Documento de medidas de seguridad en el tratamiento de datos personales en CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA conforme al Reglamento EU 2016/679

Conforme a:	Reglamento EU 2016/679 (Reglamento General de Protección de Datos, **RGPD**),
Versión del documento:	Gen. 18-09-2018
Autor:	PRODAT © 2017 SIGPAC® AVISO: El presente documento refleja la situación, medidas y controles a aplicar en el ámbito del RGPD por parte de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA y ha sido redactado específicamente por PRODAT® para la entidad.

Índice de contenidos

1. Objeto del documento de medidas seguridad

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) establece en su artículo 9 el principio de seguridad, según el cual "reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamientos de datos".

El 19 de enero de 2008 se publicó el Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RDLOPD) y se establecen las medidas de seguridad a cumplir para sistemas de información, ya sean automatizados o manuales.

El Reglamento (UE) 679/2016 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD) establece en su artículo 32, relativo a la seguridad de los datos personales, la obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Este riesgo debe valorarse de acuerdo con el estado de la técnica, los costes de aplicación, la naturaleza de los datos, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Estas medidas de seguridad de los tratamientos incluyen, entre otros aspectos:

1. la seudonimización y el cifrado de datos personales

2. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

3. la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

4. un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En este documento se detallan las medidas de seguridad y los mecanismos de verificación periódica que asumen tanto CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA como los encargados del tratamiento que éste designe, y son de obligado cumplimiento para cualquier persona que actúe bajo la autoridad del responsable o del encargado y que tenga acceso a los datos personales.

Asimismo, este documento da cumplimiento a lo establecido en el título VIII del RDLOPD, referente a las medidas de seguridad de obligado cumplimiento para todo el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información, hasta el 25 de mayo de 2018 y en todo caso mientras esta regulación sea aplicable.

Debido a la continua evolución y cambios intrínsecos de los sistemas de información y a la propia complejidad de la organización, el documento intentará ser un marco estable y, a su vez, flexible, en lugar de una descripción estática, en cuyo caso se vería sometido a continuas actualizaciones. En esta línea, el documento puede incluir referencias a otros documentos y políticas de seguridad establecidas en la organización y, en ocasiones, en lugar de incluir relaciones estáticas se describe el procedimiento para obtener dichas relaciones en el momento en que sean necesarias.

El presente documento se mantendrá en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en los sistemas de información o en la organización de los mismos.

De igual forma, el presente documento se adecuará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

1.1. Niveles de seguridad de los tratamientos de datos personales

El RGPD establece categorías de datos que en función de su naturaleza suponen un mayor riesgo para los derechos y liberales de las personas. Estos datos son los que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos genéticos, datos biométricos

dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Este documento de medidas de seguridad mantiene los niveles de seguridad establecidos en el RDLOPD, con las medidas de seguridad de nivel **básico** a aplicar en todos los casos, las medidas de nivel **medio** para tratamientos que revelen el comportamiento o perfil así como para el tratamiento de datos relativos a infracciones administrativos, y el nivel **alto** para el tratamiento de datos de categorías especiales, datos relativos a infracciones penales y datos relativos a víctimas de violencia de género.

El RDLOPD establece las medidas obligatorias que deben implantarse para el tratamiento de datos personales clasificadas en tres niveles de seguridad, en base a las tipologías de datos tratadas, correspondiendo el **nivel alto** a los datos más críticos y sobre los que se exigirá un mayor grado de protección:

En todo caso estos niveles de seguridad no son estáticos sino que se aplicarán en función del resultado de un análisis de riesgos en materia de seguridad de la información. De este análisis de riesgos se desprenderán medidas adicionales o alternativas a las especificadas en cada nivel.

Tratamientos con nivel de seguridad básico	Las medidas de nivel de seguridad básico se aplicarán a todos los tratamientos de datos de carácter personal
Tratamientos de nivel de seguridad medio	Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: ● Los relativos a la comisión de infracciones administrativas. ● Los contenidos en ficheros de solvencia patrimonial o crédito. ● Aquéllos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. ● Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. ● Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. ● Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
Tratamientos de nivel de seguridad alto	Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes tratamientos de datos de carácter personal: ● Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual u orientaciones sexuales. ● Los datos genéticos ● Los datos biométricos dirigidos a identificar de manera unívoca a una persona física ● Los relativos a la comisión de infracciones penales. ● Los que se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. ● Aquéllos con datos derivados de actos de violencia de género.
Excepciones	● Podrán implantarse las medidas de seguridad de nivel básico en los tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

	● En caso de tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando: ● Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. ● Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. ● A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad consistente en la llevanza de un registro de accesos a los datos. ● Cuando en un sistema de información existan tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de medidas de seguridad.

Los niveles de seguridad son acumulativos en el sentido de que en el nivel de seguridad medio deben aplicarse además todas las medidas de nivel básico, y en el nivel de seguridad alto deben aplicarse además todas las medidas de nivel básico y nivel medio.

El nivel de seguridad correspondiente a los tratamientos objeto del presente documento de medidas de seguridad es únicamente el nivel básico, por lo que se han excluido del documento las medidas correspondientes a los otros niveles, a efectos de simplificar al máximo el mismo.

1.2. Modalidades de tratamiento

Las medidas de seguridad de este documento se han clasificado en función de la modalidad de tratamiento en:

- Medidas para tratamientos **automatizados** (informatizados)
- Medidas para tratamientos **no automatizados o manuales** (principalmente, documentación en soporte papel)

En el caso de tratamientos mixtos o **parcialmente automatizados,** es decir que presentan una combinación de las dos modalidades, serán de aplicación las medidas de las dos categorías.

El presente documento de medidas de seguridad recoge las medidas a aplicar en todos los tratamientos, tanto automatizados como manuales, con excepción de las siguientes secciones que recogen medidas específicas para cada modalidad:

- ***Sección 4. Medidas específicas para ficheros y tratamientos automatizados***
- ***Sección 5. Medidas específicas para ficheros y tratamientos no automatizados***

2. Ámbito de aplicación del documento de medidas de seguridad

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA, como consecuencia de las actividades desarrolladas dentro de su objeto social, trata datos de carácter personal, tanto de forma automatizada como no automatizada.

El ámbito de aplicación del documento de medidas de seguridad es:

- La totalidad de tratamientos recogidos en el anexo **Tratamientos de datos objeto de este Documento** así como, en su caso, los tratamientos que se describen de forma detallada en el **Registro de actividades de tratamiento** de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA, donde se indican además las medidas de seguridad a aplicar en cada caso.

- Los locales, sistemas de información y demás medios empleados para su tratamiento descritos en el anexo **Descripción de los sistemas de tratamiento**.

- Los usuarios que realizan el tratamiento, según se detalla en el anexo **Relación de usuarios y perfiles de usuario autorizados**.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los datos personales, cualquiera que sea su modalidad de tratamiento, abarcando ficheros y bases de datos, aplicaciones y herramientas de actualización o consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes, equipos informáticos, listados de trabajo y documentos en soporte papel.

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha contratado diversas prestaciones de servicios con terceras entidades que conllevan el tratamiento de datos de carácter personal de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA por parte de dichas entidades.

- El anexo **Tratamientos encargados a terceros** contiene una relación exhaustiva de estas prestaciones de servicios así como los datos tratados por cada prestador y las medidas de seguridad a aplicar.

3. Funciones y obligaciones del personal

3.1. Funciones de La Dirección

La Dirección ejecutiva debe designar a las siguientes figuras para aplicar las políticas de protección de datos y medidas de seguridad:

- Cuando así sea preceptivo, o de manera voluntaria: designar un delegado de protección de datos; en su defecto se designará a una persona como coordinadora de protección de datos.
- Designar a uno o varios Responsables de seguridad que controlarán la aplicación de medidas de seguridad.

Además corresponde a La Dirección las decisiones relativas a:

- Autorizar expresamente la ejecución del tratamiento de datos personales fuera de los locales de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA.
- Autorizar la salida de soportes fuera de los locales de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA.
- Establecer los criterios para la definición de los permisos de acceso a los sistemas de información / archivo / videovigilancia para los diferentes perfiles de la organización, función que podrá delegarse en cada Responsable de Área o Departamento .
- Designar al personal administrador de seguridad, autorizado para conceder, alterar o anular el acceso sobre los sistemas de información y archivo.

La Dirección podrá delegar estas funciones en los Delegados de protección de Datos, Coordinadores de Protección de datos y Responsables de seguridad competentes.

3.2. Delegado de protección de datos

3.2.1. Obligación de designar un delegado de protección de datos

El RGPD establece en su artículo 37 la obligatoriedad de designar un delegado de protección de datos en los siguientes supuestos:

- Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
- Cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.
- Cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales.

Asimismo, la normativa española que desarrolla el RGPD, en fase de proyecto de ley, prevé también la obligatoriedad de designar un delegado de protección de datos en los siguientes casos:

a. Los colegios profesionales y sus consejos generales, regulados por la Ley 2/1974, de 13 febrero, sobre colegios profesionales.
b. Los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006, de 3 de mayo, de Educación, y las Universidades públicas y privadas.
c. Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en la Ley 9/2014, de 9 de mayo, General de telecomunicaciones, cuando traten habitual y sistemáticamente datos personales a gran escala.

d. Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e. Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f. Los establecimientos financieros de crédito regulados por Título II de la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial.

g. Las entidades aseguradoras y reaseguradoras sometidas a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

h. Las empresas de servicios de inversión, reguladas por el Título V del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.

i. Los distribuidores y comercializadores de energía eléctrica, conforme a lo dispuesto en la Ley 24/2013, de 26 de diciembre, del sector eléctrico, y los distribuidores y comercializadores de gas natural, conforme a la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

j. Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por el artículo 32 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

k. Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l. Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

m. Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n. Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a lo dispuesto en la Ley 3/2011, de 27 de mayo, de regulación del juego.

o. Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

La normativa también establece la opción de designar un delegado de protección de datos **de manera voluntaria**.

3.2.2. Funciones del delegado de protección de datos

El RGPD establece las siguientes funciones para el delegado de protección de datos:

- informar y asesorar a CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA y a los encargados del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de las disposiciones de protección de datos de la Unión Europea o de los Estados miembros;

- supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y la supervisión de las auditorías correspondientes;

- ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD;

- cooperar con la autoridad de control (Agencia Española de Protección de Datos o la autoridad competente);

- actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos reportará directamente a la dirección ejecutiva y órganos rectores de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA

Las funciones de los delegados de protección de datos se recogerán en su nombramiento (ver ***Anexo VI. Nombramientos***).

3.2.3. Identificación del delegado de protección de datos

(Marcar la opción que proceda:)

[X] CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA no ha designado como delegado de protección de datos

[ ] CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha designado como delegado de protección de datos a:

_____

_____

[ ] La designación es voluntaria

[ ] Delegado de protección de datos interno

[ ] Delegado de protección de datos externo

[ ] Delegado de protección de datos colegial

En caso de no designarse un delegado de protección de datos, sus funciones se asignarán a un coordinador de protección de datos.

3.2.4. Comunicación del delegado de protección de datos a la autoridad de control

La designación del delegado de protección de datos, tanto si es obligatoria como si es voluntaria, se comunicará a la autoridad de control (Agencia Española de Protección de Datos o la que proceda).

3.3. Personas designadas para coordinar la protección de datos

3.3.1. Necesidad de designar personas para coordinador la protección de datos

Es conveniente designar a personas en las que se delegue la aplicación de la normativa de protección de datos en CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA especialmente en los siguientes casos:

- Cuando no exista un delegado de protección de datos en la organización
- Cuando existiendo un delegado de protección de datos, se designe a otra persona de apoyo.

Los coordinadores de protección de datos, bajo la tutela e instrucciones del delegado de protección de datos o, en su defecto, de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA y de su dirección ejecutiva, darán apoyo y coordinarán la aplicación de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA en materia de protección de datos personales.

Los coordinadores de protección de datos reportarán directamente al delegado de protección de datos o, si no lo hubiera, directamente a la dirección ejecutiva y órganos rectores de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA

3.3.2. Identificación de los coordinadores de protección de datos

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha designado a las siguientes personas para coordinar la protección de datos:

Nombre: Juan Manuel Álvarez González Función: Coordinador.

3.4. Responsables de seguridad

3.4.1. Obligación de designar un responsable de seguridad

La designación de responsables de seguridad es obligatoria mientras sea aplicable el RD 1720/2007.

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha designado uno o varios responsables de seguridad cuya función es coordinar y controlar la aplicación de las medidas definidas en el presente documento de medidas de seguridad.

3.4.2. Funciones de los responsables de seguridad

- Actualizar el documento de medidas de seguridad y adecuación del documento de medidas de seguridad a la normativa vigente.
- Mantener una relación actualizada de los usuarios del sistema, indicando sus derechos de acceso.
- Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Establecer mecanismos para evitar que un usuario acceda a datos o recursos con derechos distintos a los autorizados
- Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.
- Establecer 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.
- Autorizar por escrito la ejecución de los procesos de recuperación de los datos de ficheros de nivel básico. Para ficheros de nivel medio o alto, deberá solicitar la autorización de la Dirección.
- Mantener una relación del personal autorizado para conceder, anular o alterar los derechos de acceso, conforme con los criterios establecidos.
- Mantener una relación del personal con acceso autorizado al lugar donde se almacenan los soportes.
- Mantener una relación del personal autorizado para acceder a los locales donde se encuentren ubicados los sistemas de información.

Las funciones de los Responsables de seguridad se recogerán en los nombramientos de los mismos (ver ***Anexo VI. Nombramientos***).

El responsable de seguridad reportará:

- al delegado de protección de datos si lo hubiera (o en su defecto personas designadas para coordinar la protección de datos)
- y también directamente a la dirección ejecutiva y órganos rectores de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA

3.4.3. Identificación de los responsables de seguridad

Responsables de seguridad y ámbitos de seguridad asignados:

Nombre y apellidos	Departamento y cargo	Perfil del responsable
JOSÉ NICOLÁS SAIZ LÓPEZ	SECRETARIO	General

3.4.4. Comunicación del responsable de seguridad a la autoridad de control

No es necesario comunicar la identidad del responsable o responsables de seguridad a las autoridades de protección de datos.

3.5. Administradores de seguridad informática, de archivo y videovigilancia

3.5.1. Funciones de los administradores de seguridad

Son las personas autorizadas para conceder, modificar o anular el acceso de los usuarios a:

- los sistemas de información (redes informáticas, ordenadores y equipos, servidores, aplicaciones, servicios en línea, etc)
- los sistemas de archivo de documentación en soporte papel
- los sistemas de videovigilancia

Deben reportar:

- Al delegado de protección de datos, si lo hubiera, o en su defecto a los coordinadores de protección de datos
- Al responsable de seguridad competente

Sus funciones también incluyen:

- Implantar las medidas de seguridad recogidas en el presente documento para aquellos sistemas de información que controlan.
- Únicamente concederán el acceso a los usuarios en base a los criterios definidos por CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA en el presente documento de medidas de seguridad y previa autorización del Responsable de seguridad competente.
- Proporcionarán semestralmente al Responsable de seguridad competente información sobre los cambios de configuración o sistemas que tengan implicaciones en la definición y aplicación de los procedimientos de copia de seguridad.

3.5.2. Identificación de los administradores de seguridad

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha designado a:

Nombre: José Manuel González Velarde Función: Coordinador del Área de Informática.

3.6. Usuarios finales de los sistemas de información, archivo o videovigilancia

3.6.1. Comunicación a los usuarios finales de la normativa de seguridad

Todos los usuarios de los sistemas de información, archivo (papel) o videovigilancia deberán aplicar las normas de seguridad necesarias para el desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Estas normas se les comunicarán de manera fehaciente y por escrito, mediante una circular interna o documento similar.

En la Circular se recogerán las principales obligaciones en materia de seguridad sobre datos de carácter personal, incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de los recursos informáticos otras finalidades diferentes de las estrictamente derivadas de desarrollo de su actividad laboral; así como la obligación de mantener el deber de secreto sobre todos los datos tratados con motivos del desempeño de su puesto de trabajo y de no comunicar los referidos datos a ninguna persona o entidad sin la autorización pertinente.

- Se incorpora a este documento de medidas de seguridad una copia de la citada Circular como ***Anexo VII. Circular de medidas de seguridad*.**

3.6.2. Funciones de los usuarios finales

Las funciones de los usuarios finales se recogen:

- En el Anexo V. Relación de usuarios y perfiles de usuario autorizados donde se establecen las operaciones autorizadas por usuario o perfil.
- En el Anexo VII. Circular de medidas de seguridad donde se establecen las obligaciones de todos los usuarios en materia de seguridad y confidencialidad.

3.7. Modelos de nombramiento

- El anexo **Nombramientos** recoge los modelos de nombramiento para designar a los delegados de protección de datos, coordinadores, y responsables de seguridad.
- Dicho anexo también recoge las obligaciones del resto del personal involucrados en la seguridad de la información, como por ejemplo:
    - administradores de sistemas informáticos
    - supervisores de archivo de documentos
    - supervisores del sistema de videovigilancia

4. Medidas específicas para ficheros y tratamientos automatizados

Para garantizar el nivel de protección exigido en el RGPD, son de aplicación las siguientes normas, procedimientos y estándares relacionados con la seguridad en los locales y sistemas de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA.

4.1. Acceso a datos a través de redes de comunicaciones

Los niveles y medidas de seguridad dispuestos a lo largo del presente documento serán exigibles de forma equivalente a los accesos a datos de carácter personal realizados a través de redes de comunicaciones, sean o no públicas.

Todos los usuarios (tanto personal de plantilla como externos) y administradores deben identificarse y autenticarse para el acceso a sistemas y aplicaciones, tanto en red local como remotamente.

4.2. Ficheros temporales y copias de trabajo de documentos

Definimos como **ficheros temporales** los ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

De un modo similar, los ficheros con datos de carácter personal que se reciban por correo electrónico deberán ser cancelados cuando hayan dejado de ser necesarios.

A efectos de facilitar el cumplimiento de esta medida, incluimos una relación de algunos de los ficheros temporales más habituales:

- Aquellos ficheros y listados elaborados ocasionalmente por los usuarios a partir de la información contenida en un fichero maestro.
- Ficheros de trabajo que se generan durante la ejecución de procesos del gestor de bases de datos o que generan las aplicaciones.
- Los ficheros que se gestionan en las colas de impresión así como los ficheros temporales almacenados en las memorias empleadas por impresoras, faxes y copiadoras de documentos.
- Los ficheros con datos de carácter personal que se reciban por correo electrónico.
- Los ficheros temporales creados por los programas de ofimática durante la edición de documentos, hojas de cálculo y demás documentos ofimáticos.
- Los ficheros temporales almacenados en la memoria

4.3. Identificación y autenticación

Los procedimientos seguidos para la identificación y autenticación de los usuarios cuando intentan acceder a los sistemas, las redes o las aplicaciones están basados en la combinación de un código de identificación de usuario y una contraseña. A cada usuario le han sido asignados identificadores individuales tanto para el acceso a los sistemas, como para el acceso a las aplicaciones (en aquellos casos en los que sea posible).

4.3.1. Asignación de identificadores y contraseñas personales para cada usuario

En la asignación de identificadores de usuario y contraseñas se tendrá en cuenta lo siguiente:

- En caso de que se utilicen identificadores de usuario, éstos y las contraseñas de acceso asociadas serán de uso personal e intransferible y por tanto **no pueden ser compartidos por varios usuarios**.

- Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y **tratadas como información personal e intransferible**. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.

- Cuando el sistema lo permita, se establecerá la **obligación de que el usuario modifique la contraseña asignada inicialmente**.

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha establecido ciertas consideraciones a la hora de elegir una contraseña que deberán ser aplicadas por todos los usuarios del sistema:

- **Se evitarán contraseñas demasiado cortas**; en términos generales se considera insegura cualquier contraseña con una longitud inferior a 8 caracteres.

- Se evitarán nombres comunes, o cualquier otra combinación que pueda identificar al usuario (fecha nacimiento, matrículas de vehículos, nombres de familiares o amigos, etc.).

4.3.2. Distribución y comunicación de las contraseñas

La comunicación de contraseñas siempre se realizará por parte del Responsable de Seguridad al usuario.

Se evitará la comunicación escrita que revele la contraseña de cualquier usuario. De comunicarse la **contraseña por escrito**, se indicará al usuario que destruya el documento utilizado una vez recibido.

Podrá efectuarse la comunicación **telefónicamente**, siempre que se asegure la identificación del receptor de la contraseña, como mínimo mediante una llamada del Responsable de Seguridad al usuario.

Podrá efectuarse la comunicación por **correo electrónico**, siempre que se asegure lo siguiente:

- Únicamente el destinatario de la contraseña tendrá acceso a la dirección de correo empleada.

- El sistema se configurará para obligar al usuario a modificar la contraseña asignada inicialmente.

- La contraseña asignada inicialmente tendrá una validez máxima de 48 horas. Si transcurrido dicho periodo de validez el usuario no ha cambiado la contraseña, la contraseña asignada automáticamente dejará de ser válida.

4.3.3. Olvido de contraseñas

En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia del Responsable de Seguridad.

4.3.4. Almacenamiento de las contraseñas

Mientras estén vigentes las contraseñas se almacenarán de forma ininteligible.

4.3.5. Frecuencia de cambio de las contraseñas

Deberán cambiarse al menos una vez al año.

Todas las contraseñas deben ser modificadas por el usuario al menos con dicha frecuencia. En los entornos en los que sea posible se automatizará este requerimiento de caducidad. Cuando no sea posible, el usuario será responsable del cambio sistemático.

4.3.6. Bloqueo de terminales tras un periodo de inactividad

Todos los usuarios deberán tener configurado su puesto de trabajo para que se exija la introducción de una contraseña al intentar volver al sistema, tras un periodo no superior a 10 minutos de inactividad.

4.4. Control de acceso

4.4.1. Política de mínimo privilegio

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha establecido mecanismos de control de acceso para garantizar que **únicamente el personal autorizado a ello puede acceder** a los diferentes recursos (redes, equipos, sistemas, ficheros y aplicaciones).

Los usuarios recibirán sus derechos de acceso siguiendo la **política de mínimo privilegio**. Es decir, únicamente a aquellos datos y recursos informáticos que precisen para el desempeño de sus funciones.

4.4.2. Identificación y autenticación de usuarios

El procedimiento seguido para la identificación y autenticación de los usuarios cuando intentar acceder al sistema, la red o las aplicaciones está basado en la combinación de un código de identificación de usuario y una contraseña. A cada usuario le ha sido asignado un identificador único tanto para el acceso al sistema, como para el acceso a las aplicaciones, de tal modo que todo usuario quede inequívocamente identificado en sus accesos.

- La sección **6. Gestión de usuarios y contraseñas** recoge los requisitos para las contraseñas en cuanto a su comunicación, confidencialidad, almacenamiento y renovación periódica.

Las contraseñas se cambiarán con una periodicidad anual, como mínimo, y mientras estén vigentes se almacenarán de forma ininteligible.

4.4.3. Relación de accesos autorizados y personal autorizado para conceder el acceso

Toda alta, baja o modificación de usuario **deberá ser autorizada por el Responsable de Seguridad**, en función de los **criterios definidos por CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA** y atendiendo a las tareas que prevea que va a desempeñar cada usuario.

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha confeccionado una **relación de accesos autorizados** para los diferentes usuarios y perfiles de usuarios. Dicha relación se ha recogido en el anexo:

- **Anexo V. Relación de usuarios y perfiles de usuario autorizados**

En dicho anexo también se recoge el **personal autorizado para conceder, alterar o anular el acceso a los recursos**, siempre conforme a los criterios establecidos por CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA y siguiendo instrucciones del Responsable de Seguridad.

4.4.4. Condiciones de acceso para el personal ajeno

El personal ajeno a CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA con acceso a los locales y recursos ámbito del presente documento de medidas de seguridad está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

4.5. 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 tratamiento realizado y se anote su realización en el documento de medidas de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

4.6. Gestión de soportes y documentos

En la gestión de soportes y documentos se tendrá en cuenta lo establecido en:

- **Sección 8., Gestión de soportes y documentos**

4.7. Copias de respaldo y recuperación

Se crearán copias de respaldo en base a lo establecido en

- **Sección 11., Procedimientos de copias de respaldo y recuperación**

5. Medidas específicas para ficheros y tratamientos no automatizados

Para garantizar el nivel de protección exigido en el RGPD, son de aplicación las siguientes normas, procedimientos y estándares relacionados con la seguridad en los locales y ficheros no automatizados de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA.

5.1. Control de acceso

Los usuarios tienen acceso únicamente a aquellos datos que precisen para el desarrollo de sus funciones. Se establecerán mecanismos para evitar que un usuario pueda acceder a recursos distintos de los autorizados. Existe una relación actualizada de usuarios, perfiles de usuario y accesos autorizados en:

- **Anexo V. Relación de usuarios y perfiles de usuario autorizados**

En dicho anexo también se recoge el personal autorizado para conceder, alterar o anular el acceso a los recursos, siempre conforme a los criterios establecidos por CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA y siguiendo instrucciones del Responsable de Seguridad.

El acceso por parte de otras personas estará estrictamente prohibido, y únicamente podrá producirse mediante petición firmada del interesado y autorización por escrito del Responsable de Seguridad.

El personal ajeno a CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA con acceso a los locales y recursos ámbito del presente documento de medidas de seguridad está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

5.2. 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, CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA establecerá los criterios y procedimientos de actuación que deban seguirse para el archivo. Corresponde la definición de dichos criterios a: la dirección de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA o al responsable del área o departamento en cuestión, con el apoyo de los responsables de seguridad competentes.

5.3. Dispositivos de almacenamiento de los ficheros no automatizados

5.3.1. Mecanismos de protección

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, se adoptarán medidas que impidan el acceso de personas no autorizadas.

5.4. Copia o reproducción y desecho de documentos

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.

5.5. Custodia de documentos

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.

5.6. Gestión de los soportes que almacenan documentos y traslado de documentos

En la gestión de soportes y documentos se tendrá en cuenta lo establecido en:

- **Sección 8., Gestión de soportes y documentos**

6. Gestión de usuarios y contraseñas

6.1. Alta, modificación, baja y reactivación de usuarios

6.1.1. Alta de usuarios

Únicamente el Responsable de Seguridad tienen competencias para autorizar el alta los identificadores de usuarios y asociarlos a los perfiles definidos para los distintos niveles de acceso a las aplicaciones y ficheros.

Toda alta de usuario en sistemas o aplicaciones, deberá ser solicitada por escrito al Responsable de Seguridad, indicado en la solicitud los datos del usuario, el área a la que pertenece, su cargo y los derechos de acceso deseados. El Responsable de Seguridad concederá los permisos de acceso que se hayan definido.

El Responsable de Seguridad valorará si alguno de los permisos solicitado no se ajusta a los criterios establecidos por CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA. En este caso, solicitará autorización específica al Responsable del Fichero, emitiendo una valoración al respecto.

Cuando los permisos solicitados se ajusten a los aprobados por CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA para el puesto de trabajo del solicitante, o bien en el caso de contar con una autorización expresa del Responsable del Fichero, el Responsable del Seguridad se ocupará, personalmente o a través de los usuarios autorizados para conceder o modificar el acceso, de la ejecución de la solicitud, indicando el perfil de acceso establecido para el nuevo usuario en cada una de las aplicaciones.

Una vez dada el alta, el Responsable de Seguridad la comunicará al nuevo usuario, indicando los datos del mismo y el identificador de usuario asignado.

6.1.2. Baja de un usuario

El Área de Recursos Humanos o el Responsable de Área usuaria donde el usuario cause baja deberá comunicar dicha baja al Responsable de Seguridad quien se encargará de cancelar el usuario y sus derechos de acceso.

El responsable de seguridad almacenará información descriptiva sobre los perfiles de acceso de los usuarios que se den de baja, durante el tiempo requerido para cumplir obligaciones legales y para auditoría.

6.1.3. Modificación de permisos de un usuario

La modificación de los derechos o permisos de acceso de un usuario requerirá de la misma autorización jerárquica, diferenciada para cada tipología de usuarios, ya descrita en el protocolo de alta. Por lo tanto, el procedimiento enunciado en el apartado de alta será extensible a este punto de modificación de permisos.

6.1.4. Reactivación de usuarios

La reactivación de usuarios exige un procedimiento diferenciado respecto al resto de protocolos enunciados anteriormente, ya que parte de la premisa de la existencia de un alta previa y no requiere de un cambio de permisos del usuario en el sistema.

Para aquellos casos en que el acceso del usuario al sistema se haya revocado por causas accidentales, como el olvido de la contraseña, un periodo prolongado de inactividad o un excesivo número intentos fallidos, la reactivación del usuario exigirá su comunicación al Responsable de Seguridad para subsanar la situación.

6.1.5. Registros

El Responsable de Seguridad mantendrá actualizada la documentación referente a:

- Perfiles de acceso e identificadores asociados por usuario.
- Altas, bajas, revocación y modificación de usuario por fechas.
- Datos sobre usuarios:
- Nombre y apellidos completos.

- Datos de instalación: inventario de recursos puestos a su disposición y de los que se hace responsable. Fecha en la que se instalaron.
- Empresa, en el caso de tratarse de personal externo.
- Área, Departamento y servicio: donde se especificará el Departamento y/o unidad en que trabaja el usuario.
- Para cada entorno donde se especificará cada aplicación y servicio donde se ha dado de alta al usuario:
    - Fecha de alta
    - Perfil de acceso
    - Tiempo de duración previsto
    - Situación actual: activo o revocado
    - Solicitud, Responsable que la aprobó, por cada acceso autorizado de que disponga.
    - Observaciones

Cualquiera de estos datos se podrá utilizar en la localización de usuarios y en la reactivación de usuarios revocados, para su control, uso o modificación.

El Responsable de seguridad mantendrá informado al delegado de protección de datos, si lo hubiera, en relación a las altas / bajas y modificaciones de usuarios.

6.2. Prestaciones de servicios sin acceso a datos

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

De no establecerse esta limitación de forma contractual, antes de proporcionar acceso al trabajador externo, se procederá a la firma del modelo Compromiso de confidencialidad y protección de datos con prestadores servicios que se incluye en el anexo Modelos de registro.

6.3. Gestión de contraseñas

6.3.1. Generación

Cada usuario tiene un identificador que se autentica mediante contraseña.

Los identificadores de usuario y las contraseñas de acceso asociadas son de uso personal e intransferible y por tanto no pueden ser compartidos.

Para el primer acceso del usuario al sistema, se le deberá comunicar de forma confidencial su identificador y su contraseña de acceso inicial. Esta comunicación deberá realizarse según lo dispuesto en el apartado de distribución.

La contraseña de acceso inicial debe ser distinta para cada usuario.

6.3.2. Privacidad

Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.

Se han establecido ciertas consideraciones a la hora de elegir una contraseña que deberán ser aplicadas por todos los usuarios del sistema:

- La longitud mínima será de 8 caracteres.
- Se evitarán nombres comunes, números de matriculas de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.
- Deberá cambiarse la contraseña con una periodicidad no inferior a un año, o en el caso de que ésta genere desconfianza del usuario, que a su vez deberá comunicar la incidencia al Responsable de Seguridad.
- Se parametrizarán los sistemas de información que tratan datos de nivel medio o alto un número máximo de reintentos de acceso fallidos (introducción reiterada de una contraseña errónea).
- Los usuarios serán responsables de su salvaguarda y custodia.

Los sistemas o aplicaciones que realizan la autenticación del usuario, permiten:

- La introducción de la contraseña y su representación en pantalla en el momento de la identificación se realizará en un formato ininteligible.
- El cambio de contraseña por parte del usuario, siguiendo las recomendaciones generales enunciadas anteriormente.

Se evitará en la comunicación escrita que se revele la contraseña de cualquier usuario. En caso necesario se tomarán las precauciones necesarias, tal y como se describe en el apartado de distribución.

En aquellos sistemas o aplicaciones que tengan una contraseña inicial o una contraseña por defecto, deberán ser cambiadas inmediatamente.

6.3.3. Almacenamiento

Las contraseñas se almacenan cifradas, y ninguna persona tendrá acceso a la descodificación de las mismas.

En el caso del sistema y la red, las contraseñas se almacenan cifradas por sus propias herramientas de seguridad. En el caso de las aplicaciones, el cifrado de las contraseñas es realizado por el sistema gestor de bases de datos o por un desarrollo "ad hoc" de la propia aplicación.

Las contraseñas de usuarios de emergencia, propios de los sistemas y con máximos privilegios, serán custodiadas por el Responsable de Seguridad.

6.3.4. Mantenimiento

Todas las contraseñas deben ser modificadas por el usuario al menos con la frecuencia establecida. En los entornos en los que sea posible se automatizará este requerimiento de caducidad. Cuando no sea posible, el usuario será responsable del cambio sistemático.

En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia del Responsable de Seguridad.

6.3.5. Distribución

La comunicación de contraseñas a los usuarios por parte del Responsable de Seguridad se realizará personalmente. Podrá efectuarse la comunicación telefónicamente, siempre que se asegure la identificación del receptor de la contraseña, como mínimo mediante una llamada del Responsable de Seguridad al usuario.

7. Régimen de trabajo fuera de los locales del responsable o encargado

Con carácter general, no está permitido el tratamiento de datos de carácter personal fuera de los locales de la entidad, excepto en los casos autorizados en el anexo:

- **Anexo V. Relación de usuarios y perfiles de usuario autorizados**

La autorización para realizar trabajos con datos personales fuera de los locales de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez de la autorización.

7.1. Modalidades de trabajo fuera de de los locales

7.1.1. Modalidad de trabajo mediante acceso remoto

Todos los accesos remotos a sistemas de información deben de ser autorizados. En todo caso, y salvo autorización previa, está terminantemente prohibido grabar en un sistema externo cualquier dato accedido remotamente.

Los responsables de sistemas de información encargados de configurar y habilitar los accesos remotos deben garantizar para los accesos remotos un nivel de seguridad equivalente al de los accesos en modo local.

7.1.2. Modalidad de trabajo mediante dispositivos portátiles

Los usuarios de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA que utilizan equipos portátiles, no podrán almacenar datos de carácter personal en los discos locales de los mismos, salvo que cuenten con autorización para ello.

Estos tratamientos deberán aplicar las mismas medidas de seguridad dispuestas en este documento, por tanto será obligatorio que en los dispositivos portátiles se habiliten los criterios establecidos sobre identificación, autenticación y control de accesos definidos en este documento de medidas de seguridad, siempre que se conecten a las redes y sistemas de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA o accedan de manera remota.

Nivel alto: no se realizarán tratamientos de datos de carácter personal en dispositivos portátiles que no permitan su cifrado, excepto en los casos recogidos motivadamente en el anexo Anexo IV. Inventarios de equipos, soportes y dispositivos de archivo y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

7.1.3. Modalidad de trabajo mediante salida de documentos

Los usuarios de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA no podrán sacar la documentación sin ser previamente autorizados.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento correspondientes, 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.

Nivel alto: Cuando se proceda al traslado físico de la documentación conteniendo datos de nivel alto, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

8. Gestión de soportes y documentos

8.1. Definición de soporte y tipos de soportes y documentos

Definimos **soporte** como aquel objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos. Algunos de los soportes más comunes son:

- Ordenadores, servidores, portátiles, unidades NAS y demás equipos informáticos.
- Dispositivos de almacenamiento como discos flexibles, cintas, discos ópticos (CD, DVD, etc), tarjetas de memoria, unidades de memoria USB, discos duros externos, etc.
- Armarios o archivadores donde se almacenan los documentos.

8.2. Identificación de soportes y documentos

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, salvo cuando las características físicas del soporte lo imposibiliten.

8.3. Inventario de soportes

Todo soporte empleado en CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA para el tratamiento de datos personales debe ser inventariado.

- Dicho inventario se ha incorporado como **Anexo IV. Inventarios de equipos, soportes y dispositivos de archivo**

Dicho anexo puede incluir el listado completo o bien una referencia al documento o sistema donde se mantiene actualizado.

8.4. Almacenamiento y acceso a los soportes

Los soportes que contengan datos de carácter personal deberán almacenarse de tal forma que sólo tengan acceso las personas autorizadas, según el régimen de autorización recogido en:

- **Anexo V. Relación de usuarios y perfiles de usuario autorizados**.

8.5. Entrada y salida de soportes y documentos

8.5.1. Autorización de la salida de soportes y documentos

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de medidas de seguridad.

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA ha aprobado una relación de salidas habituales de soportes y documentos (incluidos los enviados por correo electrónico) que han sido debidamente autorizadas (soportes de intercambio, envíos a administraciones públicas, etc.).

La citada relación figura como parte del **Anexo V. Relación de usuarios y perfiles de usuario autorizados** y ha sido comunicada a cada uno de los responsables de área.

En el caso de necesitar una autorización para la realización de salidas de soportes que no figuren en la mencionada relación, se utilizará el modelo de autorización propuesto en el **Anexo X. Modelos de autorización y registro**, que deberá contar con la firma de La Dirección o el Responsable de Seguridad habilitado para autorizar la salida de soportes y documentos de la organización.

8.6. Reutilización de soportes

Cuando se vaya a reutilizar un soporte, se procederá a eliminar toda la información almacenada en el mismo mediante el uso de una herramienta específica que impida cualquier recuperación posterior de información.

8.7. Desecho de soportes y documentos

Cuando vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal (por ejemplo porque presente errores en su tratamiento) deberá procederse a su destrucción, de manera que se impida la reconstrucción posterior del documento (por ejemplo mediante el uso de destructora).

9. Procedimiento de gestión de incidencias

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA recogerá cuantas incidencias de seguridad se produzcan sobre los datos que trata. Este procedimiento establece los mecanismos de actuación por parte de los usuarios de los sistemas de información para la comunicación, gestión y respuesta ante las incidencias.

La aplicación del presente procedimiento se establece para todos los usuarios, tanto empleados como colaboradores externos.

9.1. Tipos de incidencia a registrar

Se interpretará el concepto de incidencia en su sentido más amplio, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de los medios físicos y lógicos que pueda afectar a su disponibilidad y a la seguridad de la información que gestionan.

A continuación se presenta una lista de incidencias que serán inexcusablemente registradas. Esta lista no debe entenderse como limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubieran quedado omitidas:

- Incidencias que afecten a la identificación y autenticación de los usuarios:
  - Pérdida de confidencialidad de contraseñas.
  - Asignación o modificación de derechos sobre herramientas de control de acceso y utilidades con accesos privilegiados.
  - Períodos de desactivación de las herramientas de seguridad.
- Incidencias que afecten a los derechos de acceso a los datos:
  - Revisión de "logs" sobre intentos fallidos de accesos, accesos fuera de horas de oficina, etc.
  - Comunicación de los usuarios de sospechas de que alguien ha suplantado su personalidad.
  - Detección de puntos de acceso desatendidos y sin protección de pantalla activada.
  - Detección de contraseñas escritas en los puestos de trabajo.
  - Revisión de los informes de seguridad.
  - Revisión de los registros de acceso a datos especialmente protegidos.
- Incidencias que afecten a la gestión de soportes:
  - Comunicación de pérdida de soportes.
  - Comunicación de localización de soportes en lugares inadecuados.
  - Errores de contenido en soportes recibidos.
- Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación:
  - Errores en los procesos de realización de copias de salvaguarda.
  - Recuperaciones de datos realizadas.
  - Pruebas realizadas con datos reales, previas a la implantación o modificación de los sistemas de información.

- Cualquier otra de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el documento de medidas de seguridad.

9.2. Responsabilidades

El **Responsable de Seguridad** gestionará la implantación del procedimiento de gestión de incidencias, y realizará el seguimiento de todas las incidencias en materia de seguridad.

Todos **los usuarios serán informados de la obligación de notificar cualquier incidencia** producida en materia de seguridad.

9.3. Descripción del procedimiento e información a registrar

Los usuarios de los sistemas de información, empleados y colaboradores externos, deben participar en la implantación y seguimiento del sistema de gestión de incidencias, aceptando formalmente sus obligaciones.

9.3.1. Comunicación de incidencias de Seguridad por parte de los usuarios

Cualquier usuario que tenga conocimiento directa o indirectamente de cualquier incidencia de seguridad, actual o posible, lo comunicará con la mayor brevedad tal incidencia y las acciones que se hubiesen tomado de urgencia.

Todas las comunicaciones deberán efectuarse al Responsable de Seguridad indicando el momento en que se detectaron y utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente. Para que quede constancia de la comunicación, el usuario, además, lo comunicará por correo electrónico.

En este momento se registrará la incidencia y, si afecta a la seguridad de los datos de carácter personal, se catalogará como tal.

9.3.2. Registro y distribución de las incidencias

Con el fin de poder mantener un registro de incidencias que permita su mantenimiento y posterior tratamiento y análisis se centralizará la recepción de las mismas ante el Responsable de Seguridad.

En el caso de incidencias sobre procesos o aplicaciones se comunicarán directamente al Responsable informático, quien se ocupará de informar al Responsable de Seguridad sobre su resolución.

9.3.3. Contenido del registro de incidencias

El registro de incidencias será mantenido en exclusiva por el Responsable de seguridad. Se facilitará el acceso estrictamente a aquellos usuarios o áreas que lo necesiten, para su consulta o análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias.

El registro contendrá como mínimo los siguientes campos:

- Tipo de incidencia
- Momento en que se ha producido (en su defecto detección)
- Persona que la notifica
- Quién la recibe
- A quién se le notifica
- Efectos causados por la misma

9.4. Notificación de las violaciones de seguridad a las autoridades y personas afectadas

El RGPD establece la obligación de realizar, a partir del 25 de mayo de 2018, las siguientes notificaciones:

- Notificación a las autoridades de protección de datos (Agencia Española de Protección de Datos u otra autoridad competente) de aquellas violaciones de seguridad que supongan un riesgo para los derechos y libertades para las personas físicas, conforme al artículo 33 del RGPD. La notificación se hará dentro de las 72 horas después de tener constancia del incidente.

- Notificación al responsable del tratamiento, cuando CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA actúe como encargado del tratamiento. La notificación se hará sin dilación indebida, conforme al artículo 33.2 del RGPD.

- Notificación a las personas físicas cuyos datos se hayan visto comprometidos, de aquellas violaciones de seguridad que supongan un alto riesgo para los derechos y libertades para las personas físicas. La notificación se harán sin dilación indebida, conforme al artículo 34 del RGPD.

No realizar estas notificaciones es una infracción del RGPD y puede acarrear una sanción para CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA, por lo que se ha elaborado un procedimiento específico relativo a estas notificaciones.

Las violaciones se comunicarán de forma inmediata al delegado de protección de datos, si lo hubiera, o en su defrecto a La dirección ejecutiva de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA.

10. Procedimientos de revisión

10.1. Actualización del documento de medidas de seguridad

El presente documento de medidas de seguridad deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en los sistemas de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados.

En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

La actualización del documento de medidas de seguridad será coordinada por el Responsable de Seguridad.

10.2. Análisis de los niveles de riesgo

CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA analizará periódicamente los niveles de riesgo en materia de seguridad de los tratamientos. El resultado del análisis incluirá las medidas de seguridad necesarias para mitigar los riesgos que se detecten. Este análisis es recomendable realizarlo con carácter anual y en todo caso se realizará al menos con carácter bienal (cada dos años).

10.3. Controles periódicos para garantizar el cumplimiento del documento

En el presente apartado se recogen los controles establecidos para la verificación del cumplimiento de lo dispuesto en el documento de medidas de seguridad.

El Responsable de Seguridad será el encargado de que se lleven a cabo todos los controles descritos en el presente procedimiento así como de que queden adecuadamente registrados.

En esta sección, se describen los controles a realizar.

Cada uno de estos controles generará un registro en el que se incluirá:

- La fecha de realización del control
- La descripción concreta del control realizado
- El resultado del control
- Las acciones correctoras necesarias en su caso
- El nombre de la persona que lo ha realizado.

10.3.1. Controles con relación a la identificación, autenticación y derechos de acceso en sistemas automatizados

- En relación con los derechos de acceso, se obtendrá periódicamente una relación de usuarios con sus derechos de acceso siguiendo el procedimiento descrito en el documento de medidas de seguridad, para llevar a cabo los siguientes controles:
    - Se comprobará que los nuevos usuarios dados de Alta tengan acceso únicamente a los sistemas y/o aplicaciones solicitadas en la correspondiente notificación escrita de solicitud de alta, repitiéndose la misma comprobación para los usuarios a los que se les hayan realizado modificaciones de sus derechos de acceso. En el caso de usuarios dados de baja en este periodo de tiempo, se comprobará que les han sido revocados todos sus derechos de acceso.
    - Se realizará una selección aleatoria de dos usuarios y se comprobará que el acceso del que disponen, se corresponde con su perfil asignado.

- Verificación periódica de la correcta parametrización de los sistemas y aplicaciones en cuanto a la caducidad de las contraseñas establecida en el documento de medidas de seguridad.

- Verificación periódica de la correcta parametrización de los sistemas y aplicaciones en cuanto a la limitación del número máximo de intentos reiterados de acceso no autorizado al sistema.

- Verificación periódica de los sistemas automatizados para comprobar la existencia de usuarios con derechos de administrador o superusuario no controlados por el Responsable de Seguridad.

- Verificación de que las contraseñas almacenadas por los nuevos sistemas o aplicaciones puestas en producción se almacenan en formato ininteligible para todos los usuarios con cualquier tipo de privilegios. Este control no será periódico sino que se realizará siempre antes y después de la puesta en producción de nuevos sistemas o aplicaciones.

10.3.2. Controles con relación a la identificación y derechos de acceso a sistemas no automatizados (papel)

- En relación con los derechos de acceso, se verificará periódicamente que la relación de usuarios con sus derechos de acceso está actualizada con las altas y bajas de usuarios que se hayan dado en la organización.

- Se verificará periódicamente la vigencia de la lista de control de acceso físico al lugar o a los lugares donde se encuentran almacenados los documentos, comprobando que no falta nadie con derecho de acceso a dichos soportes y que se han dado las bajas pertinentes en dicha lista.

10.3.3. Controles con relación a la gestión de soportes y documentos

- Periódicamente se realizará una selección aleatoria de una muestra soportes inventariados, copias de "backup" y otros si los hubiera, con el fin de comprobar el correcto etiquetado de los mismos, así como su inclusión en el inventario de soportes.

- Se verificará periódicamente la vigencia de la lista de control de acceso físico al lugar o a los lugares donde se encuentran almacenados los soportes, comprobando que no falta nadie con derecho de acceso a dichos soportes y que se han dado las bajas pertinentes en dicha lista.

- Periódicamente se realizará una selección aleatoria de ordenadores de la organización, con el fin de verificar que el usuario asignado a los mismos no haya instalado ninguna aplicación no autorizada.

10.3.4. Controles con relación al control de acceso físico a los sistemas de información

- Comprobación periódica de la vigencia de las listas de acceso a los locales donde se ubican los sistemas de información con datos de carácter personal, prestando atención a la revisión de altas y bajas en dicha lista.

10.3.5. Controles con relación al acceso a través de redes de telecomunicaciones

- Periódicamente se verificará mediante muestra que los usuarios no han instalado aplicaciones que permitan el acceso remoto al sistema de información.

10.3.6. Controles con relación a los ficheros temporales

- Comprobar periódicamente, mediante la selección de una muestra, que no hay ningún fichero temporal más tiempo del previsto en los directorios de ficheros temporales de las aplicaciones.

- Comprobar periódicamente, mediante la selección de una muestra, que no hay ningún fichero temporal más tiempo del previsto en los directorios de ficheros compartidos por varios usuarios.

- Comprobación periódica de que no se almacenan ficheros temporales con datos de carácter personal en dos puestos personales elegidos al azar.

10.3.7. Controles con relación al registro de incidencias

- Comprobar periódicamente la resolución efectiva de las incidencias incluidas en el registro y verificar que las incidencias que queden pendientes de resolver, están siendo debidamente tratadas.

- De todas aquellas incidencias que hubieran requerido la ejecución del procedimiento de recuperación de datos, seleccionar periódicamente una muestra, para comprobar la correspondiente autorización de dicho proceso.

10.3.8. Controles con relación al procedimiento de copias de respaldo y recuperación de datos

- Periódicamente se comprobará el correcto funcionamiento de los procedimientos de recuperación de un fichero elegido al azar de una de las copias de respaldo.

11. Procedimientos de copias de respaldo y recuperación

El RGPD establece la obligación de realizar copias de seguridad de los datos personales objeto de tratamiento automatizado. Los procedimientos de copia de respaldo y recuperación de CONSORCIO UNIVERSITARIO CENTRO ASOCIADO A LA UNED EN CANTABRIA se han recogido en el anexo:

- ***Anexo IX. Relación de procedimientos de copia de respaldo y recuperación***

11.1. Requisitos para los procedimientos de copia de respaldo y recuperación

El Responsable de Seguridad se encarga de controlar la correcta aplicación de los procedimientos de forma que se cumplan los siguientes requisitos:

- Todos los soportes utilizados para las copias de seguridad cumplirán las normas relativas a identificación de los soportes, inventariado y almacenamiento con las **correspondientes medidas de control de acceso** (armario con llave, caja ignífuga, etc) que garanticen que únicamente sean utilizados por el personal encargado de la ejecución de los procedimientos de copia de respaldo.

- Deberá asegurarse que los procedimientos de copia de seguridad **cubran la totalidad de ficheros y tratamientos automatizados de datos personales** incluidos en servidores, bases de datos, soportes móviles y demás dispositivos.

- La **periodicidad de la copia será al menos semanal**, salvo que en dicho periodo no se hubiera producido ninguna modificación de los datos.

- Los procedimientos para la recuperación de los datos **garantizarán su recuperación en el estado en que se encontraban** al tiempo de producirse la pérdida o destrucción.

- Cuando se vayan a realizar pruebas con datos reales, será obligatorio realizar previamente copia de todos los datos afectados.

- Para evitar pérdida de datos en caso de mal funcionamiento de alguno de los soportes de copia, se mantendrán **varios soportes de copia**.

11.2. Solicitud, autorización y ejecución de procedimientos de recuperación

Para la solicitud, autorización y ejecución de los procedimientos de recuperación de datos deberán seguirse inexcusablemente los siguientes pasos:

- **Solicitud**. El peticionario enviará la solicitud de ejecución del procedimiento de restauración al responsable de seguridad. Dicha solicitud estará motivada y deberá ir visada por el responsable del área del peticionario.

- **Autorización**. El Responsable de Seguridad revisará la solicitud, para verificar que esté correctamente fundamentada.

- **Ejecución**. Salvo que la solicitud no esté convenientemente fundamentada se procederá a trasladar la orden de recuperación al personal autorizado, notificándose también al solicitante, indicando la aprobación o denegación. Deberá ponerse especial cuidado en que la ejecución del procedimiento no implique un riesgo para la disponibilidad de las aplicaciones.

- **Registro**. El Responsable de Seguridad registrará la ejecución del procedimiento en el registro de incidencias. Toda la documentación original será archivada por el Responsable de Seguridad.

11.3. Verificación periódica de procedimientos de copia de respaldo y recuperación

El Responsable de Seguridad se encargará de revisar periódicamente (cada seis meses) la correcta definición, funcionamiento y aplicación de los procedimientos de copia de respaldo y recuperación de datos. Para ello:

- Se examinará los procedimientos para verificar si son vigentes y si cubren la totalidad de los datos personales almacenados.

- Se comprobará la integridad de los soportes utilizados (herramientas SCANDISK o análogas)

- En caso de desecho de soporte, destrucción física del mismo o utilización de herramientas que garanticen la recuperación posterior de información.

- Se verificará que se realiza la copia con la periodicidad estipulada.

- Se realizará una prueba de restauración a partir de la copia de seguridad y se revisará que se restauran todos los datos de manera correcta.