

GERENCIA

- **Política de Seguridad de la Información de la UNED**

(Aprobado por Consejo de Gobierno el 13 de diciembre 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

Ámbito: BIC - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación" (CSV) en la dirección web <https://sede.uned.es/valida/>

4159ACA0D3EDFAA08AC7A94F7ED8F5D

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNED**Gerencia**

(Aprobado por el Consejo de Gobierno de 13 de diciembre de 2016)

INTRODUCCIÓN

La Universidad Nacional de Educación a Distancia (UNED) es una institución de derecho público, dotada de personalidad jurídica y de plena autonomía en el desarrollo de sus funciones, sin más limitaciones que las establecidas en las leyes.

Desde su creación, la implantación de las Tecnologías de la Información y de las Comunicaciones (TIC) ha supuesto un gran avance en la calidad del servicio público de la educación superior que se presta.

El documento fundamental para abordar la normativa de seguridad de la UNED, es su Política de Seguridad de la Información, que establece los principios y directrices a tener en cuenta en su posterior desarrollo normativo y define la estructura organizativa de la seguridad de la información.

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del **Real Decreto 3/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad (ENS)** en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación de las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir, que será aprobada por el titular del órgano superior correspondiente.

En el Preámbulo indica que los sistemas de información de las Administraciones pretenden:

“La creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar 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.

*De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y **los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar “tierras de nadie” y fracturas que pudieran dañar a la información o a los servicios prestados**”.*

El artículo 5 del ENS, “La seguridad como un proceso integral”, señala lo siguiente:

- 1 **La seguridad se entenderá como un proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Su aplicación estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
- 2 Se prestará la máxima atención a la **concienciación de las personas** que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

En el artículo 12 “Organización e implantación del proceso de seguridad” se determina que:

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

En consecuencia, el presente documento fija los criterios básicos sobre el sistema de información de la UNED y, en concreto, las normas de uso del ordenador asignado al puesto de trabajo, la red corporativa, los equipos portátiles, las aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, tanto en soporte informático como en papel.



Asimismo, **La ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas** señala en su artículo 13, apartados a y b, los siguientes derechos de las personas:

A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración y a ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.

Por otro lado, **la ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público** preceptúa en su artículo 3 apartado 2 que:

“Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados”.

En virtud de lo expuesto, de conformidad con lo establecido, es compromiso de todos los miembros de la comunidad universitaria contribuir, desde sus respectivas responsabilidades, a la mejor realización del servicio público.

Aprobación de la Política de Seguridad de la Información de la UNED

El propósito de la presente Política de Seguridad de la Información de la UNED, es establecer las bases de la fiabilidad con que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas. En este documento se recoge el conjunto de medidas necesarias, tanto técnicas como organizativas, encaminadas a conseguir un nivel de protección adecuado con el fin de asegurar el cumplimiento legal, garantizar la disponibilidad y la confidencialidad de la información.

ÍNDICE

- I. Política de Seguridad de la Información**
- II. Misión y marco normativo de la UNED**
- III. Principios de la seguridad de la información**
- IV. Estructura Normativa**
- V. Organización de la Seguridad**
- VI. Protección de datos de carácter personal**
- VII. Gestión de riesgos**
- VIII. Formación y concienciación**
- IX. Actualización y revisión periódica**
- X. Entrada en vigor**

I.- Política de Seguridad de la Información

1.- La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

2.- La consolidación del uso de las nuevas tecnologías en la UNED, exige el establecimiento de un conjunto de actividades y procedimientos para el tratamiento y gestión de los riesgos asociados a la seguridad de la información. La gestión de la seguridad de los sistemas de información es un proceso complejo que incluye a personas, tecnologías, normas y procedimientos.

3.- La Administración Electrónica permite que cualquier ciudadano o los miembros de la comunidad universitaria puedan realizar sus trámites desde cualquier lugar y en cualquier



momento, a través del uso de técnicas y medios electrónicos, informáticos y telemáticos. De esta forma la iniciación, tramitación y terminación de los procedimientos puede realizarse, con plena validez, en plenas condiciones de seguridad, y con interoperabilidad con otras Administraciones y conforme al Esquema Nacional de Seguridad y al Esquema Nacional de Interoperabilidad, Real Decreto 3/2010 y Real Decreto 4/2010 respectivamente.

4.- La Política de Seguridad de la Información pretende dar soporte al desarrollo, coordinación y racionalización de la normativa específica y a la actualización de los conceptos según la evolución de las TIC y de la legislación vinculante y alcanzar de esta forma un conjunto normativo equilibrado y completo.

II.- Misión y Marco Normativo de la UNED

El art. 3.1 de Los Estatutos de la UNED, (R.D. 1239/2011, de 8 de septiembre por el que se aprueban los Estatutos de la Universidad Nacional de Educación a Distancia) establece como fines de la UNED, el desempeño del servicio público de la educación superior mediante la investigación, la docencia y el estudio.

La UNED reconoce como funciones esenciales de su actividad la enseñanza, el estudio, la investigación y la transferencia del conocimiento, en orden al pleno desarrollo científico, cultural, artístico y técnico de la sociedad (art.7 Estatutos).

La misión de la UNED es la de “desempeñar el servicio público de la educación superior mediante la docencia, el estudio, la investigación y la transferencia del conocimiento, asumiendo el compromiso de facilitar al máximo el acceso a la enseñanza universitaria, la continuidad de estudios y la formación a lo largo de la vida a todo tipo de personas. Todo ello mediante la aplicación de una metodología didáctica específica “a distancia” que combina las tecnologías más avanzadas con la tutorización personalizada presencial y digital”.

La derogada Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, marcó un hito significativo a la contribución de la implementación de la Administración Electrónica. Junto a este marco jurídico, podemos indicar en la tabla siguiente, otra normativa en relación a esta materia.

NORMATIVA GENERAL	OBJETIVO
Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas	Derecho de los ciudadanos a relacionarse mediante medios electrónicos con las Administraciones Públicas
Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la seguridad
Real Decreto 3/2010, Esquema Nacional de Seguridad	Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información
Real Decreto 4/2010, Esquema Nacional de Interoperabilidad	Comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección Tecnológica



Ley 59/2003, de 19 de diciembre, de firma electrónica	Regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación
Real Decreto 1553/2005, de 23 de diciembre de 2005	Regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal	Garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar
Real Decreto 1720/2007, de 21 de diciembre	Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
Decreto 2310/1972, de 18 de agosto	Creación de la UNED
R.D. 1239/2011 de 8 septiembre	Estatutos de la UNED
Cualquier otra normativa que pueda aprobarse y resulte aplicable	

III.- Principios de la seguridad de la Información

La presente Política de Seguridad de la información se basa en unos principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad que realice la Universidad. Se establecen los siguientes:

1.- Principios Básicos:

- a) **Alcance y concienciación:** Todo el personal de la Universidad debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.
- b) **Responsabilidad diferenciada:** En los sistemas de información se diferenciarán de forma clara el responsable de la información, el responsable del servicio y el responsable de seguridad. El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
- c) **La seguridad como proceso integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando cualquier actuación puntual o tratamiento coyuntural.
- d) **Gestión de riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá estar permanentemente actualizado. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad.
- e) **Profesionalidad:** La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido, en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.
- f) **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto.

2.- Principios de protección de la seguridad de la información

La presente Política de Seguridad de la Información se basa en unos principios de protección que serán las bases de las actuaciones en materia de seguridad. Se establecen para ello las siguientes directrices:



- a) **Protección de datos de carácter personal:** La UNED, adoptará las medidas oportunas para garantizar el nivel de seguridad requerido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.
- b) **Clasificación y control de activos:** Los recursos informáticos y la información de la UNED, se encontrarán inventariados, con un responsable asociado. Los inventarios se mantendrán actualizados para asegurar su validez.
- c) **Seguridad física y ambiental:** Los sistemas de información serán emplazados en áreas seguras protegidas con controles de acceso físicos adecuados al nivel de criticidad de los mismos. Los sistemas y los activos de información que contienen estarán suficientemente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.
- d) **Gestión de la seguridad en comunicaciones y operaciones:** La UNED, buscará los procedimientos necesarios para asegurar la correcta gestión, operación y actualización de las TIC, realizando una adecuada protección de la información, mediante mecanismos que garanticen su seguridad.
- e) **Control de acceso:** La UNED, mediante la implantación de mecanismos de identificación, autenticación y autorización facilitará y controlará el acceso a los sistemas de información de la Universidad. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar el uso correcto.
- f) **Desarrollo y mantenimiento de los sistemas de información:** Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto, debiendo contemplarse los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información.
- g) **Gestión de la continuidad:** La UNED, establecerá un sistema de detección y reacción ante incidentes de seguridad que se produzcan y las acciones de tratamiento a seguir, para mantener la continuidad de los procesos y servicios, de acuerdo a las necesidades de los usuarios.
- h) **Cumplimiento:** La UNED, adoptará las medidas técnicas y organizativas necesarias para mantener sus sistemas de información adaptados a la normativa legal vigente, y en especial a las regulaciones legales relativas al tratamiento de datos de carácter personal, cuyas medidas específicas de tratamiento figuren en el correspondiente documento de seguridad.

IV.- Estructura Normativa

Debido a las competencias y funciones de la UNED, los temas que afectan a la seguridad de la información y su rápida evolución, resulta imprescindible la estructuración de la normativa de seguridad de la información en distintos niveles relacionados de forma jerárquica:

- 1 Política de Seguridad
- 2 Normas de Seguridad
- 3 Procedimientos de Seguridad

El personal de la UNED, tendrá la obligación de conocer y cumplir las Normas y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones, así como la Política de Seguridad de la Información.

1. Política de Seguridad de la Información

Constituye el primer nivel normativo. Se recoge en el presente documento y es aprobada por el Consejo de Gobierno, a propuesta del Comité de Seguridad de la Información.

2. Normas de Seguridad de la Información

- 1 La Política de Seguridad de la Información se desarrollará por medio de la normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.



2 Las Normas de Seguridad de la Información tienen aplicabilidad en toda la UNED, siendo el Consejo de Gobierno, el órgano responsable de la aprobación de las Normas.

3. Procedimientos de Seguridad de la Información

Los Procedimientos de Seguridad de la Información, están constituidos por instrucciones de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios. Serán aprobados por el Comité de Seguridad de la Información de la UNED.

V.- Organización de la Seguridad

Todos y cada uno de los usuarios de los sistemas de información de la UNED, son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Los cargos y puestos de trabajo que intervienen en la seguridad de la información de la UNED son los siguientes:

Gerente de la UNED	Responsable de la Información
Vicerrector de Medios y Tecnología	Responsable de Seguridad de la Información
Vicegerente de RR.HH. y organización	Responsable del Servicio
Subdirector de los servicios al usuario	Responsable del Sistema
Director del CTU	
Secretaria General	
Jefa del Dpto. de Política Jurídica de Seguridad de la Información	
Administrador de la Seguridad del Sistema	
Asesor de Seguridad	
Jefa de la Sección de Protección de Datos	

La resolución rectoral con el nombramiento de los miembros del Comité de Seguridad de la Información de la UNED, figura en el ANEXO I.

VI.- Protección de datos de carácter personal

La legislación sobre protección de datos de carácter personal establece una serie de responsables con funciones específicas.

- Los Responsables de Ficheros de la UNED son los órganos que para cada fichero se concreta en las Resoluciones en las que se aprueba la creación de ficheros.
- Los Responsables de Seguridad de la UNED son el Director del Centro Tecnológico de la UNED (CTU), la Jefa del Departamento de Política Jurídica de Seguridad de la Información para los documentos en papel y la Jefa de la Sección de Protección de Datos.
- El documento de seguridad relacionado con el tratamiento de datos de carácter personal debe ser aprobado, por el Comité de Seguridad.

VII.- Gestión de riesgos

1.- Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos, de manera continua sobre el sistema de información.



2.- Se repetirá de forma regular, al menos una vez cada dos años, cuando cambie la información manejada, los servicios prestados, cuando se detecte un incidente grave de seguridad o vulnerabilidades graves.

3.- El Comité de Seguridad propondrá la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

4.- Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y de manera fundamental las guías del Centro Criptológico Nacional.

VIII.- Formación y concienciación

La UNED desarrollará, en ejercicio de la Disposición adicional primera del ENS, actividades formativas con la finalidad de concienciar a su personal en materia de seguridad de la información, difundiendo entre los usuarios la Política de Seguridad de la Información y su desarrollo normativo.

IX.- Actualización y revisión periódica

La Política de Seguridad de la Información ha de mantenerse actualizada de forma permanente con la finalidad de adecuarla al progreso de los servicios de la Administración Electrónica, evolución de las nuevas tecnologías y de los sistemas de información.

La nueva legislación aprobada que sea aplicable así como, las normas derogadas serán actualizadas en la Política de Seguridad de la UNED, por el Comité. De igual forma se procederá a actualizar el nombramiento de los miembros del Comité que se renueven por Resolución Rectoral.

X.- Entrada en vigor

La Política de Seguridad de la Información de la UNED, que se aprueba en esta Resolución, entrará en vigor a partir del día siguiente de su publicación en el BICI.



ANEXO I

Este Rectorado, en uso de las atribuciones conferidas por el artículo 99 v) de los Estatutos de la Universidad y los artículos 10 y 29 del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ha resuelto nombrar a los miembros del Comité de Seguridad de la Información de la UNED y la función a desempeñar en el mismo.

Paloma Centeno Fernández	Responsable de la Información	Presidenta del Comité
M.ª del Carmen García Llamas	Reponsable de la Seguridad de la Información	Vocal
José Matías Hernández Sánchez	Responsable del Servicio	Vocal
José Calvo Calvo	Responsable del Sistema	Vocal
Joaquín Javier Gil Lasa	Director del CTU	Vocal
Beatriz Badorrey Martín	Secretaria General o persona en quien delegue	Vocal
Paz San Segundo Manuel	Jefa del Departamento de Política Jurídica de Seguridad y Protección de Datos	Vocal
Antonio Ruipérez García	Administrador de la Seguridad del Sistema	Vocal
Francisco Javier Martínez Martínez	Asesor de Seguridad	Asesor (con voz y sin voto)
Rosa Maján Martínez	Secretaria del Comité	Secretaria del Comité (con voz y sin voto)

Sin perjuicio de la asistencia de los miembros antes citados, podrán asistir otros cargos o técnicos de la Universidad al Comité de Seguridad de la Información, cuando se trate de temas relacionados con el Esquema Nacional de Seguridad.

Madrid, a 3 de octubre de 2016. EL RECTOR. Fdo.: Alejandro Tiana Ferrer.

