PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

MANUAL DE GESTIÓN INTERNA Y

DE NORMAS DE SEGURIDAD

VERSIÓN 13/11/12

MANUAL DE CONCEPTOS BÁSICOS

INTRODUCCIÓN

La Universidad de Cantabria tiene diversos ficheros que recogen un gran número de datos personales, necesarios para cumplir sus funciones, y relativos fundamentalmente a sus alumnos, personal y proveedores.

Estos datos personales deben estar debidamente protegidos de acuerdo con las exigencias de la Ley Orgánica de Protección de Datos de Carácter Personal y las disposiciones que la desarrollen, especialmente el Real Decreto 1720/2007

Por ello, el acceso a los ficheros que contienen datos personales está limitado al personal autorizado según los casos y, en el caso de ficheros automatizados, exige al menos el control de acceso por contraseña o cualquier otro método de seguridad que se disponga en cada momento. Por su parte, el acceso a la documentación en papel está igualmente restringida al personal que debe gestionar dicha documentación y debe protegerse mediante custodia bajo llave en los términos que disponga la normativa interna aplicable, particularmente las circulares que se dicten por la Gerencia (v. circular nº 132).

Existe un fichero a cuya información tiene acceso todo el personal, que es el directorio de personas de la UC, donde figuran su nombre y su puesto y unidad de trabajo, además de otros datos relativos a su localización y dirección.

Se considera que estos datos tienen también carácter personal, aunque se refiera a la relación profesional con la Universidad, y por ello, las diferentes obligaciones sobre seguridad, confidencialidad y protección de los datos **nos afectan a todos.**

Estas obligaciones figuran en las páginas siguientes, junto con una serie de cuestiones de carácter básico relativas a la gestión y tratamiento de datos personales que debemos conocer en la medida que nuestro trabajo implica dicha gestión o acceso.

GENERALIDADES Y CUESTIONES BÁSICAS SOBRE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Este apartado y el siguiente constituyen un resumen de conceptos básicos de la Ley Orgánica de Protección de Datos de carácter personal y de la normativa interna de la Universidad de Cantabria en esta materia. Si se desea tener un conocimiento más detallado, deberán consultarse ambas fuentes, además del Reglamento de desarrollo de la primera:

- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal
- Real Decreto 1720/2007 por el que se *aprueba el* Reglamento de desarrollo de la Ley Orgánica 15/1999 (en adelante, RLOPD)
- Normativa propia de la Universidad de Cantabria
- Normativa de derechos de acceso, cancelación y rectificación

Salvo que se indique otra cosa, los artículos citados son de la Ley 15/1999.

Terminología

Datos de carácter personal:	Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables
Fichero:	Todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de creación, almacenamiento, organización y acceso.
Tratamiento de datos:	Cualquier operación o procedimiento que se realiza con o sobre los datos personales, ya sean dichas operaciones automatizadas o no.
Cesión o comunicación de datos:	Toda revelación de datos realizada a una persona distinta del interesado
Fuentes accesibles al público:	Exclusivamente lo son las relacionadas en el art. 3. j) de la LOPD y en el artículo 7 del RLOPD, y en los términos recogidos en los mismos.
Responsable del fichero o tratamiento	Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
Encargado del tratamiento	Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Recogida de datos

1. Norma general ➔ **Información**

art 5.1 LOPD

Todos los interesados a los que se soliciten datos personales tendrán que ser **informados**:

1) De la existencia de un fichero al que se incorporarán los datos personales que se solicitan, la finalidad para la que se recogen y los destinatarios de la información.

2) Del carácter obligatorio o no de su respuesta.

3) De las consecuencias de la obtención de los datos o de su negativa a suministrarlos.

4) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

5) De la identidad y dirección del responsable del tratamiento.

Por tanto ➔ **Cláusula informativa** sobre lo anterior en todos los impresos de recogida de datos, salvo que el interesado ya haya sido informado con anterioridad en el mismo procedimiento o en el inicio de su relación con la UC o con el servicio de que se trate

Datos facilitados por terceros

art. 5.4 LOPD

- Cuando los datos personales le sean facilitados a la Universidad no por el propio afectado, sino por otra persona u organismo, la UC deberá **informar al afectado** de:

  1) Contenido y finalidad del tratamiento de datos y de la incorporación de los datos a un fichero.

  2) Procedencia de los datos

  3) Posibilidad de ejercitar los derechos antes citados.

  4) Identidad y dirección del responsable del fichero.

art. 5.5. LOPD

- No será necesaria esa información cuando expresamente una ley lo prevea. o el tratamiento tenga fines históricos, estadísticos o científicos.

Tratamiento de datos

1. Norma general ➔ **Consentimiento**

El tratamiento requerirá el consentimiento **inequívoco, específico e informado** del afectado.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, identificando la finalidad para la que se recaba, es decir, las finalidades del fichero en que se van a integrar los datos.

El consentimiento es revocable y así debe advertirse al recabarlo**.**

2. Excepciones (No necesidad de consentimiento para el tratamiento)

art. 6.1 **1)** Que una ley disponga otra cosa (es decir, que excluya la necesidad del consentimiento).

art. 6.2 ➔ **2)** Cuando los datos se recojan para el ejercicio de funciones propias de las Administraciones Públicas.

art. 6.2 ➔ **3)** Cuando se refieran a las partes de una relación laboral o administrativa y sean necesarios para su mantenimiento y cumplimiento.

art.10.2 a) RLOPD **4)** Cuando el tratamiento de los datos sea necesario para que el responsable del tratamiento cumpla un deber que le imponga una norma con rango de Ley o de derecho comunitario.

Existen otros supuestos. Los apartados que se señalan son los casos que más frecuentemente se producirán en la UC.

3. Datos especialmente protegidos

art. 7 LOPD Será **imprescindible el consentimiento inequívoco, específico, expreso e informado** del afectado para el **tratamiento y cesión** cuando sean datos relativos a:

1) Ideología y afiliación sindical.

2) Religión o creencias.

3) Salud.

4) Origen racial o étnico.

5) Vida sexual.

En los casos 3, 4 y 5, salvo que por razones de interés general una Ley disponga otra cosa y otras excepciones que pueden consultarse en el art. 7.6

Cesión de datos

1. Norma general ➔ **Consentimiento**

- Los datos sólo podrán ser cedidos para el ejercicio de funciones legítimas del cedente y del cesionario **con el previo consentimiento del afectado**.

- El consentimiento debe ser **inequívoco, específico e informado**: el afectado debe conocer la finalidad a que se destinarán los datos que se ceden y el tipo de actividad desarrollado por el cesionario

2. Excepciones *(no necesidad de consentimiento para la cesión)*

art. 11.2 a) LOPD	➔	**1)** Cuando la cesión esté autorizada en una Ley
art. 11.2. b)		**2)** Cuando los datos se han recogido de fuentes accesibles al público.
art. 11.2.c)	➔	**3)** Si hay una relación jurídica libremente aceptada cuyo desarrollo, cumplimiento y control exige necesariamente la conexión con ficheros de terceros.
art. 11.2. d)	➔	**4)** Cuando la comunicación se hace al Defensor del Pueblo, Ministerio Fiscal, Jueces y Tribunales y Tribunal de Cuentas.
art. 21. 1 y 2	➔	**5)** Cuando los datos son recogidos por la Administración Pública (UC) con destino a otras Administraciones o para el ejercicio por éstas de competencias sobre las mismas materias, o cuando la comunicación de datos se realice para el tratamiento posterior de los datos con fines históricos, estadísticos o científicos
art. 10.2 a) RLOPD	➔	**6)** Cuando el tratamiento de los datos sea necesario para que el responsable del tratamiento cumpla un deber que le imponga una norma con rango de Ley o de derecho comunitario.

3. Procedimiento interno

Normativa UC: Tit. II	➔	Las cesiones de datos previstas para cada fichero pueden ser consultadas en la sección 07-050 del Documento de Seguridad. Dichas cesiones deberán figurar en las correspondientes cláusulas informativas. Cualquier otra cesión de datos deberá ser trasladada al Comité de Seguridad y aprobada por la Gerencia. En todos los supuestos de cesiones de datos se seguirá el procedimiento establecido en la Normativa Interna de la UC.

4. Datos especialmente protegidos

Debe recordarse que la cesión de los datos relativos a ideología, salud, etc del art. 7 precisa siempre del **consentimiento inequívoco, específico e informado**, aunque a su vez, como ya se ha visto, existen también excepciones *(ver art. 7)*.

Cesión internacional de datos (Resumen art. 34 LOPD)

1. Regla general

La transferencia exige un procedimiento específico ante la Agencia Española de Protección de Datos.

2. Excepciones

- Puede hacerse la transferencia internacional si se tiene el **consentimiento** del afectado, prestado en los términos ya indicados: de forma **inequívoca, específica e informada.**

- También puede hacerse la transferencia de datos si tiene como destino un estado de la Unión Europea.

CUESTIONES BÁSICAS DE LA NORMATIVA PROPIA

Sin perjuicio de la obligada lectura de nuestra normativa propia en materia de protección de datos de carácter personal, se destacan a continuación algunos aspectos no mencionados en los apartados anteriores y que tienen importancia práctica.

Creación del Comité de Seguridad

El Comité de Seguridad está regulado en la sección 01-010 “Identificación de los responsables de seguridad y de los ficheros” y 04-020 “Funciones y obligaciones” del Documento de Seguridad.

Deber de confidencialidad

Todo el personal de la Universidad de Cantabria que intervenga en alguna fase del tratamiento de datos personales o que de cualquier modo pueda tener acceso a ellos, **está obligado al secreto profesional o deber de confidencialidad** respecto de dichos datos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con la Universidad de Cantabria. Este deber cobra especial importancia en relación con los datos especialmente protegidos (salud, discapacidad, afiliación sindical, etc.).

En este sentido, los datos personales sólo deberán ser gestionados para los fines propios de la unidad y de acuerdo con los sistemas y procedimientos habituales en ella.

OTRAS CUESTIONES

Petición de etiquetas

La unidad que precise listados o etiquetas con datos personales para envíos por correo deberá indicar la finalidad para la que las necesita a la unidad responsable del fichero, con el fin de que pueda seleccionar, en su caso, el tipo de listado más idóneo.

Ejercicio de los derechos de acceso, rectificación y cancelación y su gestión interna

Cualquier interesado cuyos datos personales estén en ficheros de la Universidad tiene derecho a conocerlos (derecho de acceso) y a rectificarlos o cancelarlos (si no existen impedimentos).

Para ello, puede solicitarlo en los modelos de impresos disponibles en la web y presentarlos por correo postal ordinario, presencialmente en el Registro General de la Universidad o bien por cualquiera de los medios previstos en el artículo 38.4 de la LRJPAC, dirigidos al Gerente.

Todas las unidades de la universidad tendrán la obligación de facilitar, a quien lo requiera, modelos de solicitud para el ejercicio de estos derechos. No obstante, los interesados pueden utilizar cualquier

otro que reúna la información exigida en el artículo 25 del RLOPD. Asimismo, estarán obligadas a facilitar información sobre el ejercicio de estos derechos (Normativa de derechos de acceso, cancelación y rectificación).

Las solicitudes se dirigirán desde el Registro General a la Gerencia.

Las diferentes unidades de la Universidad se atendrán necesaria y obligatoriamente al procedimiento de gestión interna de estos derechos, de acuerdo con el cual la Gerencia es el único órgano responsable de contestar las solicitudes. Por este motivo, las unidades facilitarán a aquélla en cada caso concreto la información o trámites que ésta les requiera.

Visitas de inspección de la Agencia Española de Protección de Datos

Ante una visita de personal de la citada Agencia, deberá dirigírseles a la Gerencia.

CUESTIONES ESPECÍFICAS PARA RESPONSABLES DE UNIDADES QUE GESTIONAN ALGÚN FICHERO DE DATOS PERSONALES

Modificación y creación de ficheros. Nuevos impresos (art. 14 normativa propia)

1. Cuando un fichero automatizado o no o una aplicación informática vaya a modificarse para incluir nuevos datos de carácter personal o vayan a establecerse nuevas cesiones o impresos de recogida de datos, el responsable de la unidad gestora del fichero lo pondrá en conocimiento del Comité de Seguridad de la UC para que por ésta se analice la necesidad de regularizar los ficheros ya declarados a la Agencia Española de Protección de Datos o de incluir o revisar textos informativos en los impresos, así como para actualizar el documento de seguridad.

Redacción de fórmulas y textos informativos para impresos

En la creación de nuevos ficheros, automatizados o no, y aplicaciones informáticas que puedan contener datos de carácter personal, el responsable de la unidad gestora velará por que el personal encargado de su diseño guarde especial cuidado en implementar las medidas de seguridad e incluir las fórmulas informativas que sean precisas en los impresos y procedimientos telemáticos de recogida de datos. Para la redacción de las cláusulas informativas y otras relativas a la protección de datos personales, la unidad gestora realizará un primer análisis de los supuestos y términos en que sean necesarias, según los modelos y pautas establecidos, para ponerlo después en conocimiento del Comité de Seguridad y someter la adecuación de la redacción y supuestos previstos a la Asesoría Jurídica.

En ficheros o tratamientos ya existentes, la unidad gestora del fichero deberá revisar los documentos de recogida de datos de nueva creación, tanto si son en soporte papel como formularios telemáticos, y realizar un primer análisis sobre la necesidad o no de incluir algún texto informativo o cualquier otro

en relación con la protección de datos personales, según los modelos establecidos, para ponerlo después en conocimiento del Comité de Seguridad y someter la adecuación de la redacción y supuestos previstos a la Asesoría Jurídica. El resultado de todo lo anterior deberá ser aprobado por el Comité de Seguridad.

Encargados de tratamiento: documentos contractuales o de compromiso

Siempre que exista o pueda existir acceso a datos personales contenidos en los ficheros de la UC por parte de terceros ajenos a ella, con motivo de la **prestación de un servicio**, ya sea mediante contrato escrito o mediante encargos específicos no formalizados mediante contrato escrito, deberá firmarse por ese tercero un documento contractual o un compromiso de acuerdo con las condiciones previstas en el artículo 12 de la normativa propia y según los modelos contenidos en ella.

La unidad gestora del fichero conservará copia de todos los documentos firmados por los encargados de tratamiento del fichero que gestiona y remitirá el original de los mismos al Comité de Seguridad. Si se trata de cláusulas insertas o anexas a un contrato administrativo se consignará la referencia de tal contrato en la documentación del fichero custodiada por la unidad gestora.(Ver artículo 13 de la Normativa interna de la UC)

Procedimiento para la cesión legal de datos

En los artículos 6 al 10 de la normativa propia de la Universidad de Cantabria se encuentra regulada esta materia.

Como norma general, debe recordarse que es necesario el consentimiento, salvo las excepciones previstas (ver el apartado “Generalidades y cuestiones básicas” de este documento). Por otra parte, en las clásulas informativas de los impresos de recogida de datos se indican las cesiones que van a realizarse recabando a través de su firma el indicado consentimiento.

Conservación y cancelación de datos

1. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, sin perjuicio de lo establecido en el punto 3.

2. Los plazos de conservación dependerán de la vinculación existente entre la Universidad de Cantabria y el interesado, siendo conservados, con carácter general, mientras subsista la relación y, una vez concluida, como máximo por los plazos siguientes, salvo lo dispuesto en el número 3:

- Cinco años para los datos de clientes, proveedores o suministradores.
- Permanentemente para los datos de estudiantes o antiguos alumnos, empleados o ex-empleados.

3. No procederá la cancelación de los datos cuando ello pudiese causar un perjuicio a intereses legítimos del interesado o de terceros, cuando existiese obligación legal de conservarlos, cuando exista una relación contractual, cuando sea preciso su mantenimiento para gestiones de pagos o

cobros o para la realización de inspecciones y auditorías, o para el adecuado ejercicio de las funciones propias de la Universidad de Cantabria.

Gestión de derechos de acceso, rectificación y cancelación. Gestión de incidencias

Los responsables de las unidades gestoras deberán tener en cuenta las obligaciones y procedimiento establecidos en relación con estos aspectos:

- Normativa y procedimientos para el ejercicio de los derechos de acceso, cancelación y rectificación
- Gestión de incidencias

Archivo de documentación

Las unidades gestoras de ficheros deberán mantener un archivo con toda la documentación sobre los ficheros de datos personales relativa a las obligaciones recogidas en la normativa de protección, que incluya, entre otra, copia de los documentos firmados por los encargados de tratamiento y por los cesionarios de datos, así como de las cesiones realizadas.

CUESTIONES ESPECÍFICAS PARA RESPONSABLES DE UNIDADES EN GENERAL

Personal de nuevo ingreso

Aunque el el servicio de recursos humanos correspondiente ya informa al personal de nuevo ingreso sobre el manual de normas de seguridad, es obligación de los responsables de todas las unidades recordar al personal que accede a ella siendo de nuevo ingreso en la Universidad, la existencia de este manual sobre protección de datos de carácter personal, accesible en la intranet.

En la sección 07-020 del Documento de Seguridad se establecen los protocolos de información, la clausulas de confidencialidad y las unidades encargadas de realizar estas funciones.

Los modelos de cláusulas de confidencialidad y el tipo de información facilitada se organizan en tres grandes grupos en función de la vinculación de cada persona con la UC y, por lo tanto, el acceso que puedan tener a los ficheros de datos personales y su derecho a tener una "cuenta personal" que les permite su identificación frente a los sistemas informáticos centrales denominada "cuenta intranet" o "cuenta personal":

a) En el primer grupo se encuadra el Personal Docente e Investigador, el Personal de Administración y Servicios y los colectivos asociados a cada uno de ellos (esta información está permanentemente actualizada en la "Normativa de cuentas personales de la UC" que puede consultarse en la página Web de la UC).

b) El segundo grupo está formado por profesionales con contrato de asistencia técnica (letrados, auditores, etc.) y el personal de empresas que prestan servicios a la UC (personal de seguridad, etc.) y que por razón de las funciones encomendadas puedan tener acceso a determinados ficheros de datos personales, siempre que no se les autorice una "cuenta intranet" o "cuenta personal" en la UC.

c) Un tercer grupo está formado por personal de empresas que prestan sus servicios a la UC pero que por razón de las funciones que desempeñan no tienen acceso a ficheros de datos personales (subcontratas de mantenimiento, limpieza, etc.).

FUNCIONES Y OBLIGACIONES
INCUMPLIMIENTO DE LAS OBLIGACIONES Y DE LAS NORMAS DE SEGURIDAD ESTABLECIDAS
(https://www.unican.es/WebUC/Unidades/ucpd/inf_profesional/

INCUMPLIMIENTO DE LAS OBLIGACIONES Y DE LAS NORMAS DE SEGURIDAD ESTABLECIDAS

Consecuencias del incumplimiento

El personal de la Universidad de Cantabria con acceso a datos de carácter personal deberá conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudieran incurrir en caso de incumplimiento de la normativa de seguridad, que podría derivar en sanciones.

El incumplimiento de las obligaciones establecidas en este manual y en la normativa interna relacionada con la protección de datos personales, así como la comisión de las infracciones tipificadas en la Ley Orgánica de Protección de Datos de Carácter Personal, podrá ser sancionado de acuerdo con la legislación laboral o el régimen disciplinario aplicable a funcionarios.

Infracciones tipificadas en la LOPD

- Son infracciones leves:
  - No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
  - No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.
  - El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
  - La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.
- Son infracciones graves:
  - Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.
  - Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.
  - Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.
  - La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.
  - El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
  - El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio

interesado.

- El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- iNo atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
- La obstrucción al ejercicio de la función inspectora.
- La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

- Son infracciones muy graves:
  - La recogida de datos en forma engañosa o fraudulenta.
  - Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.
  - No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
  - La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

ANEXOS

I Normas de seguridad que afectan al desarrollo de las propias funciones

II Normativa propia sobre protección de datos de carácter personal

III Normativa sobre ejercicio de los derechos de acceso, rectificación y cancelación

IV Normativa sobre procedimiento de gestión interna de los derechos de acceso, rectificación y cancelación

V Extracto de la Ley Orgánica de Protección de Datos de carácter personal

VI Relación de responsables de seguridad, administradores de sistemas y unidades gestoras de ficheros

VII Glosario de términos

ANEXO I

NORMAS DE SEGURIDAD QUE AFECTAN AL DESARROLLO DE LAS PROPIAS FUNCIONES

NORMAS DE SEGURIDAD QUE AFECTAN AL DESARROLLO DE LAS PROPIAS FUNCIONES

➢ Registro de incidencias (procedimiento de notificación y gestión).

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de los ficheros de la UC.

El procedimiento a seguir para la notificación de incidencias será el siguiente:

1. La incidencia se pondrá en conocimiento de la persona responsable del fichero y/o del Comité de Seguridad, quienes recabarán la información complementaria necesaria en cada caso.
2. La notificación de la incidencia se hará preferentemente por medio de un formulario web accesible desde intranet, que deberá contener la siguiente información:
   - Persona que realiza la comunicación.
   - Descripción de la incidencia.
   - Fichero al que afecta.
   - Fecha y hora de producción de la incidencia.
   - Fecha y hora de comunicación de la incidencia.
   - Posibles causas.
3. Las incidencias notificadas se incorporarán al registro informático y serán tratadas por el Comité de Seguridad.
4. Éste realizará las gestiones y análisis necesarios para completar la información que pudiera faltar sobre la incidencia y para reparar o minorar los efectos negativos de la incidencia, así como los controles y comunicaciones que sean precisos.
5. Junto a la información recogida en el formulario, el responsable de seguridad deberá completar en el registro de incidencias la siguiente:
   – Efectos derivados de la incidencia.
   – Medidas adoptadas y controles implantados o reforzados.
   – Fecha de "cierre" de la incidencia.
   – Persona que ha cerrado la incidencia.

El modelo utilizado para la notificación de incidencias está disponible en Intranet y figura como anexo 07-040 del Documento de seguridad.

El responsable de seguridad podrá adoptar, al margen del procedimiento descrito, acciones inmediatas de control, especialmente de carácter técnico: recuperación de ficheros, bloqueo de usuarios, etc.

➢ Identificación y autenticación: asignación de códigos de usuario y contraseñas.

VERIFICAR QUE ESTÉ ACTUALIZADO

Asignación de códigos de usuario: Cada usuario tendrá un solo código, para acceder a un sistema único o a varios. Los usuarios serán responsables ante la Universidad de Cantabria de todas las actividades y accesos que se realicen con su código de usuario, por lo que está expresamente prohibido ceder o comunicar la contraseña a otros.

Asignación de contraseñas: La longitud mínima de la contraseña será de 8 caracteres. La inicial serán 8 caracteres generados aleatoriamente. Las contraseña deberán incluir mayúsculas, minúsculas y números. No debe contener el nombre del usuario ni ninguna otra información fácilmente deducible. El número máximo de intentos para introducir la contraseña estará limitado de modo que quede bloqueado temporalmente.

Se hace especial hincapié en que la contraseña es **personal e intransferible**, **no puede comunicarse** a otros, debe ser **distinta** para cada usuario y **cambiada** por una nueva al recibirse la primera atribuida por el Servicio de Informática.

Comunicación de códigos de usuario y contraseñas (para altas nuevas y cambios): Se comunicarán a los usuarios mediante correo interno y nunca por teléfono o fax. La contraseña inicial tendrá que ser modificada en el plazo máximo de 15 días. Al recibir dichos códigos, el usuario debe remitir en el plazo máximo de 15 días, un acuse de recibo en el que además se le recuerda su deber de cumplir las normativas y reglamentos de la universidad.

- Autorización de acceso a datos y recursos.

  - Los usuarios tendrán acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

  - Por el Servicio de Informática se mantiene un directorio de personas autorizadas con indicación de los recursos a los que pueden acceder.

ANEXO V
EXTRACTO LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LEY ORGANICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TITULO I. Disposiciones Generales

Artículo 1. Objeto

La presente Ley Orgánica tiene por objeto garantizar y proteger, 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.

Artículo 3. Definiciones

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad,

grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 5. Derecho a información en la recogida de datos

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o de organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6 , de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia

sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguadar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 10. Deber de secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilita al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con el fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 21. Comunicación de datos entre Administraciones públicas

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvocuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2 b) , la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

TÍTULO V

Movimiento internacional de datos

Artículo 33. Norma general

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

ANEXO VI

RELACION DE RESPONSABLES DE SEGURIDAD, ADMINISTRADORES DE SISTEMAS Y UNIDADES GESTORAS DE FICHEROS

Comité de Seguridad	
Gerente	Enrique Alonso Díaz
Vicegerente de Organización	Javier García Sahagún
Jefe de la Asesoría Jurídica	Rosalia Quintana Moreno
Director del Servicio de Informática	Alfonso Iglesias Martínez
	Tel. 21091
	datospersonales@unican.es
Responsable de Seguridad de ficheros y tratamientos automatizados	
Director del Servicio de Informática:	Alfonso Iglesias Martínez
	Tel. 21082
	alfonso.iglesias@unican.es
Administradores de Sistemas y Seguridad	
Administradores de sistemas y seguridad • Jefe del Área de Sistemas y Servicios de Red	Domingo Fernández García Tel 21084 domingo.fernandez@unican.es
• Jefe del Área de Informática de Gestión	Fco. Javier López Fernández Tel. 21081 javier.lopez@unican.es
Responsables de unidades gestoras de ficheros	
• **Personal y Nóminas**	
Jefe del Servicio de PDI, Retribuciones y Seguridad Social	Ángel Carral Sáinz
	Tel. 21021
	angel.carral@unican.es

Jefe del Servicio de PAS, Formación y Acción Social	Carmen Sopeña Pérez
	Tel. 21075
	carmen.sopena@unican.es
- Subfichero Planificación	
Técnico del Gabinete de Plantilla	Jesús Ruiz Lanza
	Tel. 2068
	jesus.ruiz@unican.es
• **Prevención de Riesgos Laborales**	
Jefe del Servicio de Infraestructuras	Vicente Fernández Navarro
	Tel. 21030
	vicente.fernandez@unican.es
• **Alumnos y Títulos**	
Jefe del Servicio de Gestión Académica:	Luz Sánchez Salces
	Tel 21056
	luz.sanchez@unican.es
- Subfichero Relaciones Internacionales	
Directora de la Oficina de R.I.	Gemma Castro González
	Tel. 21038
	gemma.castro@unican.es
• **Cursos de Verano**	
Administradora de los Cursos de Verano	Jacqueline Hoya Bolado
	Tel. 20976
	jacqueline.hoyal@unican.es
• **Investigación**	
Jefa del Servicio de Gestión de la Investigación	Marianela Beivide Palacio
	Tel. 21057
	marianela.beivide@unican.es
- Subficheros Grupos de Investigación y Resultados	
Director de la OTRI	José María Desire Fernández
	Tel. 21029
	josem.desire@unican.es

• **Gestión Presupuestaria y Contable**	
Jefe del Servicio Financiero y Presupuestario	José Luis Santos Pérez
	Tel. 22272
	joseluis.santos@unican.es
– Subfichero Terceros/Sorolla)	
Jefe del Servicio de Contabilidad	Javier González Moradillo
	Tel 21025
	Javier.gonzalez@unican.es
– Subfichero Gestión Económica	
Jefa del Servicio de Gestión Económica, P. y C.	Ana Quijano Álvarez
	Tel. 21210
	ana.quijano@unican.es
• **Control de accesos y seguridad**	
Jefe del Servicio de Infraestructuras	Vicente Fernández Navarro
	Tel. 21030
	vicente.fernandez@unican.es
• **Videovigilancia**	
Jefe del Servicio de Infraestructuras	Vicente Fernández Navarro
	Tel. 21030
	vicente.fernandez@unican.es
• **Biblioteca Universitaria**	
Directora de la Biblioteca	María Jesús Sáiz Vega.
	Tel. 21194
	maria.saiz@unican.es
• **Deportes**	
Directora del Servicio de Actividades Físicas y Deportes	Begoña García Fernández
	Tel. 21885
	begoña.garcia@unican.es
• **Centro de Idiomas**	
Administradora del CIUC	Elena Laliena Aguarta
	Tel. 21213
	elena.laliena@unican.es

• **COIE**	
Director del COIE	Roberto Revuelta San Julián
	Tel. 21414
	roberto.revuelta@unican.es
• **Protocolo**	
Jefa de la Unidad de Protocolo	Alfonso Díaz Bezanilla
	Tel. 21010
	a.diaz@unican.es
• **Asesoría Jurídica**	
Jefe de la Asesoría Jurídica	Rosalía Quintana Moreno
	Tel. 21097
	rosalia.quintana@unican.es
• **Escuela Infantil**	
Directora	Olga Meng González
	Tel. 22070
	Olga.meng@unican.es
• **Orientación Universitaria**	
Técnico de Orientación Psicológica	María Luisa Rosiach Galicia
	Tel. 22024
	luisa.rosiach@unican.es
• **Defensor Universitario**	
Director de la Oficina del Defensor Universitario	Andrés Lebeña Bada
	Tel. 22022
	andres.lebena@unican.es

ANEXO VII

GLOSARIO DE TERMINOS UTILIZADOS EN ESTE MANUAL

- Administrador de sistema y seguridad: es el encargado de administrar y monitorizar el correcto funcionamiento del sistema, incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo. También deberá implementar las medidas de seguridad necesarias en los ficheros de su responsabilidad.

- Afectado / Interesado: es la persona física titular de los datos que son objeto de tratamiento.

- Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

- Consentimiento del afectado/interesado: es aquella manifestación de voluntad (libre, inequívoca, específica e informada) mediante la que el afectado consiente el tratamiento de los datos personales que le conciernen.

- Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

- Deber de confidencialidad: quienes intervengan en el tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, aun después de finalizar sus relaciones con el titular o el responsable del fichero.

- Derechos de acceso, cancelación y rectificación: los interesados tienen derecho a solicitar el acceso, la cancelación o la rectificación de los datos personales recogidos en ficheros, y a que se hagan efectivos esos derechos en el plazo de 10 días por parte del responsable del fichero.

- Documento de seguridad: se trata de la normativa de seguridad del fichero, que es de obligado cumplimiento para todo el personal con acceso a los datos personales automatizados y a los sistemas de seguridad.

- Encargado de tratamiento: persona física o jurídica, autoridad pública o cualquier otro organismo que solo o conjuntamente con otros trate datos personales por cuenta del responsable del tratamiento o fichero como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y que delimita el ámbito de su actuación para la prestación de un servicio a dicho responsable. Podrán también ser encargados de tratamiento los entes sin personalidad juridica que actúen en el tráfico como sujetos diferenciados.

- Fichero: todo conjunto organizado de datos de carácter personal que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Lo son exclusivamente las indicadas en el art. 3 j) de la Ley.

- Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- Registro de incidencias: es el soporte en el que se recogen las incidencias producidas en el tratamiento de los datos personales, su tipo, el momento en que se producen, etc.

- Responsable del fichero: es la persona o entidad responsable de decidir sobre la finalidad, contenido y uso del tratamiento de los datos en el fichero. En nuestro caso, quien tiene esta responsabilidad formal es el Gerente.

- Comité de Seguridad: es la órgano encargado de implantar, coordinar y controlar las medidas de seguridad establecidas en el documento de seguridad aplicables a todos los ficheros de la Universidad de Cantabria.

- Responsable de seguridad de ficheros o tratamientos automatizados: persona designada en el documento de seguridad para coordinar, controlar y ejecutar las medidas definidas en el mismo para los ficheros o tratamientos automatizados.

- Responsable de la unidad gestora del fichero: Es la persona responsable de la unidad que gestiona administrativamente el fichero, utilizándolo para las funciones propias de la misma, sin perjuicio de que para un mismo fichero declarado exista más de un subfichero, en cuyo caso sus obligaciones y funciones se referirán al subfichero correspondiente.

- Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.