# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE LEÓN

Acuerdo Consejo de Gobierno 14/12/2018

# Índice

# 1 Introducción

La Universidad de León depende de los sistemas de Tecnología de la Información y de las Comunicaciones (TIC) 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.

La Universidad de León 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.

Esto implica que la Universidad de León y todo su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), desarrollado en el Real Decreto 3/2010 de 8 de enero, 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.

El Anexo II del ENS determina que la Política de Seguridad se plasmará en un documento en el que, de forma clara, se precise, al menos los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades de los cargos, así como el procedimiento para su designación y renovación, la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

Cumplir con estos requisitos es el objetivo de la presente Política de Seguridad de la Universidad de León.

# 2 Alcance

Esta política se aplica a todos los sistemas TIC de la Universidad de León y a todos los miembros de la misma, sin excepciones.

El R.D. 3/2010 se aplica a todos los recursos informáticos, los datos, las comunicaciones y los servicios electrónicos, y permite a los ciudadanos y a la propia Universidad de León, el ejercicio de derechos y el cumplimiento de deberes a través de medios informáticos.

Los recursos informáticos de la Universidad de León tienen como finalidad el apoyo a la docencia, a la investigación y a las tareas administrativas necesarias para su funcionamiento. Son recursos TIC de la Universidad de León todos los sistemas centrales y departamentales, estaciones de trabajo, ordenadores de puesto, impresoras y otros periféricos y dispositivos de salida, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y almacenamiento que sean de su propiedad, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

En este ámbito no se considera un "recurso TIC de la Universidad" aquellos ordenadores personales financiados a título individual, no inventariados a nombre de la Universidad de León, aunque pudieran ocasionalmente ser usados para labores propias de investigación. Por tanto, quedan fuera de este ámbito dichos elementos así como las acciones sobre ellos o riesgos de seguridad de tales elementos. En estos casos, la Universidad se reserva el derecho de proporcionar acceso a la red desde este tipo de recursos ajenos a la misma si no se proporcionan unos mínimos requisitos de seguridad o existen indicios o evidencias de un incidente potencial de seguridad que pueda comprometer o bien la seguridad de la información de los recursos TI de la Universidad o bien su buen nombre o imagen corporativa.

# 3 Misión

La Universidad de León es una Institución de Derecho Público al servicio de la sociedad, con personalidad jurídica y patrimonio propio, que goza de la autonomía reconocida por la Constitución española, desempeña aquellas competencias expresamente atribuidas por la legislación y ejercita los derechos que el ordenamiento jurídico le otorga.

Son objetivos fundamentales de la Universidad de León los siguientes:

- Realizar una enseñanza de calidad y contribuir al avance del conocimiento por medio de la actividad investigadora.
- Crear, enseñar y difundir ciencia, cultura, arte y tecnología, y contribuir al progreso social, económico y cultural.
- Promover la máxima proyección social de sus actividades mediante el establecimiento de cauces de colaboración y asistencia a la sociedad de su entorno.
- Propiciar la creación y difusión de hábitos y formas culturales críticas, participativas y solidarias, así como una formación permanente, abierta y plural.
- Fomentar la movilidad de los miembros de la comunidad universitaria y la cooperación internacional.
- Integrar las tecnologías de la información y el conocimiento en la actividad universitaria, a fin de incrementar su eficiencia global.
- Formar a los estudiantes para su desarrollo intelectual y su inserción cualificada en el mundo laboral.

La Universidad de León, en ejercicio de su autonomía económica y financiera y de acuerdo con la legislación vigente, dispone del patrimonio y los recursos adecuados a la satisfacción de sus fines y tiene plena capacidad para gestionar sus bienes.

# 4 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 León. Para ello la universidad debe realizar las tareas adecuadas para lograr prevenir, detectar, dar respuesta y recuperarse de cualquier incidente de seguridad.

Es la política de esta entidad asegurar que:

- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- La información está protegida contra accesos no autorizados.
- Se cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio será el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos, en lo que resulta aplicable en función de su puesto
- La Universidad de León implementa, mantiene y realiza un seguimiento del cumplimiento del Esquema Nacional de Seguridad.

# 5 Marco normativo

El marco normativo en materia de seguridad de la información en el que la Universidad de León desarrolla su actividad, esencialmente, es el siguiente:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.

- 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.

- Real Decreto 951/2015, de 23 de octubre, de modificación 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

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.

- Ley 59/2003, de 19 de diciembre, de firma electrónica

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

- Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- Ley 3/2003, de 28 de marzo, de Universidades de Castilla y León.
- Estatuto de la Universidad de León.

# 6 Organización de la Seguridad

## 6.1 Comité: Funciones y Responsabilidades

El Comité de Seguridad de la Información coordina la seguridad de la información en la Universidad de León

El Comité de Seguridad de la Información estará formado por:

- Presidente: El Rector o persona en quien delegue.

- Vocales:

    - Gerencia.
    - Secretaría General.
    - Vicerrectorado con responsabilidades en TICs.
    - Asesoría Jurídica.

- Secretario: Dirección del Servicio de Informática y Comunicaciones.

El Secretario del Comité de Seguridad TIC 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 TIC 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 León 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 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 León 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 León. 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 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.

## 6.2 Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

### *Responsable de la Información*

La figura del Responsable de la Información recaerá en el Secretario/a General de la Universidad. Tendrá las siguientes funciones y responsabilidades:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Establecer los requisitos de la información que deban ser garantizados en el tratamiento de la misma.
- Valorar para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) establecidas en el ENS y fijar los niveles adecuados de seguridad.

### *Responsable del Servicio*

La figura de Responsable del Servicio recaerá en el/la Gerente de la Universidad. Son sus funciones y responsabilidades:

- 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.
- Hacer cumplir adecuadamente la Política, la Normativa y los procedimientos de seguridad en los servicios.

### *Responsable de Seguridad*

La figura de Responsable de Seguridad recaerá en el Vicerrector/a con responsabilidades en las Tecnologías de la Información y las Comunicaciones. Tendrá como funciones y responsabilidades las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad.
- Promover la formación y concienciación en materia de seguridad de la información.
- Determinar la categoría de los sistemas y las medidas de seguridad que deben aplicarse siguiendo el ENS.
- Validar los procedimientos operativos de seguridad, los planes de mejora de la seguridad y los planes de continuidad.
- Realizar o instar a realizar los análisis de riesgos con revisión y aprobación anual.
- Realizar o instar a la realización de auditorías de seguridad periódicas.
- Elaborar la Normativa de Seguridad.

### *Delegado de Protección de Datos*

La figura del Delegado de Protección de Datos será designada por el Rector Las funciones de Delegado de Protección de Datos se podrán asignar en entidades externas con experiencia en materia de protección de datos personales y seguridad de la información. De acuerdo a lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la autoridad de control.

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.

- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

### *Responsable del Sistema*

La figura de Responsable del Sistema recaerá en el Director/a del Servicio de Informática y Comunicación, siendo sus funciones y responsabilidades:

- 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.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

### *Administrador de la Seguridad del Sistema*

El administrador de la Seguridad del Sistema será nombrado por el Responsable de Sistemas a propuesta del Comité de Seguridad y tendrá como funciones y responsabilidades:

- 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.

# 7 Procedimiento de designación

El desempeño de cualquiera de las responsabilidades definidas en esta política de seguridad y en el ENS vendrá determinado por el acceso a los diferentes cargos o destinos, estatutarios o no, que han quedado vinculadas a ellas.

En el caso de que, por modificación de la RPT, desapareciese o cambiara de denominación alguno de los puestos vinculados a la aplicación del ENS, será competencia del Rector asignar el nuevo puesto al que quedará vinculada la figura.

# 8 Datos de Carácter Personal

La Universidad de León trata datos de carácter personal. En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

# 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 TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC 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 Política de Uso Aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.

- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda molestar u ofender.
- Utilizar cualquier sistema físico, lógico o el espacio radioeléctrico, que pueda llegar a deteriorar de forma notable el rendimiento habitual de los recursos TIC de la Universidad

# 11 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 León en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de una Normativa de Seguridad que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Normativa de Seguridad estará disponible en la intranet para su consulta.

# 12 Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de la Universidad de León 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 León tienen 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.

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

# 13 Terceras partes

Cuando la Universidad de León 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 TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de León 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.

# 14 Procedimientos de aprobación

La aprobación de los diferentes documentos del marco normativo se realizará por parte de los Órganos de Gobierno y Representación de la Universidad según se indica a continuación:

- Política de Seguridad será aprobada por el Consejo de Gobierno. Será responsabilidad del Comité de Seguridad de la Información la revisión del contenido de la Política y de su propuesta de actualización cuando sea necesario.
- La Normativa de Seguridad será aprobada por el Rector a propuesta del Comité de Seguridad de la Información.
- Los Procedimientos de Seguridad serán aprobados bien por el Comité de Seguridad de la Información o bien por el Responsable de Seguridad.

# 15 Aprobación y Entrada en Vigor

Esta normativa de "Política y Seguridad de la Información de la Universidad de León" deroga y deja sin efecto la "Política de Seguridad de la Universidad de León" aprobada por el Consejo de Gobierno el 28/01/2014, y será efectiva desde la fecha de aprobación en Consejo de Gobierno y hasta que sea reemplazada por una nueva Política.