MANUAL DE GESTION INTERNA Y NORMAS DE SEGURIDAD SOBRE PROTECCION DE DATOS DE CARÁCTER PERSONAL

VERSIÓN 06/05/2020

ÍNDICE

1. INTRODUCCION

La Universidad de Cantabria lleva a cabo diversas actividades de tratamiento que recogen un gran número de datos personales, necesarios para cumplir sus funciones, y relativos fundamentalmente a estudiantes, personal y proveedores.

Estos datos de carácter personal están protegidos de acuerdo con las exigencias del Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de éstos y su corrección de errores (en adelante RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

El objetivo de este manual es resumir las normas y procedimientos que está obligado a conocer todo el personal de la UC, en especial, aquel que trate con datos de carácter personal.

Asimismo, cada persona debe responsabilizarse de cumplir con las normas y procedimientos internos de la UC relativos a la protección de datos personales de acuerdo con las funciones asignadas a su puesto de trabajo.

2. CUESTIONES BÁSICAS DEL REGLAMENTO EUROPEO DE PROTECCION DE DATOS

La protección de las personas físicas en relación con el tratamiento de los datos personales es un derecho fundamental tal y como se indica en el RGPD.

Las principales cuestiones respecto a la normativa europea y estatal son las siguientes:

- **Registro de actividades de tratamiento**: los responsables del tratamiento deben llevar, publicar y mantener actualizado un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad.

  La documentación informativa completa de las actividades de tratamiento de datos personales figura en un apartado específico de la web institucional de la Universidad de Cantabria:

  https://web.unican.es/consejo-direccion/gerencia/rgpd/actividades-de-tratamiento

- **Principio de transparencia**: en la recogida de datos, el responsable del tratamiento debe informar al interesado, con suficiente claridad y sencillez, de forma exhaustiva sobre la naturaleza y condiciones del tratamiento y debe aportarle la información necesaria para posibilitar el ejercicio de sus derechos.

- **Análisis del riesgo y evaluación de impacto**: el responsable del tratamiento debe identificar, evaluar y gestionar los riesgos de los tratamientos que se pretendan realizar. En este sentido, aquellos tratamientos que conlleven elevados riesgos para los derechos y libertades de los interesados requieren de una Evaluación de Impacto.

- **Comunicación de los incidentes de seguridad a la Autoridad de Control (AEPD):** el responsable del tratamiento tiene la obligación de comunicar, en un plazo no superior a 72 horas, las brechas de seguridad que se produzcan a la Autoridad de Control y, siempre que sea posible, notificárselo a los interesados afectados. La notificación a la AEPD se realizará a menos que sea improbable que dicha incidencia constituya un riesgo para los derechos y libertades de las personas.

- **Derechos de los interesados**: se amplían los derechos de los interesados, además de los ya existentes (derecho de acceso, de rectificación, de supresión, de limitación, portabilidad y de oposición).

3. TÉRMINOLOGÍA Y CONCEPTOS BÁSICOS

1. **Datos personales**:

   Toda información sobre una persona física identificada o identificable; se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

2. **Tratamiento:**

   Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

3. **Responsable del tratamiento:**

   La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derechos de la Unión o de los Estados miembros.

   En el caso de la Universidad de Cantabria, el responsable de las actividades de tratamiento es el Gerente, a excepción de la actividad de tratamiento "Defensor Universitario" cuyo responsable es el propio Defensor Universitario.

4. **Encargado del tratamiento:**

   La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

5. **Violación de la seguridad de los datos personales:**

   Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

6. **Datos relativos a la salud:**

   Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre el estado de salud.

7. **Consentimiento del interesado:**

   Toda manifestación de voluntad libre, específica, informada o inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.

4. ESTRUCTURA ORGANIZATIVA

La estructura organizativa para la gestión de la seguridad de la información y la protección de datos de carácter personal en la Universidad de Cantabria está compuesta por los siguientes órganos:

a) COMITÉ DE SEGURIDAD

Órgano colegiado que dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de seguridad de la información.

b) COMISIÓN DELEGADA DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Órgano colegiado que garantiza las actuaciones necesarias en cuanto a la supervisión del cumplimiento de la normativa de protección de datos personales y de la política de seguridad de la información. Tiene encomendada igualmente la resolución de consultas planteadas, tanto de las unidades gestoras como del personal en materia de protección de datos personales, así como la función de gestionar e impulsar la tramitación de las solicitudes de ejercicio de derechos y, finalmente, la de trasladar al Comité de Seguridad de la Información las propuestas de normas necesarias en la materia.
Correo electrónico: seguridaddelainformacion@unican.es

c) DELEGADA DE PROTECCIÓN DE DATOS

El delegado de protección de datos (DPD) es quien, entre otras funciones, se encarga de supervisar el cumplimiento de la normativa, asesorar al responsable del tratamiento y gestionar las consultas de las personas que se pongan en contacto con el mismo en relación con el tratamiento de datos personales.
Correo electrónico: dpd@unican.es

5. PRINCIPIOS DEL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL

Todo tratamiento de datos de carácter personal deberá cumplir los principios establecidos en el artículo 5 del RGPD:

- **Licitud, lealtad y transparencia:**

  Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado, lo cual significa que se llevará a cabo conforme a las disposiciones legales de aplicación, y de acuerdo con la información proporcionada al interesado, de forma transparente para el mismo, transparencia que implica que los

interesados deben recibir información suficientemente clara sobre el tratamiento de sus datos personales y del modo de hacer valer sus derechos en relación con dicho tratamiento.

- **Limitación de la finalidad:**

  Los datos se deben de recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. El tratamiento ulterior de los datos personales con fines de archivo en interés público o fines de investigación científica e histórica no se considerará incompatible.

- **Minimización de datos:**

  Los datos deben de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

- **Exactitud:**

  Los datos deben ser exactos, y si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

- **Limitación del plazo de conservación:**

  Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales, y para determinar las posibles responsabilidades que se pudieran derivar del mismo, además de los periodos que se establezcan en materia de archivos y documentación públicos.

- **Integridad y confidencialidad:**

  Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas técnicas y organizativas de control apropiadas.

6. BASES JURÍDICAS DE LOS TRATAMIENTOS DE DATOS PERSONALES

Según indica el artículo 6.1 del RGPD, el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Las bases jurídicas de los tratamientos de datos personales que realiza la Universidad de Cantabria pueden consultarse en el registro de actividades de tratamiento:

https://web.unican.es/consejo-direccion/gerencia/rgpd/actividades-de-tratamiento

7. INFORMACIÓN QUE DEBE FACILITARSE A LOS INTERESADOS

En el momento en que se obtengan datos personales, bien directamente del interesado o bien indirectamente, deberá facilitarse al interesado la información que establece en el artículo 13 y 14 del RGPD, en relación con el artículo 11 de la LOPDGDD.

Dicha información se incluirá en los formularios o procesos de recogida de datos salvo que al interesado ya se la haya informado previamente sobre las condiciones en que se realiza el correspondiente tratamiento.

En la Universidad de Cantabria el modelo de información básica y adicional que se debe facilitar a los interesados es el siguiente:

MODELO TIPO DE INFORMACIÓN BÁSICA Y ADICIONAL A FACILITAR A LOS INTERESADOS EN LOS PROCESOS DE RECOGIDA DE DATOS

	INFORMACIÓN BÁSICA	INFORMACION ADICIONAL
Responsable del tratamiento	Identidad del responsable del tratamiento	Datos de contacto del responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos.
Finalidad del tratamiento	Descripción sencilla de los fines del tratamiento, incluso la elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
Legitimación del tratamiento	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo
		Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios de cesiones o transferencias	Previsión o no de cesiones	Destinatarios o categorías de destinatarios
	Previsión de transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
Derechos de las personas interesadas	Referencia al ejercicio de derechos	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de control
Procedencia de los datos	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

La documentación informativa completa sobre las actividades de tratamiento de datos que realiza la Universidad de Cantabria puede consultarse en la siguiente dirección:

https://web.unican.es/consejo-direccion/gerencia/rgpd/actividades-de-tratamiento

La creación o modificación de actividades de tratamiento, en todo caso, se realizará conforme al Protocolo para la creación o modificación de actividades de tratamiento en el marco del Reglamento (UE) 2016/679 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 (Anexo 1).

8. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS

Especial protección merece el tratamiento de **categorías especiales de datos** (origen étnico o racial, opiniones políticas, convicciones religiosas o políticas, afiliación sindical, datos genéticos y biométricos, datos relativos a la salud o datos relativos a la vida u orientación sexual de una persona física), en la medida en que su tratamiento puede entrañar importantes riesgos para la garantía de sus derechos y libertades.

Para el tratamiento de estas categorías especiales de datos la Comisión de Seguridad ha establecido una serie de recomendaciones que pueden consultarse en la siguiente página de la Intranet:

https://intranet.unican.es/unidades/lopd/Documents/INSTRUCCIONES%20CATEGORIAS%20ESPECIALES%20DE%20DATOS.pdf

Asimismo, si se va a realizar un tratamiento que contenga imágenes deberá seguir las recomendaciones dictadas por la Comisión de Seguridad en la siguiente dirección:

https://intranet.unican.es/unidades/lopd/Documents/RECOMENDACIONES%20PARA%20LA%20TOMA%20DE%20IMÁGENES%20Y%20GRABACIÓN%20DE%20VIDEO.pdf

En todo caso, el tratamiento de los datos pertenecientes a categorías especiales, citados al principio, deberá basarse en alguno de los supuestos previstos en el artículo 9 del RGPD, que de forma resumida son los siguientes (se reseñan los de aplicación más probable en el ámbito de la Universidad):

- Consentimiento explícito del interesado (salvo la excepción prevista en el artículo 9.1 de la LPDGDD, en cuyo caso el consentimiento no es suficiente);
- Tratamiento necesario para el cumplimiento de obligaciones en el ámbito del Derecho Laboral y de la seguridad y protección social;
- El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones;
- El tratamiento es necesario por razones de interés público esencial, sobre la base del Derecho estatal o de la Unión Europea;

- El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica, sobre la base del Derecho estatal o de la Unión Europea.

9. PROCEDIMIENTO PARA LA CESIÓN Y/O COMUNICACIÓN DE DATOS A TERCEROS

La Universidad de Cantabria solo realizará los tratamientos de datos y las cesiones de estos a terceros que estén previstas en las leyes y otras normas de obligado cumplimiento dictadas en desarrollo de las primeras o amparadas en ellas, las derivadas del desarrollo de las relaciones jurídicas que tenga establecidas con los interesados y de la prestación de los servicios que se le soliciten, las necesarias para el cumplimiento de las finalidades, misión en interés público y obligaciones legales o ejercicio de potestades públicas que tiene encomendadas, en particular las comunicaciones necesarias a otras administraciones públicas para el ejercicio de las competencias propias de éstas sobre las mismas materias. El registro de actividades de tratamiento de la Universidad de Cantabria contiene las cesiones de datos que se realizan.

Todas estas comunicaciones tienen su base legal en los supuestos del artículo 6.1 del Reglamento, según lo previsto en el artículo 8.2 de la LOPDGDD y en la Normativa Propia de la UC de Protección de Datos Personales

Igualmente, procederá el tratamiento o comunicación de datos personales cuando disposiciones específicas así lo establezcan.

En cualquier otro supuesto, solo se podrán realizar tratamientos o comunicaciones de datos personales a terceros con el consentimiento del interesado.

En el proceso de recogida de datos se informará a los interesados de cuanto establece el artículo 13 del RGPD y en especial de las bases jurídicas que legitimen el tratamiento, así como de los destinatarios o categorías de destinatarios de los datos personales, quedando en ese momento de manifiesto el consentimiento del interesado, si fuere preciso.

El tipo de comunicaciones y cesiones de datos y los procedimientos para realizarlas vienen indicados con más profundidad en los artículos 10 y 11 de la Normativa propia de la Universidad de Cantabria de protección de datos de carácter personal.

En el caso de que se produzca la cesión de datos o la comunicación de datos a terceros a través del correo electrónico, los ficheros deberán ser comprimidos y encriptados. En este caso, la clave de encriptación deberá ser facilitada a la persona autorizada del organismo o entidad receptora a través de un medio distinto al utilizado para la transmisión.

10. DERECHOS DE LAS PERSONAS INTERESADAS

Los interesados podrán ejercer ante el responsable del tratamiento los siguientes derechos en los términos y condiciones previstas en los artículos 15 al 22 del RGPD:

Derecho de acceso
Derecho a conocer si sus datos están siendo objeto de tratamiento, los fines del tratamiento, las categorías de los datos, la identificación de los destinatarios o categorías de destinatarios, el plazo de conservación previsto o la existencia de decisiones automatizadas, así como información disponible del origen de los datos cuando no se hayan obtenido del interesado.

Derecho de rectificación
Derecho a obtener del responsable del tratamiento la modificación de aquella información que le concierne y que resultara inexacta o incompleta, sin dilación indebida, así como a que se completen los datos personales que sean incompletos, habida cuenta de los fines del tratamiento. El interesado deberá acompañar documentación justificativa de la inexactitud o carácter incompleto de los datos.

Derecho de supresión
Derecho a que se eliminen sus datos cuando, entre otros, ya no sean necesarios para los fines que fueron recogidos, el titular retire su consentimiento o se haya producido un tratamiento ilícito.

Derecho de limitación
Derecho a que se restrinja el tratamiento de los datos que le afecten cuando por ejemplo se haya ejercido el derecho de rectificación o el de oposición y se esté pendiente de verificación por parte del responsable del tratamiento.

Derecho de portabilidad
Derecho a obtener sus datos personales en un formato estructurado, de uso común y de lectura mecánica, con el fin de poder trasladarlos a otro responsable del tratamiento.

Derecho de oposición
Derecho a que se dejen de tratar por el responsable los datos que le conciernen cuando se base el tratamiento en misión en interés público, o ejercicio de poderes públicos, aunque en determinados supuestos se podrá llevar a cabo una ponderación entre los intereses en juego: en concreto, el responsable del tratamiento podrá acreditar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado.

Modo de ejercitar de los derechos

El responsable del tratamiento estará obligado a informar al interesado sobre los medios a su disposición para ejercer los derechos que le corresponden. En la Universidad de Cantabria esta información se proporciona a través de la información básica y adicional que se facilita en la recogida de datos, así como en su página web institucional. De acuerdo con los procedimientos establecidos en nuestra Universidad, se pueden ejercitar los derechos mencionados anteriormente mediante las siguientes vías:

a) Accediendo a la Sede Electrónica de la Universidad de Cantabria.
b) Entregando el formulario de solicitud impreso, debidamente cumplimentado, en la Oficina de Asistencia en Materia de Registros (OAMR) de la Universidad de Cantabria sita en: Pabellón de Gobierno. Avda. de los Castros nº 54. 39005 Santander (Cantabria)o por cualquiera de los medios previstos en el artículo 16 de la Ley 39/2015.
c) Enviando el formulario firmado electrónicamente a la siguiente dirección: a: seguridaddelainformacion@unican.es

El procedimiento para la gestión interna de las solicitudes de ejercicio de derechos obedece a una serie de pautas comunes, que básicamente se refieren al análisis inicial de la petición por la Comisión de Seguridad, la intervención vía informe de las unidades gestoras de los datos sobre los que se ejercita el derecho y, en su caso, posteriormente para llevar a efecto lo solicitado, y la resolución por el responsable del tratamiento previa supervisión de la propuesta por la persona Delegada de Protección de Datos.

Podrá encontrar más información sobre el procedimiento de ejercicio de derechos de las personas interesadas en la Normativa reguladora del ejercicio de los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad de los datos de carácter personal recogidos en tratamientos de la Universidad de Cantabria.

11. COMUNICACIÓN DE BRECHAS DE SEGURIDAD

Se entiende por **brecha de seguridad o violación de la seguridad** de los datos personales todo aquel incidente de seguridad que provoque la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

El artículo 33 del RGPD establece la **obligación por parte del responsable del tratamiento de notificar a la autoridad de control competente (AEPD) cualquier brecha de seguridad,** sin dilaciones indebidas y en todo caso en un **plazo máximo de 72 horas,** a menos que sea improbable que la brecha constituya un riesgo para los derechos y libertades de las personas físicas.

Las incidencias más habituales, según Informe de notificaciones de brechas de seguridad de la AEPD (Sumario de 2018), son las siguientes:

- Dispositivo perdido/robado,
- Documentación perdida/robada,
- Hacking: virus, gusanos, troyanos, etc.
- Malware: programa malicioso, software dañino, código maligno.
- Phishing: técnica que persigue el engaño para conseguir información confidencial.
- Datos personales mostrados.
- Datos personales enviados.

Es importante **informar lo antes posible** si se detecta cualquier tipo de incidencia que afecte a la seguridad de la información de datos de carácter personal, para ello existen dos vías de comunicación:

a) Formulario Intranet UC en el siguiente enlace: https://intranet.unican.es/unidades/lopd/incidencias

b) Remitir un correo a la Comisión de Seguridad: seguridaddelainformacion@unican.es

Una vez remitida la incidencia, la Comisión de Seguridad se encargará de realizar el seguimiento de la brecha de seguridad, y si lo considera necesario (en la medida que sea probable que dicha brecha constituya un riesgo para los derechos y libertades de las personas), se notificará a la autoridad de control y, en su caso, a los interesados afectados.

12. FUNCIONES Y OBLIGACIONES DEL PERSONAL

El derecho a la protección de datos personales es de obligado cumplimiento y respeto tanto por las autoridades públicas como terceros privados, estando especialmente obligados todo aquél que trate datos personales.

Todo el personal de la UC que intervenga en alguna fase de la recogida y del tratamiento de datos personales o de cualquier modo pueda tener acceso a ellos, está obligado al secreto profesional respecto de dichos datos y al cumplimiento de las obligaciones legales establecidas, obligaciones que subsistirán aun después de finalizar su relación con la Universidad de Cantabria.

En este sentido, todo el personal de nuevo ingreso de la Universidad deberá firmar un compromiso de confidencialidad según el modelo aprobado. Igualmente, deberán suscribir dicho compromiso aquellos otros colectivos o personas no incluidos en la categoría anterior pero que puedan tener acceso a datos personales.

El deber de secreto vincula a todos los colectivos anteriormente expresados, con independencia de haber cumplido o no con la obligación formal de suscribir el compromiso de confidencialidad referido en el párrafo anterior.

Todo el personal de la Universidad de Cantabria tiene el deber de conocer y cumplir sus funciones y obligaciones en relación con el tratamiento y la protección de los datos de carácter personal, que se recogerán y especificarán en el documento de seguridad de la Universidad y en este manual de gestión interna y normas de seguridad y al que tendrá acceso todo el personal y sobre cuyas posibles actualizaciones se le mantendrá informado. En todo caso, todo el personal está obligado a conocer la normativa interna de la Universidad de Cantabria y este manual constituye únicamente un instrumento para facilitar el conocimiento de los aspectos básicos de la misma.

Las funciones y obligaciones del personal de la UC están indicadas en el Documento de Seguridad (DS 04-010):

https://intranet.unican.es/unidades/lopd/Documents/FuncionesyobligacionesdelpersonalPDF

El incumplimiento de las obligaciones establecidas en el manual de normas de seguridad y en la normativa interna relacionada con la protección de datos personales, así como lo establecido en el Reglamento Europeo de Protección de datos (RGPD) y en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), podrá ser sancionado de acuerdo con la legislación laboral y el régimen disciplinario aplicable a funcionarios.
Cualquiera de las conductas contempladas en los artículos 72 a 74 de la LOPGDD podrá quedar subsumida en alguna de las infracciones previstas en los regímenes disciplinarios de personal laboral y personal funcionario.

13. VEINTE BUENAS PRÁCTICAS GENERALES

Las recomendaciones que aparecen a continuación deben ser aplicadas al tratamiento de la información en general, y con especial atención, a los datos de carácter personal en cumplimiento de la normativa relativa a dichos datos.

1. Guarde el debido secreto y confidencialidad sobre la información que conozcan en el desarrollo del trabajo. Esta obligación de guardar secreto subsistirá aún después de finalizar las relaciones contractuales con la Universidad.

2. No saque información ni datos personales de las dependencias de la UC salvo en los casos que lo requieran las funciones asignadas y, en su caso, previa autorización y con los controles que se hayan establecido.

3. Bloquee el equipo con contraseña o desconectándose de las aplicaciones y la red, y apagando el monitor, cuando se abandone el puesto de trabajo.

4. Cierre con llave los armarios de archivo cuando no les esté utilizando, especialmente si contienen categorías especiales de datos (datos de salud, discapacidad, etc.).

5. En caso de pérdida o robo de un dispositivo de almacenamiento móvil (portátil, teléfono, memoria USB, etc.) deberá notificarse inmediatamente como incidencia de seguridad.

6. Si dispone de un dispositivo de almacenamiento móvil, se recomienda el cifrado de los datos, mantener una copia de los datos en otro soporte, contar con una contraseña de bloqueo de pantalla y/o autenticación de usuario en el dispositivo.

7. En caso de detectar cualquier indicio de problema de seguridad, inmediatamente debe poner el mismo en conocimiento de la Comisión de Seguridad por correo electrónico: seguridaddelainformacion@unican.es

8. No realice acciones que puedan poner en peligro la seguridad de la información (envío de información a través de correo electrónico sin las suficientes medidas de seguridad, …).

9. Es muy importante que no almacene ni trate datos de carácter personal en el disco duro del equipo, sino en las unidades de red de la Universidad para garantizar su conservación y evitar accesos no autorizados.

10. Se debe de cumplir la política de contraseñas establecida, especialmente la periodicidad de cambio (obligatorio una vez al año y recomendación de hacerlo con mayor frecuencia) y utilizar contraseñas de al menos ocho caracteres que combinen números, letras (mayúsculas y minúsculas) y caracteres especiales.

11. No anote o guarde las contraseñas en lugares visibles o fácilmente accesibles. Está expresamente prohibido ceder o comunicar la contraseña a otros (así como aceptarla) incluso del mismo departamento o centro de trabajo y debe custodiarse debidamente, y no teclearse bajo la mirada de otros.

12. Responsabilícese de la confidencialidad de sus contraseñas y, en caso de que sean conocidas fortuita o fraudulentamente por otras personas, debe comunicarlo como incidencia de seguridad.

13. Respecto al correo electrónico e Internet, se debe prestar atención al envío de datos de carácter personal por medio del correo electrónico. Se evitará indicar datos

personales en el cuerpo del mensaje y que los anexos que contengan datos de carácter personal deberán ir cifrados.

14. No envíe o transmita mensajes difamatorios, calumniadores, amenazantes o abusivos o cualquier mensaje que puede interpretarse como tal.

15. No abra correos procedentes de direcciones desconocidas o que no estén relacionados con motivos de trabajo y ofrezcan las suficientes garantías, para evitar la entrada de virus, troyanos o código malicioso.

16. No utilice el correo corporativo para finalidades distintas a las del puesto de trabajo.

17. Utilice CCO (enviar con copia oculta) cuando se envía a diferentes destinatarios con el fin de ocultar la visualización de las diferentes direcciones de correo.

18. Cada vez que se ausente de su mesa de trabajo o bien cuando termine su jornada laboral, deberá retirar toda aquella información que contengan datos que pudiera ser de carácter confidencial.

19. Al utilizar los escáneres/fotocopiadoras compartidas, debe asegurarse de recoger los documentos originales y, en el caso del escáner, si la carpeta de destino se comparte con usuarios sin acceso a esos datos personales, eliminar el archivo cuanto antes de esa carpeta.

20. No tire a la papelera ningún documento con datos personales ni CD o DVD sin antes destruirlo, para ello utilizar los dispositivos destinados al efecto para desechar el material como las destructoras de papel.

14. PREGUNTAS FRECUENTES

¿Dónde puedo informarme sobre protección de datos?

Puede informarse sobre protección de datos tanto en la página principal de la Universidad de Cantabria, apartado RGPD: https://web.unican.es/consejo-direccion/gerencia/rgpd/politica-general-de-proteccion-de-datos-en-la-universidad-de-cantabria, como en la Intranet de la UC, donde existe un área temática interna llamada Ley Orgánica de Protección de datos: https://intranet.unican.es/unidades/lopd

¿Dónde puedo consultar dudas sobre protección de datos?

Existe dos buzones para poder remitir sus consultas en materia de información y protección de datos de carácter personal:

- Buzón Comisión de Seguridad: seguridaddelainformacion@unican.es
- Buzón Delegada de Protección de datos: dpd@unican.es

¿Cómo se deben publicar datos con carácter personal?

Como se indica en la Disposición Adicional séptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales "*cuando sea necesario la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.*

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente".

¿Puedo ceder o comunicar los datos de que disponga a terceros?

Para ello deberá consultar los supuestos reflejados en los artículos 10 a 17 sobre comunicaciones y acceso de datos por parte de terceros de la Normativa propia de la Universidad de Cantabria de protección de datos de carácter personal.

¿Se pueden publicar las calificaciones de estudiantes?

La Agencia Española de Protección de Datos (AEPD), en un reciente Informe de fecha 21/05/2019, considera lícita la publicación de las calificaciones de los estudiantes, sin necesidad de contar con su consentimiento expreso (Informe 30/2019), sin embargo, deberán respetarse en todo caso los principios recogidos en el artículo 5 del RGPD, y los siguientes criterios:

1. No se deberá realizar la publicación en internet, de ese modo, se excluye la posibilidad de un conocimiento generalizado de las calificaciones.
2. El medio preferente para proceder a dicha publicación será intranet o en un aula virtual con acceso limitado (matriculados en las asignaturas) *
3. Los datos deberán publicarse con nombre, apellidos y cuatro cifras aleatorias del DNI o documento equivalente.
4. En caso de que no fuera posible, podrá realizarse en los tablones de los anuncios, siempre que no se encuentren en zonas comunes y se adopten las medidas necesarias para evitar su público conocimiento.
5. Respecto al plazo de las publicaciones, en el caso de las calificaciones provisionales mientras transcurra el plazo para presentar las reclamaciones y las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.

* La UC está adecuando sus sistemas informáticos para que la publicación sea sólo accesible por los estudiantes matriculados en la asignatura.

¿Qué hacer si recibimos una inspección de la Agencia Española de Protección de datos?

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

Preguntas frecuentes publicadas por la AEPD

ANEXO 1. PROTOCOLO PARA LA CREACIÓN O MODIFICACIÓN DE ACTIVIDADES DE TRATAMIENTO

1. La creación o modificación de una actividad de tratamiento deberá ser autorizada previamente por el Gerente de la Universidad de Cantabria como responsable de las actividades de tratamiento de la institución (a excepción de la actividad de tratamiento "Defensor del Universitario").

2. El Comité de Seguridad de la Información de la UC designará una comisión que se encargará de analizar las propuestas de creación o modificación de actividades de tratamiento de datos personales y proponer al Gerente la resolución correspondiente.

3. La propuesta de creación o modificación de actividades de tratamiento será formulada por el responsable del servicio o unidad que vaya a tratar los datos personales de acuerdo con el modelo que se acompaña a este protocolo y se dirigirá al Comité de Seguridad de la Información con sede en la Gerencia de la UC.
4. La Comisión analizará que la propuesta se ajusta a lo previsto en el RGPD (base legal, finalidades, tipo de datos a tratar, posibles riesgos asociados al tratamiento y medidas organizativas y de seguridad aplicables) y elaborará una propuesta que será sometida al informe del Delegado de Protección de Datos.

5. Si el informe es favorable a la creación o modificación de la actividad de tratamiento, la Comisión recabará del responsable de la actividad de tratamiento la documentación relacionada con la información que se va a facilitar a los interesados, el modelo de consentimiento para el tratamiento de datos y, en su caso, la propuesta de contrato con los encargados de tratamiento.

6. Finalmente, a la vista del informe y de la documentación indicada en el punto anterior, la Comisión propondrá al Gerente la resolución de creación o modificación de la actividad de tratamiento o, en su caso, la denegación motivada de la solicitud.

7. El Comité de Seguridad de la Información aprobará un protocolo para la creación de actividades de tratamiento vinculadas a proyectos de investigación.