Política de Seguridad de la Informacion de la USAL.

Política de Seguridad de la Información de la Universidad de Salamanca

Índice

1 Aprobación y Entrada en Vigor

Texto aprobado por el Consejo de Gobierno de la Universidad de Salamanca en sesión realizada el día 18 de diciembre de 2013.
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Introducción

La Universidad de Salamanca considera que los sistemas de Tecnologías de Información y Comunicaciones (TIC en lo sucesivo) constituyen un elemento estratégico para alcanzar sus 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 o confidencialidad 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 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 para garantizar la prestación continua de los servicios. Esto implica que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS en lo sucesivo), 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 Salamanca 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 pliegos de licitación para proyectos de TIC.
La Universidad de Salamanca debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

Prevención

La Universidad de Salamanca, para evitar o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, implementará

las medidas mínimas de seguridad determinadas por el ENS, 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, van a estar claramente definidos y documentados.
Para garantizar el cumplimiento de la Política, las Unidades, Áreas o Servicios llevarán a cabo las siguientes actuaciones:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

Detección

Puesto que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se debe 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 regularmente o cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

La Universidad de Salamanca:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, las Unidades, Áreas o Servicios de la Universidad de Salamanca desarrollarán planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

Alcance

Esta Política se aplica a todos los sistemas TIC de la Universidad de Salamanca y a todos sus miembros, sin excepciones.

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 Salamanca.
Es la política de esta entidad asegurar que:

- La información y los servicios estén protegidos contra pérdidas de disponibilidad, confidencialidad e integridad.
- La información esté protegida contra accesos no autorizados.
- Se cumplan los requisitos legales aplicables.
- Se cumplan los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad sean comunicadas y tratadas apropiadamente.
- Se establezcan procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información sea el encargado de mantener esta Política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio sea el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado sea responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.
- La Universidad de Salamanca implemente, mantenga y realice un seguimiento del cumplimiento del Esquema Nacional de Seguridad.

Marco normativo

Según la legislación vigente, las leyes aplicables a la Universidad de Salamanca en materia de Seguridad de la Información son:

- 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. BOE de 29 de enero de 2010.
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. BOE de 27 de noviembre de 1992.
- Ley Orgánica 15/99, de 13 de Diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. BOE de 19 de enero de 2008.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual. BOE de 22 de abril de 1996.
- Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público. BOE de 13 de abril de 2007.
- Ley orgánica 6/2001, del 21 de diciembre, de universidades. BOE de 24/12/2001.
- Ley 3/2003, de 28 de marzo, de Universidades de Castilla y León. BOCLYL de 4 de Abril de 2003 y BOE de 23 de Abril de 2003.
- Estatutos de la Universidad de Salamanca, aprobados por Acuerdo 19/2003, de 30 de enero, de la Junta de Castilla y León y modificados por Acuerdo 38/2011, de 5 de mayo, de la Junta de Castilla y León

Asimismo, la Universidad de Salamanca cumple con las leyes, reglamentos y normativa, nacionales o internacionales, aplicables a su actividad y relacionadas con la Organización de la Seguridad

Comité: Funciones y Responsabilidades

El Comité de Seguridad de la Información coordina la seguridad de la información en la Universidad de Salamanca
El Comité de Seguridad de la Información estará formado por:

- Responsable de la Información: la persona titular de la Secretaría General de la Universidad de Salamanca o persona en quien delegue.
- Responsable de los Servicios, la persona titular de la Gerencia de la Universidad de Salamanca o persona en quien delegue.
- Responsable de Seguridad, la persona titular del Vicerrectorado encargado de las infraestructuras informáticas o persona en quien delegue.
- Responsable del Sistema, la persona responsable de sistemas de los Servicios Informáticos

El Secretario del Comité de Seguridad será el Responsable del Sistema y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información concreta para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Ser el responsable de la ejecución directa o delegada de las decisiones del Comité. El Comité de Seguridad reportará al Rector.

El Comité de Seguridad tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Rectorado.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Universidad de Salamanca 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.
- Promover, para su aprobación, 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 Salamanca y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. 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 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 Salamanca. En particular velar 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 TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

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.

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.

Responsable de Seguridad

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información.

Responsable del Sistema

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Administrador de la Seguridad del Sistema

- Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Gestionar 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.
- Aplicar 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.

Procedimientos de designación

Los Responsables de Información, Servicio, Seguridad y Servicios Informáticos se designan según el procedimiento establecido para su cargo.
La persona responsable de Sistema será nombrada por el Comité a propuesta de la Dirección de los Servicios Informáticos.
Los Administradores de Seguridad serán nombrados por el Comité a propuesta del Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. El nombramiento se revisará cada dos años o cuando el puesto quede vacante.

Revisión de la Política de Seguridad de la Información

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

Datos de Carácter Personal

La Universidad de Salamanca trata datos de carácter personal. El Documento de Seguridad, que se puede encontrar en la Secretaría General, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de la Universidad de Salamanca 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.

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 revisará cada dos años y se podrá repetir::

- 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.

Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la Universidad de Salamanca en materia de protección de datos de carácter personal.
Esta Política se desarrollará por medio de la Normativa de Seguridad que afronta aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla en la web de Secretaría General, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Obligaciones del personal

Todo el personal de la Universidad de Salamanca tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.
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.

Terceras partes

Cuando la Universidad de Salamanca 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 informe 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 Salamanca utilice servicios de terceros o ceda información a terceros, se les hará partícipes 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.