Aprobada Consejo de Gobierno 27-11-2023

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE LEÓN

1. Tabla de contenido

2. Aprobación y entrada en vigor

Esta Política de Seguridad entrará en vigor el día siguiente de su publicación en la Normativa de Régimen Interno de la Universidad de León, con independencia de su publicación en el Boletín Oficial de Castilla y León.

Esta normativa de "Política de 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 14/12/2018, y será efectiva desde la fecha de aprobación en Consejo de Gobierno y hasta que sea reemplazada por una nueva Política.

3. Introducción

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

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que en su artículo 12 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.
- 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 (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

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.

Por tanto, para la Universidad de León, 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 para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

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 311/2022, de 3 de mayo, 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.

3.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de León, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Universidad de León:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

3.2 Detección

La Universidad de León, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

3.3 Respuesta

La Universidad de León, establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos 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 (CERT).

3.4 Recuperación

Para garantizar la disponibilidad de los servicios, la Universidad de León, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

4. Misión de la Universidad de León

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.

5. Principios Básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- Responsabilidad determinada: En los sistemas TIC se identificará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

- Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

6. Objetivos de la Seguridad de la Información

La Universidad de León, establece como objetivos de la seguridad de la información los siguientes:

Garantizar la calidad y protección de la información.

- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- 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, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- 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.
- 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 TIC. 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.
- 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.

- 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.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: 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 con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de datos personales, con especial atención a las categorías especiales de datos, para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y, en su caso, en materia de protección de datos personales.

7. 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 Real Decreto 311/2022, de 3 de mayo 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.

Esta Política se aplicará a los sistemas de información de la Universidad de León, relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su

Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue al personal afectado.

8. Marco Normativo

El marco normativo en que se desarrollan las actividades de la Universidad de León y, en particular, la prestación de sus servicios electrónicos está integrado por las siguientes normas:

- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- 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 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 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.
- 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 3/2003, de 28 de marzo, de Universidades de Castilla y León.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- 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.
- Estatuto de la Universidad de León.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Universidad de León, derivadas de las anteriores y publicadas en la sede electrónica comprendidas dentro del ámbito de aplicación de la presente Política.

9. Organización de la Seguridad

9.1 Criterios utilizados para la organización de la Seguridad de la Información

El mantenimiento y gestión de la seguridad de la información va íntimamente ligado al establecimiento de una organización de seguridad, que compromete a todos los miembros de la Universidad.

La Universidad de León, teniendo en cuenta lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para organizar la seguridad de la información, emprenderá las siguientes acciones:

1. Designará roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegada/o de Protección de Datos.
2. Constituirá un órgano estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información.

9.2 Comité de Seguridad de la Información: Funciones y Responsabilidad

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 Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

El Secretario del Comité de Seguridad de la Información 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 de la Información 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.
- Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
- Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
- Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.

9.3 Roles Funciones y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

Comité de Seguridad de la Información para la toma de decisiones con relación a la seguridad de la información de la Universidad de León.

Responsable de la Información: será la persona u órgano encargado de la protección de la información y que determinará los niveles de seguridad de la información de los activos incluidos en el ámbito del ENS en la ULE, conforme a la normativa vigente, previo informe del Responsable de Seguridad y del Responsable del Sistema.

Dicha responsabilidad recae sobre el Comité de Seguridad de la Información quien designará los Comités Técnicos necesarios para asegurar la correcta implantación de las medidas de seguridad definidas.

Responsable del Servicio: serán los encargados de establecer los niveles de seguridad de los servicios incluidos en el ámbito del ENS en la ULE, previo informe del Responsable de Seguridad y del Responsable del Sistema. Se corresponde con el **Vicerrectorado, Gerencia y Dirección del SIC con competencias en el área.**

Responsable de Seguridad: será la persona encargada de la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo con lo establecido en la Política de Seguridad de la ULE. Recae sobre el **Vicerrectorado con competencias en Tecnologías de la Información**, quien designará un **Administrador de Protección de la Información**, entre el personal de los Servicios Informáticos con funciones en el área de seguridad, con objeto de realizar y mantener la gestión de los riesgos en el ámbito del ENS.

Responsable del Sistema: será el encargado de desarrollar, operar y mantener los sistemas de información afectados por el ENS durante todo su ciclo de vida para que tenga un correcto funcionamiento y asegurar que las medidas de seguridad de los sistemas se integran dentro del marco general de la Política de Seguridad. **Recaerá sobre la persona que ejerza la Dirección de los servicios informáticos.** Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los administradores de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquel y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

Delegado de Protección de Datos

- Serán funciones del delegado de protección de datos:

  1. Informar y asesorar al responsable del tratamiento de datos de la Universidad de León y a los usuarios que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la normativa vigente en materia de protección de datos.

  2. Supervisar el cumplimiento de lo dispuesto en la normativa de seguridad y en las políticas internas de la Universidad de León en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las actividades de tratamiento y en las auditorías correspondientes.

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

  4. Evaluar el impacto en los derechos y libertades de los interesados ante la ocurrencia de incidentes de seguridad graves que, conforme al RGPD, obliguen a una notificación de violación de seguridad a la autoridad de protección de datos o las personas interesadas, así como coordinar con el soporte del responsable de seguridad el proceso de notificación.
  5. Cooperar con la Agencia Española de Protección de Datos cuando esta lo requiera, actuando como punto de contacto para cuestiones relativas a los tratamientos de datos.
  6. El delegado de protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento.

  Para ello debe ser capaz de:

  a) Recabar información sobre las actividades de tratamiento y acceder a los sistemas de información cuando lo requiera, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto.

  b) Supervisar la conformidad de las actividades de tratamiento.

  c) Informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento.

d) Recabar información para supervisar el registro de las actividades de tratamiento.

e) Supervisar el cumplimiento del principio de la protección de datos desde el diseño y por defecto en el diseño de los sistemas de información.

f) Emitir informe sobre la necesidad de llevar a cabo evaluaciones de impacto, metodologías, salvaguardas a aplicar, etc.

g) Asesorar al responsable del tratamiento sobre auditorías, actividades formativas y actividades de tratamiento que requieran especial atención.

h) Documentar y comunicar inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento las vulneraciones relevantes en materia de protección de datos.

i) Cuantas funciones le sean atribuidas por la legislación aplicable y su normativa de desarrollo.

9.4 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.

10. 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.

11. 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.

12. 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.

13. Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del RD 311/2022, de 3 de mayo, La Universidad de León, notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

14. 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.

15. 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.

16. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

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

17. 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.