POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UC

Exposición de motivos

La *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* establece el marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos, reconociendo el derecho de aquellos a comunicarse con las administraciones a través de tales medios. Dicho marco de relación se establece a través de la Administración Electrónica, compuesta tanto por los sistemas de Tecnologías de la Información y Comunicación (TIC) destinados a este fin como por el tratamiento y almacenamiento automatizado de la información que reside en los mismos.

Para garantizar la seguridad y fiabilidad de los trámites que se realicen a través de la Administración Electrónica, el artículo 42.2 de dicha ley crea el Esquema Nacional de Seguridad (ENS), cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de los medios electrónicos que permita la adecuada protección de la información. Atendiendo a dicho mandato legislativo, el *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica* dispone en su artículo 11 que todas las administraciones deberán disponer de su Política de Seguridad de la Información, que será aprobada por el titular del órgano superior correspondiente.

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.

Dada la estrecha relación de la seguridad de la información con la protección de los datos de carácter personal, la Política de Seguridad de la Información debe ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del *Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. En la Universidad de Cantabria, el "Documento de seguridad de los ficheros de los datos personales de la Universidad de Cantabria" fue elaborado por el Comité de Seguridad y aprobado por la Gerencia el 17 de febrero de 2014.

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 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

b) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

c) Ley 59/2003, de 19 de diciembre, de firma electrónica.

d) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

e) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

f) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

g) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

h) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

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.

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 de puesto, 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.

En este sentido, no se consideran recursos TIC de la universidad los 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 29.

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.

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) La seguridad como proceso integral.
b) Gestión de riesgos.
c) Prevención, detección, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica y mejora continua.
f) La seguridad como función diferenciada.

Artículo 5. La seguridad como proceso integral

La seguridad de la información es el resultado de un proceso integral que depende de todos y cada uno de los elementos técnicos, humanos, materiales y organizativos que intervienen en su tratamiento. 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.

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

Artículo 6. Gestión de 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.

Artículo 7. Prevención, detección, reacción y recuperación

1. 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.

2. Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

3. Las medidas de reacción tendrán como objeto que los incidentes de seguridad se atajen a tiempo. A tal fin, la Universidad de Cantabria:

a) Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
b) Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con ella.
c) Establecerá protocolos para el intercambio de información relacionada con el incidente, incluyendo comunicaciones con los Equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional.

4. Las medidas de recuperación deberán permitir la restauración de la información y la continuidad de los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales de trabajo.

Artículo 8. Líneas de defensa

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 si una de ellas falla la seguridad en su conjunto no se vea comprometida.

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

Artículo 9. Reevaluación periódica y mejora continua

1. La gestión de la seguridad de la información requiere una reevaluación, actualización y monitorización continua para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

2. Con carácter ordinario, los sistemas de información serán objeto de una auditoría de seguridad cada dos años. Esta auditoría verificará el cumplimiento de los

requerimientos del Esquema Nacional de Seguridad y de la presente Política de Seguridad de la Información, ajustándose a las exigencias establecidas en el artículo 34 del *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*.

3. Extraordinariamente, se realizará dicha auditoría cuando concurra alguna de las siguientes circunstancias:

a) Cuando cambie sustancialmente la información manejada.
b) Cuando cambien sustancialmente los servicios prestados.
c) Cuando ocurra un incidente grave de seguridad.
d) Cuando se reporten vulnerabilidades graves.

4. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años establecidos para la realización de la siguiente auditoría regular ordinaria.

Artículo 10. La seguridad como función diferenciada

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, el Responsable del Servicio y el Responsable de la Seguridad.

Sección Segunda: Principios particulares

Artículo 11. Principios particulares.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares, 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) Coordinación y colaboración.
b) Protección de datos de carácter personal.
c) Gestión de activos de la información.
d) Seguridad ligada a las personas.
e) Seguridad física.
f) Seguridad en la gestión de comunicaciones y operaciones.
g) Control de acceso.
h) Adquisición, desarrollo y mantenimiento de los sistemas de información.
i) Gestión de los incidentes de seguridad.
j) Gestión de la continuidad.

Artículo 12. Coordinación y colaboración

Los responsables de la seguridad de la información actuarán de manera coordinada en la aplicación y control de las medidas de seguridad de la información.

Artículo 13. Protección de datos de carácter personal

Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

Artículo 14. Gestión de activos de información

Los activos de información de la Universidad de Cantabria se encontrarán inventariados y categorizados de acuerdo a lo establecido en el Esquema Nacional de Seguridad, estando asociados a un responsable. En función de dicha categorización se determinará su nivel de protección y las medidas a aplicar.

Artículo 15. Seguridad ligada a las personas

Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y, de este modo, se reduzca el riesgo derivado de un uso indebido de dichos activos.

Artículo 16. Seguridad física

Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

Artículo 17. Seguridad en la gestión de comunicaciones y operaciones

Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

Artículo 18. Control de acceso

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.

El acceso a los sistemas de información deberá estar limitado a las personas debidamente autorizadas y en relación exclusivamente a las funciones permitidas.

Artículo 19. Adquisición, desarrollo y mantenimiento de los sistemas de información

Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

Artículo 20. Gestión de los incidentes de seguridad

1. Ante incidentes de seguridad de la información, el personal deberá ajustar su actuación a las instrucciones establecidas en el Protocolo de Incidentes, cuya aprobación corresponderá al Responsable de la Seguridad.

2. Se establecerá un Registro de Incidentes en el que quedará constancia de todos los incidentes de seguridad de la información que se produzcan y de las acciones de tratamiento que se sigan para su salvaguarda. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 21. Gestión de la continuidad

Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

CAPÍTULO III

ORGANIZACIÓN DE LA SEGURIDAD

Artículo 22. Estructura organizativa

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

a) El Comité de Seguridad de la Información.
b) El Responsable de la Información.
c) El Responsable del Servicio.
d) El Responsable de Seguridad.

Artículo 23. El Comité de Seguridad de la Información.

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

Artículo 24. Composición del Comité de Seguridad de la Información

1. El Comité de Seguridad de la Información estará integrado por el Gerente, el Secretario General, el Vicegerente de Organización, el Director del Servicio de Informática y la jefa de Asesoría Jurídica.

2. El Gerente, como Responsable de la Información, presidirá el Comité de Seguridad de la Información. En caso de inasistencia podrá delegar dicha función en otro miembro del Comité.

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

3. La Gerencia designará una persona que actuará como Secretario del Comité de Seguridad de la Información.

Corresponde al Secretario elaborar el acta de las reuniones.

Artículo 25. Funciones del Comité de Seguridad de la Información

1. Las funciones del Comité de Seguridad de la Información son:

a) Informar regularmente del estado de la seguridad de la información al Rector.

b) Promover la mejora continua del sistema de gestión de la seguridad de la información.

c) Divulgar la Política de Seguridad de la Información, promoviendo la formación y la concienciación en materia de seguridad de la información.

d) Proponer al Consejo de Gobierno la modificación de la Política de Seguridad de la Información.

e) Aprobar la normativa y procedimientos de seguridad elaborada en desarrollo de la Política de Seguridad de la Información.

f) Elaborar e impulsar la estrategia y nuevas líneas de trabajo en lo que respecta a la seguridad de la información.

g) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

h) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida, y evitar duplicidades.

i) Elaborar y aprobar los requisitos de formación y calificación de los administradores, operadores y usuarios desde el punto de vista de la seguridad de la información.

j) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Universidad de Cantabria en materia de seguridad.

k) Priorizar las actuaciones en materia de seguridad.

l) Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

m) Interpretar la normativa de seguridad y resolver los conflictos que puedan surgir entre los distintos responsables en la aplicación de la Política de Seguridad de la Información.

n) Comunicar a los órganos competentes las infracciones de la Política de Seguridad de la Información y de su normativa de desarrollo e instar, en su caso, la adopción de las medidas disciplinarias correspondientes.

2. El Comité de Seguridad de la Información se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

3. El Comité podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Artículo 26. Responsable de la Información.

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

a) Velar por la protección y el buen uso de la información.

b) Establecer los requisitos de la información en materia de seguridad.

c) Determinar los niveles de seguridad de la información.

d) Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y su cumplimiento.

e) Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

Artículo 27. Responsable del Servicio.

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

a) Coordinar las actuaciones de los distintos órganos implicados en la política de seguridad de la información.

b) Coordinar y supervisar la aplicación de la política de seguridad de la información en los servicios administrativos y económicos y en los servicios universitarios.

c) Velar por e impulsar el cumplimiento de la normativa en materia de seguridad.

d) Promover la mejora continua de la gestión de la seguridad de la información.

Artículo 28. Responsable de la Seguridad.

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

a) Promover la seguridad de la información manejada y de los servicios prestados por los sistemas TIC.

b) Establecer los requisitos de los servicios TIC en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.

c) Determinar los niveles de seguridad de los servicios.

d) Determinar las medidas necesarias para satisfacer los requisitos de seguridad de la información y de los servicios y verificar que las establecidas son adecuadas para la protección de la información manejada y los servicios prestados.

e) Determinar la categoría de cada sistema según el procedimiento descrito en el Anexo I del Esquema Nacional de Seguridad.

f) Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa, así como de la seguridad física y lógica de los recursos TIC.

g) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

h) Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Universidad de Cantabria en materia de seguridad de la información.

i) Supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y realizar informes sobre las incidencias graves para su presentación al Comité de Seguridad de la Información.

j) Proponer nueva normativa de seguridad o la modificación de la existente al Comité de Seguridad.

k) Aprobar los procedimientos de seguridad.

l) Acordar, junto con el responsable del servicio, la suspensión del manejo de cierta información o la prestación de cierto servicio si conoce deficiencias graves de seguridad.

m) Promover la formación y concienciación en materia de seguridad de la información.

Artículo 29. Estructura normativa

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, que debe ser aprobada por el Consejo de Gobierno a propuesta del Comité de Seguridad.

b) Segundo nivel: la normativa de seguridad de la información aprobada por el Comité de Seguridad de la Información en desarrollo de la Política de Seguridad de la Información. 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 el 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, 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 e la información. En ellos se indicará de forma clara y precisa:

   - Cómo llevar a cabo las tareas habituales
   - Quién debe hacer cada tarea.
   - Cómo identificar y reportar comportamientos inadecuados.

   Estos procedimientos han de ser aprobados por el Comité de Seguridad de la Información.

d) Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Ha de ser aprobada por el Responsable de la Seguridad.

CAPÍTULO IV

DERECHOS Y DEBERES

Artículo 30. 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 31. Responsabilidades en caso de incumplimiento de la normativa de seguridad de la información.

1. El Comité de Seguridad de la Información 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 instará la depuración de las responsabilidades disciplinarias a las que pudiera haber lugar.

Artículo 32. 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 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. 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.

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

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 cancelación de los datos pertenecientes a la Universidad de Cantabria a la finalización del contrato, debiendo quedar bloqueados en los términos previstos en el artículo 16.3 de la Ley Orgánica de Protección de Datos Personales y 5.1.b) de su Reglamento, y ser posteriormente eliminados según las previsiones de dichas normas.

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 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.