Certificado nº 83/24

SILVIA TAMAYO HAYA, SECRETARIA GENERAL DE LA UNIVERSIDAD DE CANTABRIA,

C E R T I F I C O: Que el Consejo de Gobierno de la Universidad de Cantabria, en su sesión ordinaria del día 18 de julio de 2024, acordó:

Aprobar la modificación de la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UC,** quedando su texto redactado en los siguientes términos:

"**Exposición de motivos**

Las Tecnologías de la Información y de las Comunicaciones constituyen herramientas indispensables para alcanzar los objetivos institucionales de la Universidad de Cantabria, apoyando las actividades de docencia, estudio, investigación y gestión. En consecuencia, los sistemas y recursos TIC deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, confidencialidad, integridad o conservación de la información, así como de los sistemas y servicios electrónicos que la sustentan.

El objetivo de la Política de Seguridad de la Información de la Universidad de Cantabria es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas se requiere una estrategia que se adapte a los cambios en las condiciones del entorno. Por ello, la institución debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos de TIC.

La Universidad de Cantabria lleva a cabo una política activa de protección de los datos personales que utiliza para su gestión y el cumplimiento de sus fines, de acuerdo con lo previsto en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales y en el 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 datos (RGPD).

La Universidad de Cantabria solo recabará los datos personales que sean adecuados, pertinentes y no excesivos en relación con las finalidades para las que se obtengan y se traten, e informará a los afectados de la existencia de los tratamientos de datos, base jurídica que legitima el tratamiento, sus finalidades, destinatarios de los datos, derechos que puede ejercitar y demás información establecida en los artículos 5,13 y 14 del RGPD y resto de normativa concordante.

CAPÍTULO I.
DISPOSICIONES GENERALES
Artículo 1. Marco normativo

La Política de Seguridad de la Información se enmarca en un amplio contexto normativo de regulación de la prestación de los servicios electrónicos a los ciudadanos que viene determinado, esencialmente, por las siguientes disposiciones:

a) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
b) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
c) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
d) 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 datos y por el que se deroga la Directiva 95/46/CE.
e) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
f) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
g) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
h) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
i) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.
j) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
k) Ley de Cantabria 1/2018, de 21 de marzo, de Transparencia de la Actividad Pública.

Artículo 2. Objeto de la Política de Seguridad de la Información

1. La Universidad de Cantabria es una institución de Derecho público con personalidad jurídica y patrimonio propios, socialmente responsable, que presta el servicio público de la educación superior, actuando con plena autonomía de acuerdo con la Constitución y las leyes. En la realización de su actividad institucional conforme a los principios de búsqueda de la calidad contrastada, eficiencia y servicio a la sociedad, la Universidad de Cantabria se sirve de los recursos de las TIC, cuya organización general corresponde al Servicio de Informática, para el apoyo a la docencia, el estudio, la investigación y la gestión.

2. La presente Política de Seguridad de la Información tiene por objeto regular las medidas y los procedimientos de seguridad de los sistemas de información y comunicación que permiten a la Universidad de Cantabria prestar el servicio público de la educación superior cumpliendo las funciones establecidas en el artículo 2 de sus Estatutos.

Artículo 3. Ámbito de aplicación

1. Esta política se aplicará a todos los servicios, sistemas y demás recursos TIC de la Universidad de Cantabria que den soporte a sus procesos y que afecten a los diferentes activos de información sustentados en ellos.

Son recursos TIC de la Universidad de Cantabria todos los sistemas centrales y departamentales, estaciones de trabajo, ordenadores, impresoras y otros periféricos y dispositivos de salida, redes internas y externas, sistemas multiusuario, servicios de comunicaciones y sistemas de almacenamiento que sean de su propiedad o estén conectados directa o indirectamente a la Red UNICAN, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

Asimismo, son recursos TIC otros servicios cloud que se presten a la misma para el cumplimiento de sus funciones.

En este sentido, no se consideran recursos TIC de la universidad aquellos ordenadores personales u otros dispositivos financiados a título individual y no inventariados a nombre de la Universidad de Cantabria. No obstante, el acceso a los recursos TIC de la universidad desde dispositivos personales estará sujeto a las condiciones que establezca la normativa elaborada en desarrollo de esta Política de Seguridad conforme a lo establecido en el artículo 41.

2. Asimismo, se aplicará también la Política de Seguridad de la Información a todas aquellas personas, Centros, Departamentos, Institutos, estructuras, entidades, unidades o servicios, sean internos o externos, que hagan uso de los recursos TIC de la Universidad de Cantabria. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su normativa de seguridad derivada, siendo responsabilidad del Comité de Seguridad de la Información y Protección de Datos Personales disponer los medios necesarios para que la información llegue al personal afectado.

CAPÍTULO II
PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
Sección Primera: Principios básicos
Artículo 4. Principios básicos

La presente Política de Seguridad de la Información se fundamenta en los siguientes principios básicos, que deberán tenerse presentes en cualquier actividad relacionada con el uso de los activos de información:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Artículo 5. Seguridad como proceso integral

1. La seguridad de la información se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información, excluyendo cualquier actuación puntual o tratamiento coyuntural.

En consecuencia, la seguridad debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

2. En aras de la integridad del sistema, todo elemento físico o lógico requerirá autorización formal, previa a su instalación en el mismo, por el Responsable del Sistema.

Artículo 6. Gestión de la seguridad basada en los riesgos

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta unos niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de las medidas de seguridad apropiadas en todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, estableciendo un equilibrio y proporcionalidad entre la naturaleza de los datos, los tratamientos realizados, los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

3. Al evaluar los riesgos, la Universidad de Cantabria tendrá en cuenta los riesgos que se derivan para los derechos y libertades de las personas con respecto al tratamiento de datos personales.

Artículo 7. Prevención, detección, respuesta y conservación

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, entre las cuales se contemplarán la disuasión y la reducción de la exposición, deberán eliminar o, al menos, reducir la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

6. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 8. Existencia de líneas de defensa

1. Se establecerá una estrategia de protección constituida por múltiples capas de seguridad, compuestas por medidas de naturaleza organizativa, operativa, física y lógica, dispuestas de tal forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Asimismo, los sistemas de información deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Artículo 9. Vigilancia continua y reevaluación periódica

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección.

Artículo 10. Diferenciación de responsabilidades

Para la aplicación de la Política de Seguridad de la Información se establece una estructura organizativa basada en la delimitación de funciones y la asignación de responsabilidades. En este sentido, se diferencian las figuras del Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

En esta política de seguridad se detallarán las atribuciones de cada responsable y los mecanismos de colaboración, así como los de coordinación y resolución de conflictos.

Sección Segunda: Requisitos mínimos de seguridad

Artículo 11. Requisitos mínimos de seguridad

Las directrices fundamentales de seguridad se concretan en un conjunto de requisitos mínimos de seguridad, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información. Se establecen los siguientes:

a) Organización e implantación del proceso de seguridad. Se desarrolla en el capítulo III de la presente política.

b) Análisis y gestión de los riesgos. Se desarrolla en el procedimiento de análisis y gestión de riesgos.

c) Gestión de personal. Se desarrolla en el procedimiento de gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos. Se desarrolla en el procedimiento de control de accesos.

f) Protección de las instalaciones. Se desarrolla en el procedimiento de seguridad física.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad. Se desarrolla en el apartado de relación con terceros y en el procedimiento de gestión de proveedores.

h) Mínimo privilegio. Se desarrolla en el procedimiento de seguridad lógica.

i) Integridad y actualización del sistema. Se dispone de un procedimiento en el que se ha establecido cómo se debe realizar el mantenimiento del equipamiento y la gestión de parches y vulnerabilidades.

j) Protección de la información almacenada y en tránsito. Se desarrolla en los procedimientos de seguridad lógica, seguridad física y protección de la información.

k) Prevención ante otros sistemas de información interconectados. Se desarrolla en el procedimiento de seguridad lógica.
l) Registro de la actividad y detección de código dañino. Se desarrolla en el procedimiento de seguridad lógica.
m) Incidentes de seguridad. Se desarrolla en el procedimiento de gestión de incidentes.
n) Continuidad de actividad. Se desarrolla en el procedimiento de gestión de la continuidad.
o) Mejora continua del proceso de seguridad. Se desarrolla en el procedimiento de gestión de la seguridad de la información (SGSI).

Artículo 12. Organización e implantación del proceso de seguridad

1. La seguridad de los sistemas de información debe comprometer a todos los miembros de la organización.

2. La política de seguridad deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

Artículo 13. Análisis y gestión de los riesgos

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de los servicios realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

4. Cuando los sistemas de información contengan datos de carácter personal, el análisis de riesgos deberá identificar los factores de riesgos para los derechos y libertades de las personas interesadas cuyos datos están presentes en el tratamiento con el fin de hacer una primera evaluación del riesgo intrínseco, adoptar las medidas y garantías que lo mitiguen y estimar el riesgo residual.

Artículo 14. Gestión de personal

El personal propio o ajeno, relacionado con los sistemas de información deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad para que, de este modo, se reduzca el riesgo derivado de un uso indebido de dichos activos, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.

Todos y cada uno de los usuarios de los sistemas de información de la Universidad de Cantabria son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de la Universidad de Cantabria tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y 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.

Los miembros de la Universidad de Cantabria recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Universidad de Cantabria, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Artículo 15. Profesionalidad

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Artículo 16. Autorización y control de los accesos

1. Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

2. El acceso a los sistemas de información deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 17. Protección de las instalaciones

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales, en función del análisis de riesgos. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

La totalidad de las oficinas cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen. Asimismo, las instalaciones de la Universidad de Cantabria están dotadas de los dispositivos de extinción de incendios marcados por la legislación vigente en esa materia y de salidas de emergencia debidamente señalizadas.

Artículo 18. Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Artículo 19. Mínimo privilegio

La Universidad de Cantabria promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen un grado de seguridad y de protección de datos por defecto, otorgando los mínimos privilegios necesarios para su correcto desempeño conforme a lo dispuesto en el artículo 20 del Real Decreto 311/2022, de 3 de mayo.

Artículo 20. Integridad y actualización del sistema

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa por el Responsable del Sistema.

2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 21. Protección de información almacenada y en tránsito

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación del Real Decreto 311/2022, cuando ello sea exigible.

Se realizarán copias de seguridad que aseguren la posibilidad de recuperación en caso de incidente.

Artículo 22. Prevención ante otros sistemas de información interconectados

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

Artículo 23. Registro de actividad y detección del código dañino

1. Para el cumplimiento del Real Decreto 311/2022 y con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa

sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas y de conformidad con lo dispuesto en el Reglamento General de Protección de datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, la Universidad de Cantabria podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Artículo 24. Incidentes de seguridad

1. Se dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 del Real Decreto 311/2022 y las instrucciones y guías técnicas que lo desarrollan.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

3. Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo siguiendo los procedimientos establecidos, para que se tomen las medidas oportunas y se registre la incidencia.

4. Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a las incidencias en materia de seguridad. Existirán procedimientos que abarquen todos los tipos posibles de incidentes.

Artículo 25. Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Artículo 26. Mejora continua del proceso de seguridad

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

Artículo 27. Auditoría de seguridad

1. Los sistemas de información comprendidos en el ámbito de aplicación de esta política serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

2. Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas.

3. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda.

4. Además, con carácter anual, se realizará una auditoría interna de verificación de cumplimiento del ENS cumpliendo el principio de independencia.

CAPÍTULO III
ORGANIZACIÓN DE LA SEGURIDAD

Artículo 28. Estructura organizativa

La estructura organizativa para la gestión de la seguridad de la información está compuesta por los siguientes órganos:

a) El Responsable de la Información
b) El Responsable del Servicio
c) El Responsable de Seguridad
d) El Responsable del Sistema
e) El Delegado de Protección de Datos
f) El Comité de Seguridad de la Información y de Protección de Datos Personales.
g) La Comisión de Protección de Datos Personales
h) Oficina de Seguridad TIC
i) Centro de Operaciones de Ciberseguridad
j) Responsables internos de tratamientos de datos de carácter personal.

Artículo 29. Responsable de la Información

La figura del Responsable de la Información recaerá en el Gerente de la Universidad de Cantabria, que tendrá asignadas las siguientes funciones y responsabilidades:

a) Velar por la protección y el buen uso de la información.
b) Establecer y elevar para su aprobación al Comité de Seguridad de la Información y Protección de Datos Personales los requisitos de seguridad aplicables a la Información (niveles de seguridad de la información), dentro del marco establecido en el Anexo I del Real Decreto 311/2022, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
c) Dictaminar respecto a los derechos de acceso a la información.
d) Aceptar los niveles de riesgo residual que afectan a la información.
e) Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de los que es responsable, especialmente la incorporación de información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información y Protección de Datos Personales, en su próxima reunión.
f) Velar por la inclusión de cláusulas sobre seguridad en los contratos y convenios con terceras partes y su cumplimiento.
g) Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

Artículo 30. Responsable del Servicio

La figura del Responsable del Servicio recaerá en el Vicegerente de Organización de la Universidad de Cantabria, que tendrá las siguientes funciones y responsabilidades:

a) Establecer y elevar para su aprobación al Comité de Seguridad de la Información y de Protección de Datos Personales, los requisitos de seguridad aplicables a los servicios (niveles de seguridad de los servicios) dentro del marco establecido en el Anexo I del Real Decreto 311/2022, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
b) Dictaminar respecto a los derechos de acceso a los servicios.
c) Aceptar los niveles de riesgo residual que afectan a los servicios.
d) Poner en comunicación del Responsable de Seguridad cualquier variación respecto a los servicios de los que es responsable, especialmente la incorporación de nuevos servicios a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información y Protección de datos Personales, en su próxima reunión.

Artículo 31. Responsable de Seguridad

La figura del Responsable de Seguridad tendrá las siguientes funciones y responsabilidades:

a) Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
b) Promover la formación y concienciación en materia de seguridad de la información.

c) Designar responsabilidades de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
d) Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información y Protección de Datos Personales.
e) Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
f) Gestionar las revisiones externas o internas del sistema.
g) Gestionar los procesos de certificación.
h) Elevar al Comité de Seguridad de la Información y Protección de Datos Personales, la aprobación de cambios y otros requisitos del sistema.
i) Aprobar los procedimientos de seguridad que forman parte del mapa normativo (y no son competencia del Comité) y poner en conocimiento al Comité las modificaciones que se hayan realizado a lo largo del periodo en curso.
j) Actuar como punto de contacto (PoC).

Artículo 32. Responsable del Sistema

La figura de Responsable del Sistema recaerá en el Director del Servicio de Informática de la Universidad de Cantabria, que tendrá asignadas las siguientes funciones y responsabilidades:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
b) Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Detener el acceso a información o prestación del servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
d) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
e) Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información y Protección de Datos Personales.
f) Participar en la elaboración e implantación de los planes de mejora de la seguridad y en los planes de continuidad.
g) Llevar a cabo, en su caso, las funciones del administrador de seguridad del sistema:
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrolladas en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Artículo 33. Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

a) Informar y asesorar a la Universidad de Cantabria, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
b) Supervisar el cumplimiento de lo dispuesto en la normativa de seguridad y de las políticas internas de la Universidad de Cantabria, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
c) Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y las auditorías correspondientes.
d) Cooperar con la Agencia Española de Protección de datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
e) El Delegado de Protección de Datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones del tratamiento. Para ello realizará las siguientes funciones y actividades:
- Recabar la información para determinar las actividades de tratamiento
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o al encargado de tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en el principio de protección de datos desde el diseño y por defecto.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.

f) Asesorar al Responsable de la Información sobre áreas en las que acometer auditorías, actividades de formación a realizar y operaciones de tratamiento sobre las que dedicar más tiempo y recursos.

Artículo 34. El Comité de Seguridad de la Información y de Protección de Datos Personales

El Comité de Seguridad de la Información y de Protección de Datos Personales es el órgano colegiado que dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de seguridad de la información y de protección de datos personales.

Artículo 35. Composición del Comité de Seguridad de la Información y de Protección de Datos Personales

1. El Comité de Seguridad de la Información y Protección de Datos Personales estará integrado por el Rector o persona en quien delegue, el Secretario General, el Responsable de la Información, el Responsable del Servicio, el Responsable de Seguridad, el Responsable del Sistema, el Vicerrector competente en materias de seguridad de la información, la jefa de Asesoría Jurídica y el Delegado de Protección de Datos Personales.

2. El Rector o persona en quien delegue presidirá el Comité de Seguridad de la Información.

Corresponde al Presidente convocar las reuniones del Comité y fijar el orden del día.

3. El Presidente designará una persona que actuará como Secretario del Comité de Seguridad de la Información.

Corresponde al Secretario elaborar el acta de las reuniones.

4. El Comité de Seguridad de la Información y de Protección de Datos Personales podrá invocar la presencia en sus reuniones tanto de otros representantes de la universidad como de especialistas externos, de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Artículo 36. Funciones del Comité de Seguridad de la Información y de Protección de Datos Personales

1. Las funciones del Comité de Seguridad de la Información y de Protección de Datos Personales son:

a) Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.

b) Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
c) Estar permanentemente informado de la relación de esquemas de certificación de seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
d) Estar permanentemente informado de la normativa relativa a la protección de datos personales, incluyendo guías, manuales e informes jurídicos de la Agencia Española de protección de datos, así como de otras autoridades de control.
e) Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, y cuyo cumplimiento será supervisado por el Presidente.
f) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
g) Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de seguridad de la información al Consejo de Dirección.
h) Resolver conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando al Consejo de Dirección aquellos casos en los que no tenga suficiente autoridad para decidir.
i) Asesorar en materia de seguridad de la información y protección de datos personales, siempre y cuando le sea requerido.
j) Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
k) Proponer el Reglamento de uso de recursos TIC para todo el personal para su aprobación por Consejo de Gobierno.
l) Aprobar el Marco normativo en el que se encuadran las Normativas y Procedimientos de seguridad para la implantación del ENS.

2. El Comité de Seguridad de la Información y Protección de Datos Personales, se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera una mayor frecuencia en las reuniones.

3. En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.

Artículo 37. La Comisión de Protección de Datos Personales

1. La Comisión de Protección de Datos Personales es el órgano asesor del Comité de Seguridad de la Información y de Protección de Datos Personales y la responsable de supervisar el cumplimiento de la normativa de protección de datos personales.

2. La Comisión de Protección de Datos Personales estará integrada por los siguientes miembros:
a) El Vicegerente de Organización.
b) La Jefa de la Asesoría Jurídica.
c) El Responsable del Sistema
d) El Delegado de Protección de Datos Personales.
e) El Responsable de Seguridad

3. La Comisión de Protección de Datos Personales tendrá las siguientes funciones:
a) Proponer al Comité de Seguridad de la Información las normas necesarias de acuerdo con la estructura normativa establecida en el artículo 41 de esta política.
b) Resolución de las consultas planteadas por las unidades gestoras en materia de protección de datos personales.
c) Resolución de las consultas planteadas por las personas en materia de protección de datos personales.
d) Gestionar e impulsar la tramitación de las solicitudes de ejercicio de derechos de protección de datos personales.
e) Recibir y tramitar las peticiones de autorización, modificación o supresión de actividades de tratamiento de datos personales, proponiendo al Responsable de la Información, la resolución que proceda.

f) Incorporar los tratamientos autorizados al Registro de Actividades de Tratamiento y llevar el Inventario de Actividades de tratamiento, manteniéndolo permanentemente actualizado.
g) Promover la realización de auditorías periódicas del RGPD que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de protección de datos personales.

Artículo 38. La Oficina de Seguridad TIC

1. La Oficina de Seguridad TIC desarrollará la adecuación al ENS, la normativa y gestión de riesgos, el análisis y mejora continua y otras funciones conexas o concordantes.

2. El Comité de Seguridad de la Información y Protección de Datos Personales propondrá al Consejo de Gobierno la estructura y los recursos y medios necesarios para garantizar el cumplimiento de estas funciones.

3. El Director de la Oficina de Seguridad TIC será el Responsable de Seguridad, que actuará como enlace con el Comité de Seguridad de la Información y de Protección de Datos Personales.

4. El Director de la Oficina de Seguridad TIC organizará grupos de trabajo y convocará reuniones, recabando los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad de la Información y de Protección de Datos Personales, para su aprobación, en su caso.

5. Las funciones de la Oficina de Seguridad TIC serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad de la Información y de Protección de Datos Personales:

a) Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.
b) Redacción y presentación de propuestas al Comité de Seguridad de la Información y de Protección de Datos Personales. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
c) Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al Comité de Seguridad de la Información y de Protección de Datos Personales para su revisión y posterior aprobación del órgano superior.
- Elaborar la normativa de Seguridad de la Información.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
- Promover la realización de las auditorías periódicas ENS que permitan verificar el cumplimiento de las obligaciones de la universidad en materia de seguridad de la información.

Artículo 39. El Centro de Operaciones de Ciberseguridad

1. El Centro de Operaciones de Ciberseguridad (COCS) prestará servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, a la vez que mejorará la capacidad de respuesta del sistema ante cualquier ataque.

2. Estos servicios serán asumidos por el Servicio de Informática.

3. El Comité de Seguridad de la Información y Protección de Datos Personales propondrá al Consejo de Gobierno la estructura y los recursos y medios necesarios para garantizar el cumplimiento de estas funciones.

4. La dirección y responsabilidad del COCS recae en el director de la oficina de seguridad TIC, que se coordinará con el Responsable del Sistema en la definición y aplicación de medidas de seguridad y en la operativa de supervisión del COCS.

5. El Centro de Operaciones de Ciberseguridad tendrá las siguientes funciones:

a) Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.

b) Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.

c) Operaciones de seguridad sobre los dispositivos de defensa.

d) Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

e) Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.

f) Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.

g) Análisis forense digital y de seguridad.

h) Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

Artículo 40. Responsables internos del tratamiento de datos personales

1. Son responsables internos del tratamiento de datos las personas que dirigen las diferentes unidades organizativas, responsables de actividades de tratamiento de datos, o aquellas designadas por el gerente que, en calidad de tales, deben velar por el cumplimiento de las condiciones asignadas a cada tratamiento.

2. En caso de los trabajos bajo la responsabilidad de grupos de investigación, la responsabilidad interna corresponde al investigador principal (IP).

3. Las funciones y obligaciones de los responsables internos del tratamiento se indican en el documento de seguridad de las actividades de tratamiento de la Universidad de Cantabria.

Artículo 41. Estructura normativa

1. La Universidad de Cantabria establece un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

a) Primer nivel: la Política de Seguridad de la Información, el Reglamento de Uso de Recursos TIC, la Política de Protección de datos personales y la normativa propia de la Universidad de Cantabria de protección de datos de carácter personal que deben ser aprobadas por el Consejo de Gobierno a propuesta del Comité de Seguridad de la Información y Protección de Datos Personales.

b) Segundo nivel: la normativa de seguridad de la información será aprobada por el Comité de Seguridad de la Información y Protección de Datos Personales en desarrollo de la Política de Seguridad de la Información, como, por ejemplo, la Normativa de cuentas institucionales y normativa del servicio de correo. En ella se establecerá una política de uso aceptable de los sistemas de información, que incluirá los siguientes contenidos:

- Lo que se considera uso indebido de los equipos que intervienen en el proceso de administración electrónica y otros procesos en el alcance.
- El uso correcto de equipos, servicios e instalaciones.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Esta normativa, una vez aprobada por el Comité de Seguridad de la Información y de Protección de Datos Personales, deberá adoptarse por Resolución rectoral.

c) Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad de la información.

Estos procedimientos serán aprobados por el Comité de Seguridad de la Información y Protección de Datos Personales, a propuesta del Responsable de Seguridad.

d) Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Estos documentos podrán ser aprobados por el Responsable de Seguridad, en colaboración con el Responsable del Sistema.

2. La normativa de seguridad y de protección de datos personales y, muy especialmente, la Política de Seguridad de la información, el Reglamento de Uso de recursos TIC, la Política de Protección de datos personales y la Normativa propia de la Universidad de Cantabria de protección de datos de carácter personal será conocida 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. Estará disponible para su consulta en la página web de la Universidad de Cantabria y en la Intranet.

CAPÍTULO IV
DERECHOS Y DEBERES

Artículo 42. Promoción de la concienciación y la formación sobre seguridad

1. Todos los miembros de la Universidad de Cantabria tienen el derecho de conocer y la obligación de cumplir esta Política de Seguridad de la Información y la normativa de seguridad desarrollada a partir de ella. A tales efectos, la Universidad de Cantabria se compromete a promover la concienciación y formación en esta materia, disponiendo los medios necesarios para que la información llegue a las personas afectadas.

2. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC tienen derecho a recibir formación en materia de seguridad de la información y a ser informados de sus deberes y obligaciones en esta materia. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo, en la medida en que sea necesaria para realizar su trabajo.

Artículo 43. Responsabilidades en caso de incumplimiento de la normativa de seguridad de la información

1. El Comité de Seguridad de la Información y de Protección de Datos Personales podrá determinar si por parte del personal que tiene acceso a la información o la trata en el ejercicio de su tarea profesional existe algún tipo de incumplimiento de las obligaciones previstas en la Política de Seguridad de la Información o en su normativa de desarrollo.

2. En caso de incumplimiento, se tomarán medidas preventivas y correctivas encaminadas a salvaguardar y proteger los sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

3. Constatado el incumplimiento, el Comité de Seguridad de la Información y de Protección de Datos Personales instará la depuración de las responsabilidades disciplinarias a las que pudiera haber lugar.

4. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario del personal al servicio de las Administraciones Públicas o de la propia Universidad de Cantabria u otra legislación aplicable.

Artículo 44. Relación con terceros

1. Cuando la Universidad de Cantabria preste servicios a otros organismos o maneje información de éstos se les hará partícipes de esta Política de Seguridad de la Información y de la normativa de seguridad. Para ello se establecerán canales de comunicación y coordinación entre los respectivos Comités de Seguridad de la Información o unidad que desempeñe funciones similares y se establecerán procedimientos de actuación para reaccionar ante posibles incidentes de seguridad.

2. Asimismo, cuando la Universidad de Cantabria utilice servicios de terceros o les ceda información, se les hará igualmente partícipes de esta Política de Seguridad de la Información y de la normativa de seguridad. Dicha parte quedará sujeta a las obligaciones y medidas de seguridad establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

3. Cuando ello implique el encargo de tratamiento de datos personales a terceros, la Universidad y el tercero deberán formalizar el correspondiente contrato o acto jurídico de encargo del tratamiento, con el contenido mínimo establecido en el artículo 28 del RGPD. La Universidad, como

responsable del tratamiento, deberá velar por que el encargado ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos establecidos en la normativa de protección de datos y se garantice la protección de los derechos de las personas interesadas.

4. Cuando algún aspecto no pueda ser satisfecho por el tercero, se requerirá un informe del Responsable de Seguridad en el que se precisen los riesgos en los que se incurre y la forma de tratarlos, que deberá ser aprobado por el Responsable de la Información.

5. Se establecerán procedimientos específicos de detección, comunicación y resolución de incidencias.

6. Los terceros deberán garantizar:
a) La adecuada concienciación de su personal en materia de seguridad de la información.
b) El cumplimiento de políticas de seguridad de la información basadas en estándares auditables y su sometimiento a controles y revisiones de terceros que certifiquen el cumplimiento de estas políticas.
c)La ejecución del destino de los datos personales, una vez cumplida la prestación, conforme a lo que se establezca en el correspondiente contrato de encargado de tratamiento de datos personales.

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.

Disposición transitoria única

1. Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el Comité de Seguridad de la Información y Protección de Datos personales se reunirá, al menos, una vez al trimestre.

2. Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados por la universidad, el Comité de Seguridad de la Información y Protección de Datos Personales, se reunirá según el régimen ordinario previsto en el artículo 36.

Disposición final. Entrada en vigor

Esta Política de Seguridad de la Información entrará en vigor al día siguiente de su aprobación por el Consejo de Gobierno de la Universidad de Cantabria".

Y para que conste, expido la presente certificación que lleva el Visto Bueno del Sr. Rector Magnífico de la Universidad, en Santander, a dieciocho de julio de dos mil veinticuatro.

Vº Bº
EL RECTOR,

Ángel Pazos Carro

* Este certificado se emite con anterioridad a la aprobación del acta.