BICI

Curso 2015-2016
9 de mayo de 2016
Número 29 / Anexo IV

Boletín Interno de Coordinación Informativa

GERENCIA

- **Normativa de seguridad y buen uso del Sistema de Información de la Universidad Nacional de Educación a Distancia**

Aprobado por el Consejo de Gobierno de la UNED en su sesión de 26 de abril de 2016

Secretaría General
Negociado de Información Normativa
https://sede.uned.es/bici/

C/ Bravo Murillo,38, 28015
Tlfno.: 91 398 6023
Correo: bici@adm.uned.es

Normativa de seguridad y buen uso del Sistema de Información de la UNED

ÍNDICE

Objetivo

La Normativa de seguridad y buen uso del Sistema de Información de la UNED se elabora en el marco de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RLOPD) y el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad (en adelante ENS), modificado por el RD 951/2015, de 23 de octubre y la normativa de desarrollo en materia de seguridad de la información.

Dado que este documento trata de salvaguardar un derecho fundamental, mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el usuario que accede y trata información de carácter personal en el desempeño de sus funciones, deberá guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la UNED.

El RD 1720/2007, en su artículo 5, define los datos de carácter personal como: “Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”.

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

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

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el usuario final del sistema (tanto en el uso de la informática como en soporte papel). Por tanto éste necesita ser consciente de las situaciones de riesgo en materia de seguridad de la información y, al mismo tiempo, debe disponer de unas normas respecto al uso correcto de los sistemas informáticos a su alcance, así como de los soportes o documentos en papel y, con especial relevancia, deberá preservar la confidencialidad de la información de carácter personal que esté siendo tratada.

En consecuencia el presente documento fija las pautas de seguridad del uso del ordenador asignado al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, tanto en soporte informático como en papel.

Es fundamental que todo el personal de la UNED que utilice equipos informáticos y acceda o trate información de carácter personal para la realización de sus funciones conozca esta Normativa.

Asimismo se aplicará a cualquier otra persona o entidad externa que utilice o acceda a los recursos informáticos de la Universidad al prestar servicios a la misma.

Uso de equipos informáticos y cualquier otro dispositivo de acceso a la información

La UNED facilita a los usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo.

A modo orientativo, se enumeran a continuación algunas pautas para una utilización responsable de los recursos informáticos, teniendo en cuenta que determinadas actuaciones pueden tener implicaciones legales.

- Respetar la configuración física de los equipos no conectando otros dispositivos a iniciativa del usuario, así como no variar su ubicación.
- Mantener la configuración software de los equipos, no desinstalando o instalando programas o cualquier otro tipo de software distinto a la configuración lógica predefinida.
- Las contraseñas de acceso al equipo, al sistema y a la red, concedidas por la UNED, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. De este modo, los usuarios no deberán:
  - Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red corporativa.
  - Intentar modificar o acceder al registro de accesos.
  - Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a los ficheros.
  - En general, el empleo de la red corporativa, sistemas, equipos informáticos y cualquier medio puesto al alcance del usuario, vulnerando el derecho de terceros, los propios de la Institución o, bien, para la realización de actos que pudieran ser considerados ilícitos.
- No se podrán utilizar archivos o ficheros titularidad de la UNED para uso particular y de terceros. Por ello, no se deberá copiar o enviar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de la Universidad en ordenadores propios, *pen drives* o cualquier otro soporte informático. En caso de que así fuera necesario, serán eliminados una vez que hayan dejado de ser útiles para los fines que motivaron su creación. Asimismo, durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático de su propiedad, deberá restringir el acceso y uso de la información que obra en los mismos.
- Se establecerán medidas de protección adicionales que aseguren la confidencialidad y la seguridad de la información almacenada en el equipo cuando el usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.

Uso de la red corporativa

La red corporativa es un recurso compartido y limitado, que sirve no sólo para el acceso de los usuarios internos de la UNED a la intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas.

Los usuarios deberán cumplir las siguientes medidas de seguridad establecidas por la UNED:

- La utilización de Internet por parte de los usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como personal de la UNED o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. Se debe, por tanto, evitar la utilización que no tenga relación con las funciones del puesto de trabajo del usuario.

- No está permitido el uso de programas para compartir contenidos, con finalidades distintas a las relacionadas con el puesto de trabajo.
- El correo electrónico se considera como un instrumento básico de trabajo. El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones.
- Los envíos masivos de información así como lo correos que se destinen a gran número de usuarios serán sólo los estrictamente necesarios.
- No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia.
- La UNED podrá adoptar las medidas oportunas para asegurar el uso apropiado de los recursos telemáticos disponibles, con el fin de garantizar el servicio público encomendado.

Acceso a aplicaciones y servicios

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

Los usuarios deberán cumplir las siguientes medidas de seguridad establecidas por la UNED para el uso de aplicaciones y servicios corporativos:

- El acceso al ordenador y a las distintas aplicaciones corporativas se realizará previa identificación mediante usuario y contraseña u otro mecanismo de seguridad. Previamente deberá ser autorizado por el responsable correspondiente.
- La custodia de la contraseña es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona.
- Las contraseñas no deben anotarse, deben recordarse.
- Las contraseñas deben cambiarse periódicamente y en ningún caso será superior a un año. Los usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente.
- Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable correspondiente.
- Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones establecidas y apagar los equipos al finalizar la jornada laboral, excepto en los casos en que el equipo deba permanecer encendido.

Acceso y tratamiento de datos de carácter personal en soporte automatizado y en papel

FICHEROS AUTOMATIZADOS

La información de carácter personal contenida en ficheros informáticos deberá cumplir lo siguiente:

- **Claves de acceso al sistema informático.-** Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse de su mal uso, divulgación o pérdida. No se podrá, asimismo, emplear identificadores y contraseñas de otros usuarios para acceder al sistema informático. En caso de que fuera necesario acceder al sistema, en ausencia de un compañero, se intentará previamente contactar con él. Para el acceso será necesario, en todo caso, solicitar la autorización del responsable de la Unidad o Departamento y posteriormente el CTU habilitará el acceso eventual. Una vez finalizada la tarea que motivó el acceso, deberá ser comunicado, de nuevo, al CTU.

- **Bloqueo o apagado del equipo informático.-** Bloquear la sesión del usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esta precaución, sobre todo, deberá tenerse en cuenta, por el personal que tenga una atención directa al público.
- **Almacenamiento de archivos o ficheros en la red informática.-** Guardar todos los ficheros de carácter personal empleados por el usuario en el espacio de la red informática habilitado por la UNED, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.
- **Manipulación de los archivos o ficheros informáticos.-** Únicamente las personas autorizadas podrán introducir, modificar o anular los datos personales contenidos en los ficheros. Los permisos de acceso de los usuarios a los diferentes ficheros serán concedidos por la UNED, en concreto por el CTU. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá pedir autorización al Responsable del Fichero.
- **Generación de ficheros de carácter temporal.-** Los Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea determinada. Estos ficheros deben ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación y mientras estén vigentes deberán ser almacenados en la carpeta habilitada en la red informática. Si transcurrido un mes el usuario detecta la necesidad de continuar utilizando la información almacenada en el fichero, deberá comunicárselo al Responsable de seguridad, para adoptar sobre el mismo las medidas oportunas.
- **No utilización del correo electrónico para envíos de información de carácter personal sensible.-** No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros. Se pondrá en conocimiento del CTU para que implemente el cifrado, encriptado u otro mecanismo que salvaguarde la seguridad, la integridad y privacidad de la información.
- **Comunicación de las entradas y salidas** de soportes con datos de carácter personal (tales como discos duros, DVDs, CDs, cintas de datos,…) fuera de las instalaciones de la UNED a los Responsables de los Ficheros oportunos.
- **Comunicación de las incidencias que afecten a la seguridad del sistema de información y especialmente aquellas que afecten a los datos de carácter personal.- Comunicar al Responsable de seguridad de ficheros automatizados** las incidencias de las que tenga conocimiento, siempre que puedan afectar a la seguridad de los datos personales.
  E-mail: incidenciaslopd@adm.uned.es

  Entre otros, tienen la consideración de incidencia de seguridad que afecta a los ficheros automatizados, los supuestos siguientes:
  - La pérdida de contraseñas de acceso a los Sistemas de Información
  - El uso indebido de contraseñas
  - El acceso no autorizado de usuarios a ficheros, sin el perfil correspondiente
  - La pérdida de soportes informáticos con datos de carácter personal
  - La pérdida de datos por el mal uso de las aplicaciones
  - Ataques a la red
  - Infección de los sistemas de información por virus u otros elementos dañinos
  - Fallo o caída de los Sistemas de Información.

FICHEROS NO AUTOMATIZADOS O EN PAPEL

En relación con los ficheros en soporte papel, el usuario deberá cumplir con lo siguiente:

- **Custodiar las llaves de acceso a archivadores o dependencias.-** Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contengan soportes o documentos en papel con datos de carácter personal.
- **Cerrar los despachos o dependencias.-** En caso de disponer de un despacho, cerrar con llave la puerta al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- **Almacenamiento de soportes o documentos en papel.-** Guardar todos los documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada laboral. Cuando estos documentos no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.
- **No dejar en fotocopiadoras, faxes o impresoras documentos con datos de carácter personal.-** Asegurarse de que no quedan documentos impresos que contengan datos personales en la bandeja de salida de fotocopiadoras, impresoras o faxes.
- **Documentos no visibles en los escritorios, mostradores u otro mobiliario.-** Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.
- **Desechado y destrucción de soportes o documentos en papel con datos personales.-** No tirar soportes o documentos en papel donde se contengan datos personales a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información.
  A estos efectos, deberá ser desechada o destruida preferentemente mediante destructora de papel.
  No se deben depositar en papeleras o contenedores de papel, soportes o documentos no destruidos que contengan datos personales.
- **Archivo de soportes o documentos.-** Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de la UNED. Dichos criterios deberán garantizar la correcta conservación de los documentos, así como la localización y consulta de la información.
  Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos.
  No podrá acceder o utilizar, sin autorización, los archivos pertenecientes a otros Departamentos o Unidades que compartan la sala o dependencia habilitada para archivo.
- **Traslado de soportes o documentos en papel con datos de carácter personal.-** En los procesos de traslado de soportes o documentos deberán adoptarse las medidas dirigidas para impedir el acceso o manipulación por terceros.
- **Traslado de dependencias.**- En caso de cambiar de dependencia, en el proceso de traslado de los soportes o documentos en papel, éste se deberá realizar con la debida cautela. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier persona aquellos documentos o soportes en papel donde consten datos de carácter personal.
- **Envío de datos personales sensibles en sobre cerrado.-** Si se envían a terceros ajenos a la UNED datos especialmente sensibles (salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte o documento papel, se debe realizar en sobre cerrado por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.
- **Comunicar las entradas y salidas** de ficheros en papel con datos de carácter personal fuera de las instalaciones de la UNED a los Responsables de los Ficheros.

- **Comunicación de las incidencias que afecten a la seguridad de datos de carácter personal.-** Comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales a los Responsables de Seguridad de ficheros no automatizados:
  E-mail: incidenciaslopd@adm.uned.es
  Tienen la consideración de incidencia de seguridad, que afecta a los ficheros no automatizados o en papel, las siguientes:
  - La pérdida de las llaves de acceso a los archivos, armarios y dependencias, donde se almacena la información de carácter personal
  - El uso indebido de las llaves de acceso
  - El acceso no autorizado de usuarios a los archivos, armarios y dependencias, donde se encuentran ficheros con datos de carácter personal
  - La pérdida de soportes o documentos en papel con datos de carácter personal
  - El deterioro de los soportes o documentos, armarios y archivos, donde se encuentran datos de carácter personal

Entrada en vigor

La Normativa de Seguridad y buen uso del Sistema de Información de la UNED entrará en vigor al día siguiente de su publicación en el BICI