INTRODUCCIÓN

La seguridad de la información constituye uno de los valores fundamentales en la gestión de cualquier organización. Su aplicación es compleja, porque abarca 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y de garantía de los derechos digitales (en adelante LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RLOPD), imponen la obligación a las empresas y organismos, tanto públicos como privados, de establecer unas medidas de seguridad destinadas a garantizar la protección de los datos de carácter personal contenidos en ficheros automatizados o en formato papel.

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, 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 permitan 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”.

Este Reglamento se fundamenta en la siguiente normativa aprobada por la UNED:

a) Reglamento de seguridad y buen uso del sistema de información de la UNED (BICI 30 de enero de 2018, Anexo I)
b) Normativa de seguridad y buen uso de la información de la UNED (BICI 9 de mayo de 2016, anexo IV)

Objeto y ámbito de aplicación

Artículo 1. Objeto del Reglamento.

El Centro a la UNED en Illes Balears, en adelante UNED-Illes Balears, 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 de enseñanza regladas y no regladas, conferenciantes, profesorado tutor y personal de administración y servicios.

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, este 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.

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 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.

Artículo 2. Ámbito de aplicación.

Esta instrucción será de aplicación a todos los miembros de la comunidad universitaria de UNED-Illes Balears que utilicen los recursos informáticos de este centro asociado, bien sea de forma local o remota y accedan o traten información de carácter personal en soporte informático o en papel, para la realización de sus funciones.

Así mismo, es de aplicación 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 los Sistemas de Información

Artículo 3. Uso de los Sistemas de Información.

Los datos, dispositivos, programas y equipos informáticos que UNED-Illes Balears 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 formativas lo justifiquen y previa autorización.

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 y previa autorización. 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 organización, 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 UNED-Illes Balears 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 del centro 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 del Centro 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:

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 del Centro o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. La utilización que no tenga relación con las funciones del puesto de trabajo del usuario, necesita autorización previa de los responsables.

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 estas instrucciones.

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. El Centro 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 del Centro es propiedad del mismo. 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.

3. Se evitará almacenar información sensible, confidencial o protegida en soportes tales como CDs, DVDs, 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 por correo certificado o a través de correo ordinario que permita su completa confidencialidad, para envíos fuera del Centro.

5. Los usuarios no deberán abandonar documentos que contengan datos personales en faxes, impresoras, escáneres u otra maquinaria. Asimismo, no se dejará documentación visible en los escritorios, mostradores u otro mobiliario.

6. 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.

7. 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.

8. En el caso de dar de baja dispositivos hardware, que contengan datos de carácter personal, el usuario deberá solicitar el borrado seguro de datos al Centro.

9. Se comunicarán al responsable del fichero las entradas y salidas de la información contenida en dispositivos móviles (portátiles, teléfonos, tablet) o soportes como memorias USB, CDs, DVDs, etc., así como en soporte papel, fuera de las instalaciones del Centro.

10. 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.

Control de accesos

Artículo 7. Acceso a aplicaciones y servicios.

El acceso a programas informáticos corporativos 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:

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 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y de garantía de los derechos digitales (en adelante, LOPD); y del Real Decreto 1720/2007, de 21 de diciembre (BOE del 19 de enero de 2008), por el que se aprueba el Reglamento de desarrollo de la LOPD.

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.

Incidencias de seguridad de la Información

Artículo 9. Incidencias de seguridad de ficheros automatizados.

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de la información.

Entre otros, tienen la consideración de incidencias de seguridad que afectan a los ficheros 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 de ficheros en papel.

Tienen la consideración de incidencias de seguridad, que afectan a los ficheros en 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.

1. Una vez producida la incidencia, el usuario conocedor de la misma, debe comunicarla a la dirección del centro presencialmente o por mail: director@palma.uned.es info@palma.uned.es

2. Informará al Responsable del fichero.