POLÍTICA DE SEGURIDAD DE LA UNIVERSIDAD DE VALLADOLID DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD.

(Aprobado por el Consejo de Gobierno en sesión de 15 de julio de 2016, BOCyL nº 144 de 27 de julio, modificado por el Consejo de Gobierno en sesión de 29 marzo de 2019, BOCyL nº 68 de 8 de abril)

Acuerdo del Consejo de Gobierno de la Universidad de Valladolid por el que se aprueba la "Política de Seguridad de la Universidad de Valladolid" de conformidad con el Esquema Nacional de Seguridad.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 dispone la creación, a través de reglamento, del Esquema Nacional de Seguridad.

En cumplimiento y desarrollo de la misma, se aprobó 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. Esta norma tiene por objeto el establecimiento de los principios básicos y requisitos mínimos de una política de seguridad en la utilización de medios electrónicos, que permita la adecuada protección de la información.

Es de aplicación a las administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos que se gestionen en el ejercicio de sus competencias.

Con la misma se pretende proporcionar las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de una serie de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos de manera que permita a los ciudadanos el ejercer sus derechos y a la Universidad de Valladolid cumplir sus deberes a través de estos medios electrónicos.

El citado Real Decreto establece en su artículo 11 que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente, en el caso de la Universidad de Valladolid, por el Consejo de Gobierno.

Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos.

h) Seguridad por defecto.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de actividad.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

En cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad, el Consejo de Gobierno, previo informe de los Servicios Jurídicos de la Universidad de Valladolid ha acordado la aprobación del documento que figura a continuación en todos y cada uno de los puntos contemplados en el mismo.

El presente acuerdo entrará en vigor el día siguiente de su publicación en el tablón de anuncios de la Sede Electrónica de la Universidad de Valladolid, con independencia de su publicación en el Boletín Oficial de Castilla y León.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

II. 14. 3

1 Aprobación y Entrada en Vigor

Texto aprobado el día 15 de julio de 2016 por el Consejo de Gobierno de la Universidad de Valladolid.

Esta Política de Seguridad entrará en vigor el día siguiente de su publicación en el tablón de anuncios de la Sede Electrónica de la Universidad de Valladolid, con independencia de su publicación en el Boletín Oficial de Castilla y León.

2 Introducción

La Política de Seguridad de la Información se elabora en cumplimiento de las siguientes exigencias legales:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.
- 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 (LOPD).

La Universidad de Valladolid utiliza los sistemas Tecnologías de Información y Comunicaciones (en adelante TIC) para alcanzar sus fines y objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información 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 con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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 para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos (en adelante ENS y LOPD), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La Universidad de Valladolid debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada del 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 pliegos de licitación para proyectos de TIC.

La Universidad de Valladolid debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

2.1 Prevención

La Universidad de Valladolid debe evitar, o al menos prevenir con los medios más adecuados, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas de seguridad determinadas por el ENS y la LOPD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal de la Universidad, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los Servicios Universitarios deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

2.3 Respuesta

La Universidad de Valladolid debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Servicios Universitarios o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (Computer Emergency Response Team, en adelante CERT).

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los Servicios Universitarios de la Universidad de Valladolid desarrollarán planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

3 Objetivo

Corresponde a la Universidad de Valladolid lo previsto en el artículo 1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y en el artículo 6 de los Estatutos de la Universidad de Valladolid.

4 Alcance

La Política de Seguridad de la Universidad de Valladolid se aplica a toda la comunidad universitaria y a sus activos de información: y a todos sus sistemas TIC sin excepción

5 Declaración de la Política de Seguridad de la Información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de la Universidad de Valladolid.

Es política de esta universidad asegurar que:

- En la Universidad de Valladolid se reconoce expresamente la importancia de la información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la Institución, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- La Universidad de Valladolid implementa, mantiene y realiza un seguimiento del ENS y de la LOPD, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger, a su vulnerabilidad y a su clasificación.
- El Responsable de la Seguridad de la información involucrada en la prestación de los servicios electrónicos incluidos en el alcance del ENS pondrá los medios adecuados para ello, sin perjuicio de que cada profesor, personal de administración y servicios, alumno o usuario asuma su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en estas normas y en los procedimientos complementarios.
- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de la Universidad de Valladolid.
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en el documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a los empleados públicos de la Universidad de Valladolid y a colaboradores, previniendo la comisión de errores, omisiones, ilícitos administrativos, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible.
- El personal de la Universidad de Valladolid deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones.
- Se establecerá además la separación de funciones y la revisión independiente de los

registros, de modo que cuando sea necesario, se pueda conocer quién ha hecho qué, cuándo y desde dónde.

- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.

6 Marco normativo

El marco normativo en el que se desarrollan las actividades de la Universidad de Valladolid comprende:

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades
- Estatutos de la Universidad de Valladolid.
- Ley 3/2003, de 28 de marzo, de Universidades de Castilla y León.

Las otras leyes, reglamentos y normativa, nacional o internacional, a la que la Universidad de Valladolid está sujeto pueden consultarse en la página web de la universidad: www.uva.es.

7 Organización de la Seguridad

7.1 Comité: Funciones y Responsabilidades

El Comité de Seguridad de la Información coordina la seguridad de la información en la Universidad de Valladolid.

El **Comité de Seguridad de la Información** reportará a los órganos de gobierno de la Universidad de Valladolid y estará formado por:

- Responsable del Servicio.
- Responsable de la Información.
- Responsable de Seguridad.
- Responsable del Sistema.
- Administrador de Seguridad de Sistemas.
- Delegado/a de Protección de Datos de la Universidad de Valladolid, si este cargo fuera desempeñado por persona empleada pública de la propia institución, o, alternativamente, el Director/a Técnico/a en materia de Privacidad.[1]

Estará presidido por el Responsable del Servicio. El **Secretario del Comité de Seguridad de la Información** será el Responsable de Seguridad y tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El **Comité de Seguridad** tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información en la Universidad de Valladolid.

[1] Se modifica el segundo párrafo por Acuerdo del Consejo de Gobierno de 29 de marzo de 2019

- Elaborar la estrategia de evolución de la Universidad de Valladolid en lo que respecta a seguridad de la información.
- 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 en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Consejo de Gobierno.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Universidad de Valladolid y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Universidad de Valladolid En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información al Consejo de Gobierno.

7.2 Roles: Funciones y Responsabilidades

Los responsables de la seguridad de la Universidad son los siguientes:

- **Comité de Seguridad de la Información**
- **Responsable del Servicio:** Gerente.
- **Responsable de la Información:** Secretario General.
- **Responsable de Seguridad:** Personal Técnico del STIC.
- **Responsable del Sistema:** Personal Técnico del STIC.
- **Administrador de la Seguridad de Sistemas:** Personal Técnico del STIC.
- **Grupos de trabajo:** En determinadas áreas de la gestión universitaria se podrán

nombrar Grupos de trabajo, integrados por los correspondientes Jefes de Servicio responsables de la información y prestación de servicios así como por el personal Técnico del STIC responsable de la administración de sistemas de esas áreas.

Las funciones y responsabilidades se detallan a continuación:

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

Responsable de Seguridad

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- 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.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Responsable del Sistema

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y

aprobar las modificaciones importantes de dicha configuración.

- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Administrador de la Seguridad del Sistema

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los Responsables de la Seguridad y del Sistema 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.

Grupos de trabajo

- Con carácter general, apoyar en la respectiva área al Comité de Seguridad de la Información en el desarrollo de sus funciones, así como proponer las medidas que considere adecuadas en materia de seguridad de la información.
- Llevar a cabo todas aquellas tareas que le sean encomendadas por el Comité de Seguridad de la Información.

7.2.1 Tareas:

RFICH – Responsable del Fichero

RINFO – Responsable de la Información

RSERV – Responsable del Servicio

RSEG – Responsable de la Seguridad

RSIS – Responsable del Sistema

ASS – Administrador de la Seguridad del Sistema

TAREA	RESPONSABLE
Notificar los ficheros ante el Registro General de Protección de Datos.	RFICH + RINFO
Garantizar el cumplimiento de los deberes de secreto y seguridad.	RFICH + RINFO
Garantizar derechos ARCO	RFICH + RINFO
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o el Comité de Seguridad de la Información
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	Elabora: RSEG Aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	Elabora: comité de seguridad Aprueba: Consejo de Gobierno

Normativa de seguridad	Elabora y aprueba: comité de seguridad de la información
Procedimientos operativos de seguridad	Elabora y aprueba: RSEG Aplica: ASS
Estado de la seguridad del sistema	Monitoriza: ASS Reporta: RSEG
Planes de mejora de la seguridad	Elaboran: RSIS + RSEG Aprueba: comité de seguridad de la información
Planes de concienciación y formación	Elabora: RSEG Aprueba: comité de seguridad
Planes de continuidad	Elabora: RSIS Valida: RSEG Coordina y aprueba: comité de seguridad Ejercicios: RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	Elabora: RSIS Aprueba: RSEG

7.3 Procedimientos de designación y de resolución de conflictos

7.3.1 Procedimientos de designación:

El Sr. Rector nombrará:

- Al Responsable del Servicio.
- Al Responsable de la Información.
- Al Responsable de Seguridad, que reportará al comité de seguridad de la información.
- Al Responsable del Sistema, oídos el responsable del servicio y el de la información, que reportará al Responsable de la Seguridad.
- Al Administrador de Seguridad del Sistema, a propuesta del Responsable del Sistema, al que reportará.

El Comité de Seguridad de la Información designará a los miembros de los distintos Grupos de trabajo.

7.3.2 Procedimientos de resolución de conflictos:

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior

jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad de la Información.

7.4 Política de Seguridad de la Información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

8 Datos de Carácter Personal

La Ley Orgánica de Protección de Datos (LOPD) garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

El documento de seguridad que regula la normativa de protección de datos se encontrará en la Sede Electrónica de la Universidad de Valladolid. Dicho documento recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de la Universidad de Valladolid se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

Para garantizar dicha protección, se adoptan las medidas de seguridad que se corresponden con las exigencias previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universidad de Valladolid.

9 Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos.

10 Desarrollo de la política de seguridad de la información

La política de seguridad se desarrollará en la documentación de seguridad, que regulará normas específicas de seguridad de la información de un área o aspecto determinado, aprobadas por el Comité de Seguridad de la Información, entre ellas, la política de uso aceptable, seguridad de la gestión de recursos humanos, seguridad física y del entorno, gestión de comunicaciones y operaciones, así como control de accesos.

El Responsable de Seguridad podrá aprobar procesos, procedimientos TIC o instrucciones técnicas TIC de un determinado ámbito de actuación

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla en la intranet de la Universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

11 Obligaciones del personal

Todos los miembros de la Comunidad Universitaria de la Universidad de Valladolid tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

A Todos los miembros de la Comunidad Universitaria de la Universidad de Valladolid se les informará adecuadamente sobre concienciación en materia de seguridad. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Universidad, 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. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12 Terceras partes

Cuando la Universidad de Valladolid preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de Valladolid utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.