# Reglamento de uso de Recursos TIC en la Universidad de Cantabria

**Aprobado en CG 26/09/2025**

Contenido

## Artículo 1: Aspectos generales

Las Tecnologías de la Información y de las Comunicaciones (TIC) facilitan el acceso a servicios y recursos tanto dentro como fuera de la Universidad de Cantabria y permiten la comunicación con usuarios de todo el mundo.

La Universidad de Cantabria promueve y estimula el uso de las TIC, respeta la privacidad de los usuarios y asume como principio que la comunidad universitaria hace un uso responsable, ético, legal y eficiente de los recursos que la institución pone a su disposición.

El Consejo de Gobierno de la Universidad de Cantabria, en su sesión ordinaria de 18 de julio de 2024, aprobó la Política de Seguridad de la Información, cumpliendo así la exigencia del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Dicha Política prevé en su estructura normativa el desarrollo de un "Reglamento de uso de Recursos TIC", que será conocido por y estará a disposición de todos los miembros de la universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Las normas más específicas se concretarán en normativas y procedimientos de seguridad, que serán aprobados de acuerdo con lo indicado en la Política de Seguridad de la Información.

El propósito de este Reglamento de uso de los recursos de Tecnologías de la Información y de las Comunicaciones de la Universidad de Cantabria es garantizar que dichos recursos serán utilizados para el desarrollo de las funciones y competencias propias de la misma, conforme a lo establecido en sus Estatutos.

Son objetivos de este Reglamento:

1. Proteger el prestigio y el buen nombre de la Universidad de Cantabria.
2. Garantizar la seguridad, rendimiento y privacidad de los sistemas y comunicaciones tanto de la Universidad de Cantabria como de terceros.
3. Evitar situaciones que puedan causar a la Universidad de Cantabria algún tipo de responsabilidad civil, administrativa o penal.
4. Concienciar a los usuarios de la necesidad de hacer un uso correcto de los recursos y colaborar para que estos sirvan eficazmente a los fines propios de la Universidad.

El desconocimiento de este Reglamento no exime de su cumplimiento. Todos los miembros de la Universidad de Cantabria tienen la obligación de conocer y cumplir tanto la Política de Seguridad de la Información como el Reglamento de uso de recursos TIC, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

## Artículo 2: Ámbito de aplicación

Este Reglamento será de aplicación a todas las personas que utilicen los recursos TIC proporcionados por la Universidad, o que cuenten con sistemas o redes conectadas, directa o indirectamente, a la Red UNICAN. En adelante, estas personas se denominarán "usuarios", con independencia de que tengan o no cuenta de usuario asignada por la Universidad.

A los efectos de este Reglamento, tienen la consideración de “recursos TIC de la UC” todos los sistemas centrales, departamentales, estaciones de trabajo, ordenadores personales, impresoras, redes internas y externas, sistemas multiusuario, servicios de comunicaciones y cualquier otro recurso que sea propiedad de la Universidad o esté conectado, directa o indirectamente, a la Red UNICAN.

Se excluyen expresamente de esta definición los dispositivos particulares cuya conexión a la red universitaria no implique cesión de gestión o administración a la UC, sin perjuicio de las medidas de seguridad que deban cumplir para su uso conforme al Esquema Nacional de Seguridad.

## Artículo 3: Normas de uso

La utilización de los recursos informáticos y servicios de red de la Universidad de Cantabria se ajustará a lo dispuesto en la legislación vigente, especialmente en materia de protección de datos personales, propiedad intelectual e industrial y protección del honor e intimidad y, en su caso, a las normas propias de esta Universidad que resulten aplicables.

Los recursos TIC habrán de ser utilizados de forma adecuada para el intercambio de información de contenido académico, administrativo, educativo o de investigación, relacionado con las actividades propias de la Universidad.

Queda prohibido cualquier uso privado o comercial no autorizado de los recursos TIC de la UC. Esta prohibición aplica a las cuentas, dispositivos y servicios puestos a disposición de los usuarios.

La institución velará por el buen uso de los recursos TIC considerando aspectos como la eficiencia, productividad, utilización y riesgos de seguridad.

Los usuarios deben tener en cuenta que, por razones de mantenimiento, seguridad y cumplimiento de obligaciones legales en materia de registro de actividad, los Sistemas de Información y la propia información que albergan son inventariados y monitorizados por el Servicio de Informática, que mantiene los correspondientes registros informáticos durante los plazos necesarios o legalmente establecido.

Con el fin de asegurar estos objetivos y de garantizar un uso eficiente de dichos recursos, se establece un conjunto de normas y responsabilidades que afectan a los usuarios en relación con la integridad de los citados recursos y el uso adecuado de datos y servicios.

### Artículo 3.1: Sobre la integridad de los recursos

Se prohíbe realizar cualquier acto que interfiera en el correcto funcionamiento de los recursos TIC.

Específicamente:

- Está prohibido causar daños físicos a los equipos o infraestructuras (destrucción, sustracción, traslados no autorizados, ...).
- No se podrá conectar a la red de comunicaciones corporativa ningún dispositivo que no haya sido admitido y habilitado por la institución y siempre deberá contar con configuración establecida por el Servicio de Informática.
- No se permite la instalación de equipos de comunicaciones o aplicaciones para el acceso remoto, comunicación inalámbrica e intercambio de información (rutas, redes, ...) entre sistemas de la Red UNICAN y el exterior, salvo autorización expresa por el Servicio de Informática.

- No está permitido realizar acciones que deterioren o sobrecarguen los recursos TIC, hasta el punto de perjudicar a otros usuarios o al rendimiento general. Esto incluye cualquier tipo de ensayo o experimento que afecte a la infraestructura TIC en producción. Dichos ensayos deberán realizarse exclusivamente en entornos de laboratorio aislados.
- Los usuarios están obligados a adoptar y respetar todas las medidas de seguridad, herramientas y configuraciones que el Servicio de Informática determine para la protección de la integridad de los recursos TIC, incluso aunque tengan capacidad de modificarlas. Asimismo, deberán seguir sus recomendaciones e instrucciones al respecto. En caso de un incidente de seguridad los usuarios deberán notificarlo y colaborar con el Servicio de Informática en su investigación y resolución.

**Artículo 3.2: Sobre accesos no autorizados y uso de datos y contenidos**

Los usuarios no podrán acceder a recursos para los que no estén debidamente autorizados. En todo caso, deberán cumplir las normas específicas que se fijen en cada sistema o servicio, y respetar el material protegido por la normativa de derechos de autor.

Los administradores de los sistemas podrán acceder a la información contenida en los medios digitales facilitados a los trabajadores exclusivamente por motivos de mantenimiento y seguridad, así como para cumplir con las obligaciones en materia de registro de actividad que establece la legislación vigente (Art. 24 del RD 311/2022 de 3 de mayo, que regula el Esquema Nacional de Seguridad).

Asimismo, los administradores de los sistemas, a iniciativa de los órganos competentes de la UC, podrán acceder a dichos medios digitales a efectos de controlar el cumplimiento de las obligaciones laborales y de lo dispuesto en este reglamento y demás normas en materia de uso de recursos TIC.

El acceso al contenido de medios digitales propiedad de la UC de personas fallecidas se llevará a cabo de acuerdo con lo previsto en la normativa de protección de datos personales. Asimismo, se podrá acceder al contenido de esos medios de trabajadores que dejen de pertenecer a la UC, con el fin de recuperar información de interés institucional.

Específicamente:

- Las cuentas de identificación institucionales asignadas son de uso personal e intransferible. Estarán sujetas a su propia normativa de asignación, uso y revocación.
- Las personas que tengan acceso a información de carácter personal deberán tener presente la legislación vigente en la materia, así como obligaciones que conlleva, además de la normativa propia de la Universidad.
- No se permite ocultar o enmascarar ninguna identidad para realizar operaciones en nombre de otro usuario ni suplantar la dirección de red de un equipo usando una distinta de la asignada oficialmente.
- El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata al Servicio de Informática, con el fin de que se le retiren los recursos informáticos que tuviera asignados. Del mismo modo, cuando los medios informáticos o de comunicaciones proporcionados por la Universidad de Cantabria estén asociados al desempeño de un determinado puesto o función, la persona usuaria deberá devolverlos inmediatamente a la unidad responsable al finalizar su vinculación con dicho puesto o función.

- No está permitido realizar de forma intencionada acciones o utilizar sistemas software o hardware cuya finalidad sea la obtención de contraseñas, el acceso a información ajena o la elusión de los sistemas de protección de datos y de seguridad informática. Esto incluye sniffers, scanners de puertos, software de búsqueda de vulnerabilidades, etc. Estas acciones únicamente podrán ser realizadas por personas expresamente autorizadas por el Servicio de Informática para mejorar y mantener la seguridad y la operatividad de los servicios de la Universidad.
- Se prohíbe cualquier actividad que suponga una violación de la privacidad de los datos o el trabajo de los otros usuarios.
- Toda información que se encuentre protegida por derechos de autor que sean titularidad de terceros o que sea propiedad de la Universidad de Cantabria, deberá utilizarse con arreglo a la legislación vigente y a la normativa universitaria. Esto incluye el software licenciado para la Universidad de Cantabria, que no podrá usarse en equipos ajenos a la UC salvo que así lo permita el acuerdo de licencia.
- Se prohíbe la instalación y uso de programas para la descarga e intercambio de material que viole los derechos de autor o cualquier otra regulación legal vigente.
- El correo facilitado por la Universidad de Cantabria, así como las herramientas informáticas, colaborativas y de almacenamiento son exclusivamente para uso profesional. La Universidad de Cantabria se reserva el derecho, previa autorización del Comité de Seguridad de la Información, debidamente justificada y por escrito, a recuperar la información necesaria para el correcto funcionamiento de la Universidad.

**Artículo 3.3: Obligaciones de los usuarios**

- Deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Esta obligación afecta exclusivamente a los equipos propiedad de la Universidad de Cantabria, que es a los que se presta un servicio de soporte técnico.
- Evitarán comportamientos de riesgo que puedan permitir el acceso o propagación de malware en los equipos.
- Apagarán los equipos al finalizar la jornada laboral, tanto por seguridad como por eficiencia energética. El Servicio de Informática facilitará instrucciones y mecanismos que permitan un uso más eficiente de los recursos.
- Deberán notificar al Servicio de Informática, a la mayor brevedad posible, cualquier comportamiento anómalo de su equipo, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad.
- Serán responsables de la información extraída fuera de la organización por medios que les hayan sido asignados (equipos portátiles, dispositivos de almacenamiento extraíble, almacenamiento en la nube, etc.), especialmente cuando se trate de información sensible, confidencial o protegida.
- Se deberán aplicar medidas de seguridad proporcionales a la sensibilidad de la información tratada. El Responsable de Seguridad velará por el cumplimiento de estas medidas.

**Artículo 3.4: Uso aceptable del equipamiento informático propio de la UC**

- Los equipos deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales y tareas asignadas por la Universidad de Cantabria a los usuarios autorizados.
- Se deberán aplicar las configuraciones aprobadas por el Servicio de Informática.
- Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que afecten a la seguridad de los Sistemas de Información de la Universidad de Cantabria.
- Está prohibido alterar cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del Servicio de Informática.
- Será responsabilidad de cada departamento, servicio, unidad o usuario individual el cumplimiento de esta normativa, especialmente en cuanto a las operaciones que se hagan con privilegios de administración y que puedan comprometer la seguridad de la información alojada en la Universidad de Cantabria. El Responsable de Seguridad velará por el cumplimiento de estas medidas.
- Si el personal de soporte técnico detectase cualquier anomalía que indique una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Seguridad, quien tomará las medidas que correspondan.

**Artículo 3.5: Administración e instalación de software en equipos informáticos**

- La instalación y administración de los equipamientos informáticos debe asignarse a personal especialista, con la formación adecuada para garantizar una implementación segura y eficiente, acorde a la normativa.
- Es responsabilidad de los miembros del Servicio de Informática la instalación, administración y mantenimiento del equipamiento de usuario. De manera excepcional y justificada, podrán delegarse dichas funciones a los usuarios que lo soliciten, siempre que acrediten las competencias necesarias y acepten de forma explícita las responsabilidades que conlleva, garantizando en todo momento el cumplimiento de la normativa.
- Los servidores adquiridos por departamentos, áreas o grupos de investigación deberán ser administrados por personal expresamente designado, que será responsable de las tareas de administración y mantenimiento, de acuerdo con este Reglamento y los procedimientos y normas de seguridad que se aprueben.

**Artículo 3.6: Recursos de almacenamiento de información**

Respecto al uso de los recursos de almacenamiento facilitados por la Universidad de Cantabria se tendrán en cuenta las siguientes consideraciones:

- Estudiantes: Solo podrá utilizar los recursos facilitados por la Universidad de Cantabria para fines estrictamente relacionados con su actividad universitaria. El acceso a dichos recursos será deshabilitado al acabar la relación con la Universidad.

- Empleados o personal vinculado a la UC con cuenta institucional: Solo podrá utilizar los recursos para fines estrictamente profesionales. El acceso a dichos recursos será deshabilitado al acabar la relación con la Universidad.

Se considerará que la relación con la Universidad finaliza:

- En el caso de empleados o personal vinculado con cuenta institucional, por cese o finalización del contrato, cualquiera que sea su causa. Además, cuando desaparezca el vínculo que motivó la creación de dicha cuenta.
- En el caso de los estudiantes, en el curso académico en que dejen de estar matriculados.

En ambos casos se establecerán periodos de cortesía ajustados a las necesidades de cada categoría de usuarios. Se avisará con tiempo suficiente por correo, informando de que se va a proceder al borrado de la información, para que el usuario pueda hacer copia de la información que considere de interés.

En el caso de los empleados o personal vinculado a la UC con cuenta institucional, deberán tener en cuenta los derechos legales que asisten a la Universidad sobre la información asociada a su actividad como personal de la UC, y traspasarla de manera adecuada a la institución durante este periodo de cortesía.

### Artículo 3.7: Dispositivos portátiles propiedad de la UC

En el caso de los dispositivos portátiles (ordenadores, tabletas, teléfonos móviles, etc.) deben tomarse las siguientes precauciones:

- Vigilarlos adecuadamente para evitar que sean sustraídos, así como el acceso a ellos por parte de personas no autorizadas. En el caso de que sean sustraídos, se ha de poner inmediatamente en conocimiento del Servicio de Informática para la adopción de las medidas que correspondan y deberá cursarse su baja en el inventario.
- Evitar almacenar información sensible, confidencial o protegida en los ordenadores u otros dispositivos portátiles y eliminar periódicamente datos innecesarios.
- Cuando se traten datos de nivel alto de seguridad o confidenciales (cuando la tipología de la información tratada así lo requiera), deberán tener cifrado el almacenamiento de datos, y disponer de software que garantice un arranque seguro, así como mecanismos de auditoría.
- Nunca almacenar contraseñas en archivos de texto ni almacenarlas en los navegadores.
- Tener actualizado y protegido convenientemente el equipo según las recomendaciones del Servicio de Informática.
- Conectarse semestralmente a la red corporativa, bien localmente o bien mediante VPN (Red privada virtual), para permitir la actualización de aplicaciones, sistema operativo, antivirus y demás medidas de seguridad.
- Activar el salvapantallas con contraseña tras un periodo de inactividad.
- Existirá un inventario actualizado de los equipos portátiles propiedad de la Universidad de Cantabria que será gestionado por el Servicio de Informática.

### Artículo 3.8: Uso de dispositivos personales

Los dispositivos propiedad de los usuarios (portátiles, móviles, tabletas, etc.) que se conecten a la red de la Universidad deberán mantener actualizados tanto los sistemas operativos como las aplicaciones instaladas. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.

La Universidad podrá disponer de mecanismos de monitorización que permitan comprobar el cumplimiento del punto anterior, y podrá adoptar las medidas que considere necesarias para evitar riesgos para la organización.

### Artículo 3.9: Uso de las redes de comunicaciones

El acceso a la red de comunicaciones de la Universidad de Cantabria estará restringido a los usuarios a los que hace referencia esta normativa.

Esta normativa se aplica al uso de todos los elementos que conforman la red corporativa de la Universidad de Cantabria, ya sea desde ubicaciones propias de la Universidad (Centros y Edificios de la misma), desde ubicaciones externas que, como consecuencia de convenios o relaciones contractuales, hagan uso dicha red, o desde cualquier otra ubicación que utilice, de una u otra forma, la red de la Universidad de Cantabria.

Se admitirán revisiones del tráfico de red, siempre que exista un requerimiento legal adecuado (basado en la sospecha fundada del incumplimiento de la presente normativa), por necesidades del órgano responsable de la información, o por razones de emergencia (cuando exista riesgo de repercusión grave para la red de datos de la Universidad de Cantabria, los dispositivos conectados a ella, o los servicios o información que contiene). Se entenderá como “sospecha fundada” aquella basada en indicios objetivos y verificables de un posible incidente de seguridad, a partir de alertas de sistemas de seguridad, registros de actividad que evidencien accesos indebidos o no autorizados o comunicaciones o denuncias recibidas por canales habilitados.

La Universidad tiene la capacidad de descifrar el tráfico de red en los dispositivos de comunicaciones, para poder detectar malware y tráfico no legítimo, sujeto a las limitaciones impuestas por la normativa de protección de datos personales.

Todos los usuarios de la red de la Universidad de Cantabria tienen la obligación de cooperar activamente con el Servicio de Informática, tanto en las tareas de mantenimiento del inventario de los recursos, como en su gestión y uso. Igualmente tienen la obligación de cooperar en las tareas de diagnóstico, que faciliten la resolución de las incidencias técnicas que se puedan producir.

Igualmente serán de aplicación las políticas de uso de red y resto de normativas de la Comunidad de RedIRIS, por pertenecer la Universidad a dicha Comunidad.

Únicamente se permitirá la conexión a la red cableada de comunicaciones de la Universidad de Cantabria, ya sea de forma física o remota, a aquellos equipos autorizados por el Servicio de Informática, y que utilicen la infraestructura de cableado autorizada por dicho Servicio.

### Artículo 3.10:  Uso de sistemas de difusión de la información

Se deberá hacer un uso ético y legal de los recursos de difusión de la información, como son el correo electrónico, la publicación web o cualquier otro medio de difusión electrónica de la información que la Universidad ponga a disposición de los usuarios.

Cuando sea necesario, cada servicio podrá disponer de su propia normativa para regular adecuadamente sus características y particularidades.

Específicamente:

- No se permite utilizar el correo electrónico, la publicación web o cualquier otro medio de difusión electrónica de información para la difusión de contenidos amenazantes, contrarios a los derechos humanos, al honor y la dignidad de las personas o que vulneren los principios expresados en los Estatutos de la Universidad o la legislación vigente.
- No se permite utilizar estos medios para realizar manifestaciones o adquirir compromisos en nombre de la Universidad sin la debida competencia o autorización.
- Las listas de distribución de correo solo deberán usarse para mensajes relacionados con su finalidad específica, y su uso se ajustará a la normativa establecida por el Servicio de Informática.
- Está prohibido el abuso del correo electrónico. Son ejemplos de abuso:
    - Difusión de contenido inadecuado o ilegal (relacionado con hechos delictivos o ilícitos).
    - Uso de canales no autorizados, como el uso de estafetas no autorizadas para reenviar correo propio.
    - Difusión masiva no autorizada, incluyendo el envío de publicidad o correo no solicitado (mensajes encadenados, spam…)
    - Ataques dirigidos a impedir o dificultar el servicio, ya sea contra usuarios concretos o al propio sistema de correo.

Los administradores de sistemas tomarán las medidas necesarias para evitar que tales sistemas puedan ser usados para estas prácticas. La detección de estos comportamientos llevará aparejada la suspensión de los servicios asociados a la cuenta del usuario, sin perjuicio de las posibles sanciones disciplinarias que procedan de acuerdo con la normativa aplicable.

## Artículo 4: Credenciales de acceso

Todo usuario dispondrá de unas credenciales (usuario y contraseña) que serán personales e intransferibles, con las que realizará el inicio de sesión y el acceso a los sistemas de información a los que esté autorizado.

Es responsabilidad del usuario custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad establecidas por la Universidad de Cantabria, para garantizar que aquellas no puedan ser utilizadas por terceros. En caso de detectar que sus credenciales puedan estar siendo usadas por otra persona, deberá comunicarlo inmediatamente a la Universidad siguiendo los procedimientos que se establecidos en el procedimiento de gestión de incidentes de seguridad.

Ninguna persona podrá utilizar las credenciales de acceso de otro usuario, aunque cuente con su autorización expresa.

Además del usuario y contraseña, podrán implantarse otros mecanismos de control de acceso o de refuerzo de la seguridad, como la autenticación multifactor, el certificado digital o equivalentes, en función de los riesgos y la criticidad de la información a proteger.

Cada sistema cuenta con un mecanismo de control de acceso. Para entrar, siempre será necesario autenticarse ante el sistema con las claves de acceso proporcionadas.

Los usuarios tienen las siguientes obligaciones respecto a la gestión y utilización de sus claves de acceso:

- Custodiarlas con diligencia, asegurando su confidencialidad; por lo tanto, no deberán anotarse en soportes accesibles por otros usuarios.
- Cerrar sesión o bloquear el equipo cuando lo dejen desatendido.
- Las claves de acceso se crearán y utilizarán de acuerdo con las instrucciones establecidas por el Servicio de Informática:
    - Deben ser suficientemente complejas y difícilmente deducibles por terceros, evitando emplear como contraseña el propio identificador.
    - Se evitará utilizar como contraseña palabras sencillas o relacionadas con el usuario tales como el nombre propio, el DNI, la matrícula del coche, la fecha de nacimiento, etc.
    - Deben renovarse obligatoriamente al menos cada doce meses.
    - Deben ser distintas a las anteriores.
    - No se debe utilizar la misma contraseña para servicios de la Universidad de Cantabria y servicios ajenos a la misma.
    - Si otras personas han participado en la creación o distribución de la contraseña, el usuario estará obligado a cambiarla la primera vez que la utilice.

El usuario deberá cambiar la contraseña de forma inmediata en el caso de que se haya visto comprometida o se sospeche que lo puede haber sido.

## Artículo 5: Acceso físico a las instalaciones

Áreas públicas:

- El acceso a las áreas públicas no está restringido. En estas zonas no deberán ubicarse equipos ni información sensible, confidencial o protegida que puedan ser accedidos por terceros sin autorización.
- En áreas donde se realicen tareas de atención a usuarios, no deberán dejarse documentos sobre las mesas ni información visible en pantallas que pueda ser vista por personas no autorizadas. Debe mantenerse especial precaución en zonas en las que se trate información sensible o confidencial y, en los casos en los que se manejen datos de carácter personal, deberán aplicarse las medidas de seguridad correspondientes, que se detallarán en los procedimientos de seguridad.

Áreas restringidas:

- Para el acceso a las áreas restringidas (centros de datos, salas de servidores, etc.) será necesaria autorización previa.

- En caso de que visitantes o personal no autorizado deban acceder a las instalaciones o a la información, deberán estar siempre acompañado por personal autorizado de la organización, que velará en todo momento por la seguridad de los recursos.

## Artículo 6: Datos de carácter personal y deber de secreto

La información de la Universidad de Cantabria que comprenda datos de carácter personal está protegida por la legislación vigente de protección de datos personales y garantía de los derechos digitales.

Todos los sistemas de información de la Universidad de Cantabria se ajustarán a los niveles de seguridad exigidos en función de la naturaleza y finalidad de los datos tratados.

Todo usuario que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos de forma indefinida, incluso una vez finalizada su la relación laboral o profesional con la Universidad de Cantabria.

## Artículo 7: Incidencias de seguridad

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de las instalaciones o los sistemas de Información de la Universidad de Cantabria, o cualquier posible infracción de la Normativa, deberá comunicarlo inmediatamente al Responsable de Seguridad, siguiendo el procedimiento de gestión de incidentes de seguridad.

Cuando el incidente de seguridad afecte a datos de carácter personal deberá notificarse de forma inmediata a la Delegada de Protección de Datos y/o a la Comisión de Protección de Datos Personales, aplicando el protocolo de información establecido por la legislación vigente.

El Responsable de Seguridad velará por el correcto registro de incidentes de seguridad ocurridos y de las acciones tomadas para su resolución, informando al Comité de Seguridad de la Información, para que este adopte las acciones organizativas y legales que apliquen en cada caso.

Dichos registros se emplearán para la mejora continua de la seguridad del sistema.

## Artículo 8: Incumplimiento del reglamento

En caso de incumplimiento de las reglas y obligaciones explicitadas en este Reglamento, el Servicio de Informática notificará, siempre que fuera posible, tal circunstancia al usuario. Además, el incumplimiento de este Reglamento podrá llevar aparejada la inmediata suspensión del servicio prestado y/o el bloqueo temporal de sistemas, cuentas o conexiones de red, en la medida en que resulte necesario para garantizar el buen funcionamiento de los servicios y proteger los intereses de la Universidad de Cantabria y del resto de usuarios.

Los usuarios tienen la obligación de colaborar con el Servicio de Informática para corregir, cesar y, en su caso, rectificar, el ejercicio de acciones que incumplan este Reglamento.

Si los afectados consideran que las medidas correctoras adoptadas por el Servicio de Informática son excesivas, pondrán esta circunstancia en conocimiento del Vicerrectorado competente en la materia, que resolverá sobre la proporcionalidad de las mismas en cada caso concreto. Lo anterior no será aplicable para el caso de sanciones disciplinarias, que se regirán por su propio procedimiento.

En caso de que se produzcan hechos graves, antisociales o reiterados en el tiempo, el Servicio de Informática los pondrá en conocimiento de los órganos de gobierno de la Universidad que resulten competentes para adoptar las medidas pertinentes en orden a su inmediata cesación. Todo ello sin perjuicio de ejercitar las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, frente a todas aquellas personas que pudieran estar implicadas en dichos incumplimientos.

Además, la Universidad de Cantabria se reserva el derecho a ejercitar las acciones legales pertinentes para la protección y defensa de sus legítimos intereses en aquellos supuestos de hecho no directamente contemplados en el presente Reglamento, a los que sin embargo pudieran ser aplicable otro marco jurídico.

## Artículo 9: Exención de responsabilidad

La Universidad de Cantabria queda eximida de cualquier responsabilidad derivada del mal funcionamiento de los servicios que tenga su origen en una circunstancia accidental, de fuerza mayor o de cualquier otra causa no imputable a la misma.

## Artículo 10: Desarrollo

A propuesta del Vicerrector que tenga atribuida las correspondientes competencias en cada momento, el Comité de Seguridad de la Información aprobará y publicará las normativas necesarias para el desarrollo del presente Reglamento.

## Artículo 11: Disposición adicional. Consideraciones lingüísticas

Todas las denominaciones relativas a los órganos de la universidad, a sus titulares e integrantes y a miembros de la comunidad universitaria, así como cualesquiera otras que en la presente normativa se efectúen en género masculino, se entenderán hechas indistintamente en género femenino, según el sexo del titular que los desempeñe o de aquel a quien dichas denominaciones afecten. Cuando proceda, será válida la cita de los preceptos correspondientes en género femenino.