Memoria de Impacto Normativo[1]

Anteproyecto[2] **de REGLAMENTO SOBRE BUEN USO DEL SISTEMA DE INFORMACIÓN DE LA UNED**

Órgano proponente: Gerencia

Título de la norma: Anteproyecto de Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED

Tipo de norma: Reglamento

Objetivos: Adaptación a la legislación vigente del Reglamento ya aprobado por Consejo de Gobierno el 12 de diciembre de 2017.

Procedimiento/tramitación (Ordinario/ Urgente[3]): Ordinario

Informes (No requiere/ requiere, especificar en su caso…)**:** No requiere

Trámite de información pública y audiencia a la comunidad universitaria (10/5 días)[4]: 5 días

Comisión competente para su conocimiento tras el trámite de información pública y audiencia: Comisión de Asuntos Generales

Análisis de Impactos:

Impacto normativo (nuevo reglamento que regula una materia/modificación o derogación de reglamentos previos/modificación puntual de una norma, etc.)**:**

Este Reglamento, que fue aprobado por Consejo de Gobierno de 12 de diciembre de 2017, debía modificarse tras la publicación de la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digítales, por lo que el Comité de Seguridad de la Información de la UNED aprobó las modificaciones que se presentan con fecha 22 de noviembre de 2023.

---

[1] Modelo de Memoria de Impacto Normativo basado en el Procedimiento para la elaboración de disposiciones de carácter general de la Universidad Nacional de Educación a Distancia, aprobado por el Consejo de Gobierno de 15 de diciembre de 2020. No es preceptivo usar este modelo o seguir este esquema.

[2] La propuesta normativa de nuevo reglamento o de reglamento de reforma recibe el nombre de "Anteproyecto". Tras la audiencia pública, a la vista de las observaciones, alegaciones y sugerencias recibidas, el órgano promotor de la iniciativa procederá a la redacción definitiva de la propuesta, que pasa a denominarse "Proyecto", y que se presentará en la Comisión correspondiente junto con los informes preceptivos, o bien potestativos si se hubieran pedido. Tras su aprobación en Consejo de Gobierno pasa a ser una norma jurídica (Reglamento) y se queda únicamente con su título para su publicación en BICI.

[3] Art. 6. Procedimiento: "Cuando razones de oportunidad lo aconsejen, el/la Rector/a podrá acordar la aplicación del procedimiento de urgencia, en el que se reducirán a la mitad los plazos establecidos en las presentes normas. El/la Rector/a informará en la correspondiente sesión del Consejo de Gobierno sobre las razones por las que decidió aplicar el mencionado procedimiento de urgencia"

[4] Arts. 3 y 5 Procedimiento: 10 días procedimiento ordinario/ 5 días procedimiento de urgencia/5 días modificación puntual que no imponga obligaciones relevantes.

Otros impactos relevantes (señalar si la propuesta tiene o no, a juicio del órgano promotor, otros impactos relevantes, como impacto económico y presupuestario, impacto en materia de cargas administrativas, impacto de género, impacto en el ámbito familiar -en especial en la infancia y en la adolescencia-, impacto medioambiental, impacto en la implementación de los Objetivos de Desarrollo Sostenible, entre otros).

Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED

Aprobado por el Consejo de Gobierno, el 12 de diciembre de 2017
Modificado por el Comité de Seguridad de la Información el 22 de noviembre de 2023

#SOMOS2030

www.uned.es

Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED

Comité de Seguridad de la Información

Departamento de Política Jurídica de Seguridad de la Información

Noviembre 2023

Sumario

Preámbulo

La seguridad de la Información constituye uno de los valores fundamentales en la gestión de cualquier organización. Su aplicación 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.

En la sociedad de nuestros días vivimos en un universo digital de información y de datos. La proliferación de ordenadores, teléfonos inteligentes y la vertiginosa evolución de Internet han tenido como consecuencia una expansión, sin precedentes, de la información y de los datos de carácter personal que se gestionan. La Universidad del siglo XXI, por tanto, la UNED, tiene que afrontar este hecho, especialmente porque posee una de las bases de datos personales más importantes del país, la de los estudiantes que a lo largo de su historia han pasado por esta institución.

El Reglamento 2016/679 General de Protección de Datos (en adelante RGPD) que entró en vigor el 25 de mayo de 2016 y comenzó a ser de plena aplicación el 25 de mayo de 2018, recoge expresamente a lo largo de su articulado (entre otros en los artículos 24,25 y 32) la obligación del responsable del tratamiento de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de los tratamientos realizados. Igualmente, el artículo 28 de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD) establece también esta obligación para los responsables y encargado del tratamiento.

La Disposición Adicional Primera de la LOPDGDD indica que “El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del RGPD” y que “Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como

impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad".

El Real Decreto 311/2022, de 4 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, tiene por finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, señala en su artículo 13.h que uno de los derechos de las personas en sus relaciones con las Administraciones Públicas es: "la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas".

Del mismo modo, en su artículo 17.3 "Archivo de documentos" dispone que: "Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos".

Por ello, conocer el Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED, es uno de los pilares de la gestión de calidad de nuestra Universidad.

Título Preliminar. Objeto y ámbito de aplicación

Artículo 1. Objeto del Reglamento

La UNED tiene entre sus objetivos garantizar la seguridad de los Sistemas de Información, mediante la implantación del ENS, así como garantizar la protección de los datos de carácter personal de todas aquellas personas que con ella se relacionan: estudiantes, profesores, personal de administración y servicios y, en general, cualquier otro ciudadano que en algún momento de su vida tenga relación con nuestra institución, poniendo los medios necesarios para llevar a cabo las medidas de índole técnico y organizativo que garanticen un nivel de seguridad adecuado al riesgo que conlleva el tratamiento de la información y de estos datos de carácter personal en la Universidad.

Uno de los eslabones, normalmente, más débil 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 privacidad y 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.

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.

En consecuencia, el presente documento fija las pautas de seguridad del uso de los sistemas de información asignados 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.

Artículo 2. Ámbito de aplicación

Este Reglamento será de aplicación a todos los miembros de la comunidad universitaria que utilicen los recursos informáticos de la universidad, bien sea de forma local o remota y accedan o traten información y datos de carácter personal en soporte informático o en papel, para la realización de sus funciones.

Así mismo, 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.

Título I. Uso de los Sistemas de Información

Artículo 3. Uso de los Sistemas de Información

Los datos, dispositivos, programas y equipos informáticos que la Universidad pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones y fines previstos, debiendo constituir una herramienta de trabajo o estudio y no deben ser utilizados para fines privados.

Artículo 4. Uso de los equipos informáticos y cualquier otro dispositivo de acceso a la Información

La política de seguridad de la información comportará el cumplimiento por parte de los usuarios de las siguientes obligaciones dirigidas a una utilización responsable de los recursos informáticos.

1. Respetar la configuración física de los equipos no conectando otros dispositivos a iniciativa del usuario, así como no variar su ubicación, excepto cuando las actividades docentes o investigadoras lo justifiquen. Estas deberán ser acreditadas en caso de producirse alguna incidencia en el Sistema de Información.

2. Mantener la configuración software de los equipos, no desinstalando o instalando programas o cualquier otro tipo de software distinto a la configuración lógica predefinida, excepto cuando las actividades docentes o investigadoras lo justifiquen. Estas deberán ser acreditadas en caso de producirse alguna incidencia en el Sistema de Información.

3. 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:

   a) Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red corporativa.

   b) Intentar modificar o acceder al registro de accesos.

   c) Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a los ficheros.

   d) En general, emplear 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.

4. 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, por motivos de trabajo, 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.

5. 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.

Artículo 5. 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:

1. 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.

2. No está permitido el uso de programas para compartir contenidos, con finalidades distintas a las relacionadas con el puesto de trabajo.

3. 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, en el artículo 7 de este Reglamento.

4. Los envíos masivos de información, así como los correos que se destinen a gran número de usuarios, serán sólo los estrictamente necesarios.

5. Se evitará abrir anexos de mensajes, ficheros sospechosos o de procedencia desconocida.

6. 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.

Artículo 6. Uso de la información

La información contenida en los Sistemas de Información de la UNED es propiedad de la misma.

Los usuarios deben conocer y cumplir las normas de uso que se enumeran a continuación:

1. La información contenida en los Sistemas de Información o que circule por sus redes de comunicaciones debe ser utilizada exclusivamente para el cumplimiento de las funciones profesionales o académicas del usuario.

2. Los usuarios sólo podrán acceder a aquella información para la que posean autorización, concedida por el Centro de Tecnología de la UNED (CTU), en función del colectivo al que pertenezcan, manteniendo absoluta reserva sobre la misma.

3. Se evitará almacenar información sensible, confidencial o protegida en soportes tales como CD, DVD, memorias USB, pen drives, listados, etc., o dejar visible tal información en la pantalla del ordenador.

4. En el caso de envíos de documentación en soporte papel, que contengan datos sensibles, se deberán realizar bien en sobre cerrado si se tratase de correo interno dentro de la Universidad, o bien, por correo certificado o a través de correo ordinario que permita su completa confidencialidad, para envíos fuera de la Universidad.

5. La información se deberá almacenar 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. En el caso de los documentos en papel, se guardarán en un lugar seguro impidiendo que un tercero no autorizado pueda tener acceso.

6. Se evitará almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento de la red compartida de la UNED.

7. Los usuarios no deberán abandonar documentos que contengan datos personales en faxes, impresoras, escáneres, u otra maquinaria. Asimismo, no se dejará documentación con datos de carácter personal visible en los escritorios, mostradores u otro mobiliario, si no se estuviera utilizando.

8. En el caso de que deban transmitirse datos sensibles, confidenciales o protegidos, se cifrarán o se utilizará cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte.

9. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser destruidos, preferentemente, mediante máquinas destructoras de papel o por el procedimiento utilizado por la empresa adjudicataria de este servicio, de forma que no sea recuperable la información que pudieran contener.

10. En el caso de dar de baja dispositivos hardware, que contengan datos de carácter personal, el usuario deberá solicitar al Centro de Atención al Usuario (CAU) el borrado seguro de datos, que el técnico, autorizado por el usuario y con el V.º B.º del responsable de la unidad, realizará mediante un proceso de formateo a bajo nivel del disco duro.

11. Se comunicarán, al responsable del tratamiento, las entradas y salidas de la información contenida en dispositivos móviles (portátiles, teléfonos, tabletas) o soportes como memorias USB, CD, DVD, etc., así como documentos en papel, fuera de las instalaciones de la UNED.

12. Los ficheros temporales, creados para el desarrollo de una tarea determinada, deberán ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación y mientras estén vigentes deberán almacenarse en la carpeta habilitada en la red informática. Si transcurrido un mes, el usuario detecta la necesidad de seguir utilizando la información deberá comunicarlo al responsable de seguridad, para adoptar las medidas oportunas.

Título II. Control de accesos

Artículo 7. 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. El acceso se realizará previa identificación, mediante las claves de usuario y contraseña proporcionadas a los usuarios y, por ello, deberán cumplir con las siguientes medidas de seguridad establecidas por la UNED:

1. La custodia de la contraseña es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona.
2. Las contraseñas no deben anotarse, deben recordarse.
3. 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 crean conveniente.
4. Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable de seguridad.
5. 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.

Artículo 8. Datos de carácter personal

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, se obliga al cumplimiento del Reglamento (UE) 2016/679 General de Protección de Datos, de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales y de la normativa de desarrollo de estas disposiciones que pudiera ser de aplicación a los tratamientos de la Universidad.

Dichos deberes del usuario incluyen el deber de secreto de los datos de carácter personal y la custodia de los mismos; el deber de seguridad de los datos para evitar su alteración, pérdida, tratamiento o acceso no autorizado, el deber de no comunicación de los datos de carácter personal objeto de tratamiento a un tercero, salvo para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con previo consentimiento del interesado y el deber de diligencia ante brechas o violaciones de seguridad que pudieran ser detectadas por el usuario.

Título III. Incidencias de seguridad de la información y de los datos de carácter personal

Artículo 9. Incidencias de seguridad en los tratamientos automatizados

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de la información y a los datos de carácter personal.

Entre otros, tienen la consideración de incidencias de seguridad que afectan a los tratamientos automatizados, los supuestos siguientes:

1. La pérdida de contraseñas de acceso a los Sistemas de Información.
2. El uso indebido de contraseñas.
3. El acceso no autorizado de usuarios a ficheros, sin el perfil correspondiente.
4. La pérdida de soportes informáticos con datos de carácter personal.
5. La pérdida de información por el mal uso de las aplicaciones.
6. Ataques a la red.
7. Infección de los sistemas de información por virus u otros elementos dañinos.
8. Fallo o caída de los Sistemas de Información.

Artículo 10. Incidencias de seguridad en los tratamientos en soporte papel

Tienen la consideración de incidencias de seguridad, que afectan a los tratamientos en soporte papel, las siguientes:

1. La pérdida de las llaves de acceso a los archivos, armarios y dependencias, donde se almacena la información.
2. El uso indebido de las llaves de acceso.
3. El acceso no autorizado de usuarios a los archivos, armarios y dependencias, donde se encuentra archivada la información.
4. La pérdida de soportes o documentos en papel.
5. El deterioro de los soportes o documentos, armarios y archivos, donde se encuentra guardada la información.

Artículo 11. Comunicación de las incidencias que afecten a la seguridad del Sistema de Información y a la Protección de Datos

Una vez producida la incidencia, el usuario conocedor de la misma, debe comunicarla al Centro de Atención al Usuario (CAU) telefónicamente o a través de las direcciones: **soportePAS@csi.uned.es** o **soportePDI@csi.uned.es**. Si afectan a los datos de carácter personal pueden comunicarse también a la dirección electrónica: **incidenciaslopd@adm.uned.es**.

En las incidencias que afecten a los datos de carácter personal, se tendrá en cuenta lo siguiente:

1. Se informará al Responsable del tratamiento o en su defecto al Responsable de su Unidad.

2. En el caso de que se hayan visto afectados tratamientos con datos de carácter personal y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible que el Responsable del tratamiento autorice la ejecución del citado procedimiento: para ello el CAU deberá requerir al usuario la citada autorización.

3. Asimismo, el personal del CAU adoptará junto con el Responsable de Seguridad las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia y se evite que se pueda producir en futuras ocasiones.

4. El CAU remitirá, mensualmente, al Departamento de Política Jurídica de Seguridad de la Información un informe con las incidencias producidas que afecten a la pérdida de datos de carácter personal, a la dirección de correo electrónico: **incidenciaslopd@adm.uned.es**, para su registro.

Disposición final primera. Incumplimiento del Reglamento

Todos los usuarios de la UNED están obligados a cumplir lo prescrito en el presente Reglamento sobre Seguridad y buen uso del Sistema de Información.

El incumplimiento de este Reglamento y los posibles incidentes que puedan derivarse, serán responsabilidad del usuario, así como las implicaciones legales correspondientes.

Disposición final segunda. Entrada en vigor

El Reglamento sobre Seguridad y buen uso del Sistema de Información de la UNED entrará en vigor al día siguiente de su publicación en el BICI.