personales.

- Determinar y registrar las personas que tienen acceso autorizado a aquellos datos y recursos que precisen para el desarrollo de las funciones de los usuarios. Para ello debería de haber perfiles no lineales.
- Comunicar los datos de dichas personas al Responsable Propietario de Nivel Bajo Tecnológico.

Registro de Incidencias Funcionales.

- Se debe registrar: El tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma. Además se deberán consignar, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y , en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
- Autorizar por escrito, por delegación del responsable del fichero, la ejecución de los procedimientos de recuperación de los datos.

B) Responsables Propietarios de Ficheros de Nivel Bajo. Tecnológico.

Identificación y Autenticación.

- Determinar el personal que será administrador de acceso. Debe informarse de ello al Responsable Propietario. Funcional.
- Permitir el acceso a las personas que le indique el Responsable Propietario de Nivel Funcional.
- Se establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Disponer de un timeout por tiempo de inactividad.
- Si es con contraseña, habrá un sistema de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
- Las contraseñas se cambiarán con la periodicidad de al menos cada 12 meses y mientras estén vigentes se almacenarán de forma ininteligible.

Soportes (Entrada/Salida y Desecho/reutilización).

- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido a personal autorizado para ello en el documento de seguridad.
- Autorizar, por delegación del responsable del fichero, la salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero.
- Se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en ellos, previamente a que se proceda a su baja en el inventario.

Registro de Incidencias Tecnológicas.

- Se debe registrar: El tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma. Además se deberán consignar, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
- Autorizar por escrito, por delegación del responsable del fichero, la ejecución de los procedimientos de recuperación de los datos.

Acceso Físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Copias de respaldo y recuperación.

- Llevar a cabo procedimientos que garantizarán la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
- Realizar copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.
- Conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que estén los equipos informáticos que los tratan

C) Responsables Propietarios de Ficheros de Nivel Medio.

Además de todas las funciones y responsabilidades definidas anteriormente los responsables propietarios de ficheros de Nivel Bajo deben añadir las siguientes:

Designar Responsable de Seguridad del fichero.

Deberá designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el fichero. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o bien diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Realizar Auditoría Bienal.

Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad establecidas en el título VIII del Reglamento.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Establecer sistemas de registros de entrada/salida de soportes.

Debe establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de soporte o documento, la fecha y hora, el emisor, el número de soportes o documentos incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

D) Responsables Propietarios de Ficheros de Nivel Alto. Funcional.

Además de todas las funciones y responsabilidades definidas anteriormente para los Responsables Propietarios de Nivel Bajo. Funcional y Medio deben añadir las siguientes:

Sistemas de gestión y distribución de soportes.

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o

manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos

Copias de respaldo y recuperación en lugar diferente.

Si el fichero es de nivel alto, el responsable de las copias de respaldo y recuperación, deberá conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Transmisión segura de datos de carácter personal de nivel alto.

Se hará a través de redes de telecomunicaciones cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

E) Responsables Propietarios de Ficheros de Nivel Alto. Tecnológico.

Sistemas de gestión y distribución de soportes.

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Copias de respaldo y recuperación en lugar diferente.

Si el responsable de las copias de respaldo y recuperación, deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Registro de accesos.

- De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido (mínimo 2 años).
- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos.

Copias de respaldo y recuperación en lugar diferente.

Si el responsable de las copias de respaldo y recuperación, deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Transmisión de datos de carácter personal de nivel alto.

Se hará a través de redes de telecomunicaciones cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

IV.5. Funciones y Obligaciones para los Responsables Propietarios de los ficheros de datos personales mixtos (automatizados y en papel).

Será de aplicación lo establecido anteriormente para los ficheros automatizados, con las correspondientes peculiaridades.

Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Copia o reproducción.

La generación de copias o la reproducción de los documentos únicamente podrá realizarse bajo el control del personal autorizado en el documento de seguridad.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Acceso a la documentación.

El acceso a la documentación se limitará exclusivamente al personal autorizado.

Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Para ficheros no automatizados de nivel de SEGURIDAD ALTO, además de lo anteriormente previsto se debe tener en cuenta:

Almacenamiento de la información.

Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

IV.6. Administradores y Personal Informático.

Funciones y obligaciones generales.

- Realizar el mantenimiento preventivo periódico a todos los equipos, dispositivos electrónicos y conexiones de red.
- Mantener y administrar las cuentas de usuario de todas las aplicaciones que utiliza el usuario (Active Directory, Correo electrónico, sistema telefónico, sistemas propios, etc.).
- Elaborar e implementar un plan de copias de seguridad de toda la información de carácter personal del fichero almacenada en los servidores y en los equipos personales establecidos.
- Elaborar e implementar políticas de seguridad informática interna y externa de la red.
- Administrar las diferentes aplicaciones servidoras y los sistemas gestores de base de datos.
- Participar activa y técnicamente en el desarrollo de software y atender nuevos requerimientos de las aplicaciones propias.
- Capacitar al personal en el uso de aplicaciones propias y adquiridas y en políticas de uso aceptable de los recursos informáticos.
- Evaluar nuevas tecnologías emergentes para la posible aplicación de las mismas en el tratamiento de datos personales.

Entorno de sistema operativo y de Comunicaciones.

Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado en el correspondiente documento de acceso al Fichero. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del Fichero, como los llamados "queries", editores universales, analizadores de

ficheros, etc., que deberán estar bajo el control de los administradores autorizados relacionados en el correspondiente documento.

El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso y si fuera el fichero de nivel alto deberá guardarse en lugar diferente a donde se encuentran los sistemas de tratamiento.

Sistema Informático o aplicaciones de acceso al Fichero.

Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

Salvaguarda y protección de las contraseñas personales.

Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determine, pero nunca superior a un año. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

El archivo donde se almacenen las contraseñas deberá estar protegido para conservar la confidencialidad e integridad y estará bajo la responsabilidad del administrador del sistema.

Procedimientos de respaldo y recuperación.

Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el apartado II.9 de este documento.

IV.7. Puestos de trabajo.

Antes de tomar posesión del puesto de trabajo.

Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que debería conocer la correspondiente normativa en protección de datos personales española: Ley 15/1999, Reglamento RD 1720/2007 y Documento de Seguridad de la Universidad de Sevilla (US) ya que el cumplimiento legal es responsabilidad de cada usuario autorizado. Cada uno de ellos firmará un recibí del Documento de Seguridad de la US antes de tomar posesión del puesto de trabajo.

Durante el desempeño de la función correspondiente en el puesto de trabajo.

Protección de datos personales en formato papel:

- Los usuarios autorizados de los puestos de trabajo (UAPT) deben realizar o solicitar al servicio correspondiente el cierre con llave de los despachos al abandonar en último lugar los mismos.
- Los UAPT deben dejar los informes, expedientes y listados con datos personales siempre en un armario o archivador cerrado con llave cuando no se encuentre en el puesto de trabajo.

- Los UAPT deben tener precaución con los documentos con datos personales que se dejen en fotocopiadoras, fax, encima de la mesa no son accedidos por personal no autorizado.
- Los UAPT no deben ceder ni comunicar nunca datos personales a otras Administraciones, Entidades o Particulares sin autorización del Responsable Propietario del Fichero.
- Para la destrucción de documentos o listados que contengan datos personales en soporte papel, deberán utilizar la destructora de papel con un nivel DIN adecuado de la destructora, para datos de nivel alto deberá ser 4 o 5 y para otros datos el nivel debería ser 3.

Protección de datos personales en formato digital:

- Los UAPT garantizarán que la información que muestran los sistemas informáticos no pueda ser visible por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras u cualquier otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
- Cuando el UAPT abandone su puesto de trabajo, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización y acceso a los datos personales protegidos. Esto podrá realizarse a través de un protector de pantalla que impida dicha visualización y/o acceso. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos.
- Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de fichero, los responsables de cada puesto deberán preocuparse de retirar los documentos conforme vayan siendo impresos.
- Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el Responsable Propietario del fichero, quedando constancia de esta modificación en el Registro de incidencias.
- Si la identificación/autenticación se realiza mediante contraseñas, éstas tienen carácter personal e intransferible, por lo que no pueden compartirse, deben cambiarse periódicamente, es recomendable cambiarla cada tres meses y obligatoriamente cada año y deben cumplir la Política de contraseña establecida en el Documento de Seguridad de la Universidad de Sevilla. En caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá notificarlo como incidencia y proceder a su cambio.
- Cuando se sustituya un ordenador, debe solicitarse al servicio correspondiente el borrado o destrucción segura de los datos personales que contiene. También de cualquier otro soporte informático que contenga datos personales y se vaya a desechar.
- El UAPT debe comunicar al Responsable Propietario del fichero o la persona responsable de ello según el Documento de Seguridad de la US sobre cualquier incidencia que detecte y que pueda afectar a la seguridad de los datos de carácter personal (pérdida de expediente, pérdida de listado, pérdida de soporte informático con datos personales, robo de contraseña, pérdida de la integridad de los datos, etc.). El Responsable Propietario del fichero o la persona responsable de ello deberá proceder al registro de dicho incidente de seguridad.
- Los UAPT que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos.

- En la mayoría de los ficheros se encuentran metadatos, el usuario del puesto de trabajo debe evitar que estos sean conocidos por personas no autorizadas a dichos metadatos.
- Todo fichero temporal con datos personales debe ser borrado o destruido de forma segura cuando deje de ser necesario y mientras se esté utilizando se debe garantizar el nivel de seguridad correspondiente al tipo de dato personal tratado.
- Los UAPT deben facilitar el ejercicio de los derechos de los interesados (Cláusulas de información y ejercicio de derechos ARCO) comunicándoles a estos que deben ejercerlos ante el Gabinete Jurídico de la Universidad de Sevilla, además a requerimiento de éste debe facilitar los datos correspondientes a este Gabinete para dar respuesta los interesados.
- Los UAPT pueden ser observado a través de la cámara de los dispositivos informáticos sin que lo sepa. Por tanto es recomendable utilizar una pegatina para tapa la cámara cuando no se utilice.
- Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo la autorización del Responsable de seguridad o por administradores autorizados.
- El UAPT debe cancelar los datos personales cuando hayan dejado de ser necesarios y pertinentes para la finalidad para cual fueron recabados y siempre que no exista ley al respecto que obligue a su conservación.
- Las personas autorizadas a entrar en las instalaciones donde se almacenan/tratan datos personales no deberán poder sacar de las mismas, sin autorización del Responsable Propietario, del fichero equipos o información.
- Los UAPT deben mantener actualizado el software que dispone en su puesto de trabajo (sistema operativo, aplicaciones corporativas, antivirus…) y comprobar que no tiene instalado nuevos dispositivos hardware que desconozcas su utilidad (keyloggers, memorias USB…).
- Uso de dispositivos móviles (tablet y smartphone): No está autorizado de forma general el uso de dispositivos móviles para el tratamiento de datos personales. Si el UAPT estuviera autorizado por el Responsable Propietario del Fichero para usar dispositivos móviles debe comprobar que la configuración del dispositivo móvil es segura (Se puede usar de forma gratuita la herramienta Conan Mobile del INCIBE) y si se trasladan datos de nivel alto estos deben ir cifrados en el dispositivo móvil.
- Uso de redes wifi inseguras: No está autorizado de forma general el uso de redes wifi inseguras para el tratamiento de datos personales. Pues estas redes no disponen de clave y envían los datos (incluyendo nombre de usuario y contraseña) sin ningún cifrado ni protección y los hace accesibles a cualquier persona con ciertos conocimientos informáticos.
- Uso de Cloud Computing (Computación en la nube): No se puede usar para el tratamiento de datos personales recogidos en los ficheros de la US mientras la Universidad de Sevilla no establezca el correspondiente contrato de tratamiento de datos personales por terceros y se determine si hay transferencia internacional de datos personales.
- Uso de las redes sociales: No se pueden usar para el tratamiento de datos personales recogidos en los ficheros de la US mientras la Universidad de Sevilla no establezca el correspondiente contrato de tratamiento de datos personales por terceros y se determine si hay transferencia internacional de datos personales.
- Protección contra etiquetas RFID: Si no se encuentra autorizado no se puede acceder a etiquetas que contengan datos personales de los ficheros contenidos en la US, y si se encuentra autorizado podrá acceder a los datos personales de la misma para las funciones declaradas en el fichero

correspondiente, pero no se puede realizar el rastreo de las personas que usan estas etiquetas RFID, ni usarse para el análisis de comportamientos individuales.

Al cese del usuario en la función que desempeña en el puesto de trabajo.

- Deberá devolverse todos los activos de la Universidad de Sevilla que se le asignaron para el puesto de trabajo.
- Los permisos de acceso deben eliminarse en el mismo momento del cese en el puesto de trabajo.
- Guardar secreto de toda la información relacionada con los datos personales que ha sido tratada en la Universidad de Sevilla.

CAPÍTULO V. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

Se considerarán como "incidentes de seguridad", entre otros, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal. El procedimiento a seguir para la notificación de incidentes será:

- Comprobar que se trata realmente de un incidente de seguridad de la información y no de un error fortuito de una aplicación o del sistema operativo.
- Recordar y/o anotar la actividad que se estaba desarrollando y cómo y porqué se piensa que se trata de un incidente de seguridad e informar al servicio de gestión de incidentes correspondiente
- Ceñirse a los hechos y omitir los juicios de valor.
- No comunicar el incidente a personal ajeno a la Universidad de Sevilla para evitar fugas de información.
- No alterar el estado del sistema o sistemas implicados. Esperar a recibir una comunicación por parte del servicio de gestión de incidentes para actuar de nuevo sobre el sistema.

El usuario y el administrador son responsables de llevar a cabo los procedimientos especificados para notificar del incidente al servicio correspondiente de gestión de incidentes.

A continuación, se procederá a gestionar la incidencia de acuerdo al siguiente procedimiento de respuesta a incidentes:

- Priorizar los incidentes de seguridad existentes en base a su nivel de severidad: actividades que afecten a la salud pública, ataques a servidores críticos o a información confidencial, ataques automatizados (denegación de servicio, gusanos), nuevos ataques.
- Distribuir la carga de trabajo entre los miembros del servicio de gestión de incidentes, pero manteniendo una línea de colaboración entre ellos.
- Aplicar los procedimientos elaborados a través de la política "Identificando y recogiendo evidencias de una intrusión".
- Tomar medidas para asegurar el sistema como:
    - Desconectar el sistema de la red informática si el impacto sobre la red es nulo.
    - Modificar las reglas de los cortafuegos para que sólo permitan las conexiones estrictamente necesarias.
    - Detener las aplicaciones del sistema que no sean estrictamente necesarias.
    - Notificar a los usuarios por el método que se considere más adecuado de que se está llevando a cabo una tarea de mantenimiento.
    - Vigilar el estado del tráfico sobre el sistema en busca de conexiones desconocidas.
- Tras llegar a una conclusión sobre el análisis del sistema tomar las medidas oportunas para que vuelva a funcionar de manera normal, siempre en comunicación con el afectado.

- Modificar las contraseñas del sistema afectado como medida general ante cualquier tipo de incidente de seguridad.

El mantener un registro de incidencias es una condición que regula el Art. 90 del Reglamento y que se convierte en una herramienta indispensable para la prevención y detección de posibles ataques a la seguridad, así como la persecución de los responsables de los mismos. En el registro de incidencias se consignarán los procedimientos de recuperación de datos que afecten a los ficheros de nivel alto. En el Anexo II se incluye el formato de documento 03-080-10 para llevar a cabo dicho registro de incidencias.

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero. En el formato 03-080-20 del Anexo II se incluye los documentos de autorización por parte del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

CAPÍTULO VI. PROCEDIMIENTO DE REVISIÓN

El Documento de Seguridad ha de estar siempre al día por lo cual ha de recibir cualquier tipo de modificación que se produzca tanto desde el punto de vista técnico, organizativo como jurídico.

Ha de recoger todas las modificaciones que se produzcan tanto en el hardware como en el software así como en la estructura de los ficheros.

Asimismo aquellas modificaciones que se produzcan en las medidas de seguridad de la Universidad.

Debe incorporar las variaciones que se produzcan en los diferentes procedimientos así como los cambios que se produzcan en las funciones y obligaciones de las personas que tengan relación con los ficheros de datos de carácter personal.

Asesoría Jurídica deberá comunicar cualquier disposición sea del rango que sea que tenga que ver de algún modo con los ficheros de carácter personal teniendo especial cuidado con las disposiciones de carácter reglamentario e instrucciones de la Agencia de Protección de Datos que aparezcan.

No hay que olvidar que el mantenimiento del Documento de Seguridad es tarea de varios y no sólo de su depositario: el Servicio de Informática y Comunicaciones de la Universidad de Sevilla.

Toda revisión del Documento de Seguridad se hará conforme a lo dictado en el documento 03-130-00.

Auditoría

Para los ficheros de datos personales de nivel medio y alto de la Universidad de Sevilla se han de realizar Auditorías. La Auditoria que se realice ha de reunir las siguientes condiciones:

- Puede ser interna o externa.
- La periodicidad ha de ser al menos cada dos años.
- Se verificará el cumplimiento del Reglamento en materia de seguridad.
- El informe de auditoría dictaminará sobre la adecuación de las medidas de seguridad y controles al presente Reglamento.
- Identificará sus deficiencias y propondrá las medidas correctoras y complementarias necesarias.
- Deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
- El informe una vez analizado por el responsable de seguridad quedará a disposición de la Agencia de Protección de Datos. (Art. 96.3)

CAPÍTULO VII. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, en cuanto puedan suponer infracciones disciplinarias, se someterán al régimen disciplinario que resulta aplicable.

Para establecer el cumplimiento de lo indicado en el Documento de Seguridad se podrían realizar controles periódicos de acuerdo a lo establecido en el documento 03-090-00 del Anexo II.

APÉNDICE: LENGUAJE DE GÉNERO

Este documento ha sido redactado con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.

ANEXO I: NOMBRAMIENTOS

Para los nombramientos de las personas que serán los Responsables de Seguridad y los Responsables Propietarios de los ficheros se podrán usar los siguientes formatos:

01-010-00 Identificación del responsable de seguridad.

01-020-00 Identificación de los responsables propietarios de los ficheros.

Los documentos que contienen la información sobre los Responsables Propietarios de Ficheros vigentes se encuentran en la aplicación Web de Gestión de la LOPD, con acceso seguro.

01-010-00	IDENTIFICACIÓN DEL RESPONSABLE DE SEGURIDAD		EN VIGOR DESDE
ELABORADO POR UNIVERSIDAD DE SEVILLA	FECHA 18 DICIEMBRE 2015	APROBADO POR COMISION DE SEGURIDAD	FECHA 16 DICIEMBRE 2016

Función: Coordinación general y aspectos jurídicos

Responsable de Seguridad a efectos jurídicos: Director/a Gabinete Jurídico

División o Departamento: Gabinete Jurídico

Dirección: San Fernando, 4

Teléfono: 954.551.092

e-mail: servjuri2@us.es

Función: Coordinación general y aspectos técnicos

Responsable de Seguridad a efectos técnicos: Responsable de Seguridad Delegado/a

División o Departamento: Servicio de Informática y Comunicaciones

Dirección: Campus Reina Mercedes, s/n

Teléfono: 954.550.171

e-mail: seguridad-lopd@listas.us.es

ANEXO II: FORMATOS DE DOCUMENTOS

Para el cumplimiento de lo indicado en cada uno de los apartados de este Documento de Seguridad y de acuerdo con el Reglamento se utilizarán los siguientes formatos.

Todos estos formatos para la gestión de lo previsto en la LOPD y el Reglamento 1720/2007 se encuentran en la aplicación Web de Gestión de la LOPD, con acceso seguro.

02.- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

- 02-010-00 Inventario de hardware (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 02-020-00 Inventario de software (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).

03.- Medidas, normas, procedimientos, reglas y estándares.

- 03-060-20 Relación de personal autorizado para acceder a datos de carácter personal (A cumplimentar por los responsables propietarios. Nivel Funcional y Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-060-30 Personal administrador de accesos (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-060-40 Control de Acceso Físico (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-070-00 Procedimiento de gestión de soportes (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-070-10 Inventario de soportes (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-070-20 Autorizados para acceder al almacén de soportes (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- Registro de entrada de soportes (A cumplimentar por los responsables propietarios. Nivel Funcional y Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- Registro de salida de soportes (A cumplimentar por los responsables propietarios. Nivel Funcional y Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-080-10 Registro de incidencias (A cumplimentar por los responsables propietarios. Nivel Funcional y Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-080-20 Autorizados para hacer recuperación de datos (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-110-00 Procedimiento de control de accesos físicos.
- 03-120-00 Procedimiento de copias de respaldo (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).
- 03-140-00 Procedimiento de pruebas con datos reales (A cumplimentar por los responsables propietarios. Nivel Tecnológico, de cada uno de los ficheros de nivel alto declarados).

08.- Glosario.

- 08-020-00 Glosario de términos de protección de datos.

***