POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE LA LAGUNA

NIN-0003

Información normativa

Fecha de aprobación:	16 de marzo de 2022
Fecha de publicación:	23 de marzo de 2022

*:first-child]:mt-0">

Índice de contenidos

Aprobación y entrada en vigor

Texto aprobado por el Consejo de Gobierno de la Universidad de La Laguna, en su sesión del día 16 de marzo de 2022. Esta Política de Seguridad de la Información, en adelante Política, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Introducción

La Universidad de La Laguna depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) 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 seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados. Para hacer frente a 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 los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados. De este modo, todas las unidades administrativas de la universidad tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos de TIC. Para la Universidad de La Laguna, 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 7 del ENS, con la aplicación de las medidas que se relacionan a continuación.

Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Universidad de La Laguna 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 y 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 La Laguna autoriza los sistemas antes de entrar en operación, evalúa regularmente la seguridad incluyendo el análisis de los cambios de configuración realizados de forma rutinaria y solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

Detección

La Universidad de La Laguna 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 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, conforme a lo indicado en el artículo 8 del ENS (Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que la información llegue regularmente a los responsables.

Respuesta

La Universidad de La Laguna 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 y establecerá protocolos para el intercambio de información relacionada con el incidente, incluyendo comunicaciones en ambos sentidos con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

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

Misión de la Universidad de La Laguna

La Universidad de La Laguna pone a disposición de la ciudadanía la realización de trámites online y nuevas vías de participación que garanticen el desarrollo y la eficacia de sus funciones y cometidos. Al potenciar el uso de las nuevas tecnologías en la Universidad de La Laguna se persigue fomentar la relación electrónica de todos los actores (docentes, estudiantes, investigadores, personal de administración y servicios y otros) con la universidad.

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: el alcance estratégico, que requiere el compromiso y apoyo de todos los niveles directivos de la universidad para coordinar la seguridad con el resto de iniciativas estratégicas; la responsabilidad determinada, mediante la designación del Responsable de la Información, del Responsable del Servicio, del Responsable del Sistema y del Responsable de la Seguridad; la seguridad integral, entendida como un proceso que abarca elementos técnicos, humanos, materiales y organizativos, presente desde el diseño de los sistemas TIC; la gestión de riesgos, como parte esencial del proceso de seguridad para mantener un entorno controlado y minimizar los riesgos hasta niveles aceptables, equilibrando naturaleza de los datos, impacto, probabilidad y coste de las medidas; la proporcionalidad, de modo que las medidas de protección, detección y recuperación sean proporcionales a los riesgos y a la criticidad de la información y los servicios; la mejora continua, revisando y actualizando periódicamente las medidas de seguridad, que serán atendidas y auditadas por personal cualificado; y la seguridad por defecto, de forma que los sistemas se diseñen y configuren garantizando un grado suficiente de seguridad desde el inicio.

Objetivos de la seguridad de la información

La Universidad de La Laguna establece como objetivos de la seguridad de la información garantizar la calidad y protección de la información y lograr la plena concienciación de los usuarios respecto a la seguridad de la información. Para ello, los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable. Se impulsará la seguridad ligada a las personas mediante mecanismos que aseguren que quienes accedan a los activos de información conozcan sus responsabilidades. Los activos de información se ubicarán en áreas seguras con controles de acceso físicos adecuados, y los sistemas y activos se protegerán frente a amenazas físicas o ambientales. Se establecerán procedimientos para la gestión segura de las comunicaciones y operaciones, protegiendo la información transmitida según su nivel de sensibilidad. El control de acceso limitará el acceso mediante mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, registrando la utilización del sistema para asegurar la trazabilidad y auditar su uso adecuado. En la adquisición, desarrollo y mantenimiento de los sistemas de información se contemplarán los aspectos de seguridad en todas las fases del ciclo de vida, garantizando la seguridad por defecto. Se implementarán mecanismos para la gestión de incidentes de seguridad, para garantizar la prestación continuada de los servicios críticos y para la protección de datos, adoptando las medidas técnicas y organizativas conforme a la legislación de seguridad y privacidad. Asimismo, se adoptarán las medidas necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

Alcance

Esta Política se aplicará a los sistemas de información de la Universidad de La Laguna 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.

Marco normativo

El marco normativo en que se desarrollan las actividades de la Universidad de La Laguna y, en particular, la prestación de sus servicios electrónicos está integrado por normas como el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad, sus instrucciones técnicas de seguridad, las resoluciones sobre auditoría y notificación de incidentes, la Ley Orgánica 3/2018 de protección de datos y el Reglamento (UE) 2016/679, además de la legislación sobre procedimiento administrativo, régimen jurídico del sector público, interoperabilidad, servicios de la sociedad de la información, telecomunicaciones, reutilización de la información del sector público, conservación de datos de comunicaciones, propiedad intelectual, estatuto del empleado público, documento nacional de identidad y firma electrónica, transparencia, contratos del sector público, seguridad pública en materia de administración digital y servicios electrónicos de confianza. También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Universidad de La Laguna derivadas de las anteriores y publicadas en la sede electrónica.

Organización de la seguridad de la información

Criterios de organización

La Universidad de La Laguna, teniendo en cuenta el Real Decreto 3/2010 (ENS) y la Guía CCN?STIC?801, organizará la seguridad de la información mediante la designación de roles de seguridad (Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos) y la constitución de un órgano consultivo y estratégico colegiado denominado Comité de Seguridad de la Información o Comité de Seguridad TIC (COMSEGTIC), presidido por una persona física que asumirá la responsabilidad formal de sus actos.

Roles y órganos de la seguridad de la información

Los Responsables de los Servicios y de la Información serán los jefes y responsables de los diferentes órganos y unidades administrativas con responsabilidad funcional en sistemas de información. El Responsable de Seguridad de la Información será un cargo o funcionario de nivel ejecutivo designado formalmente por el Rector o el Equipo de Dirección, que no podrá ser órgano de gobierno unipersonal ni tener responsabilidad sobre la prestación de los servicios TIC ni dependencia jerárquica del Responsable del Sistema. El Responsable del Sistema será el Jefe del Servicio de Tecnologías y Comunicaciones de la Universidad de La Laguna. El Comité de Seguridad TIC estará presidido por el Rector o persona en quien delegue y contará como vocales con el Secretario General, el Responsable del Sistema, el Responsable de Seguridad de la Información, representantes de Información y Servicios, asesores que se consideren oportunos y el Delegado de Protección de Datos, que participará con voz pero sin voto cuando se aborden cuestiones de protección de datos.

Responsabilidades de los responsables de la Información y de los Servicios

Son funciones de los Responsables de la Información y de los Servicios establecer y elevar al Comité de Seguridad los requisitos de seguridad aplicables a la información y a los servicios dentro del marco del ENS, dictaminar respecto a los derechos de acceso, aceptar los niveles de riesgo residual que afectan a la información y a los servicios, y comunicar al Responsable de Seguridad cualquier variación respecto a la información y los servicios de los que son responsables, en especial la incorporación de nuevos servicios o información.

Responsabilidades del Responsable de Seguridad

El Responsable de Seguridad debe mantener y verificar el nivel adecuado de seguridad de la información y de los servicios electrónicos prestados por los sistemas de información, promover la formación y concienciación en seguridad, designar responsables para el análisis de riesgos y la documentación del sistema, asesorar sobre la categoría del sistema, participar en la elaboración e implantación de los planes de mejora y continuidad, gestionar revisiones y procesos de certificación y elevar al Comité de Seguridad los cambios y requisitos del sistema. Le corresponde aprobar los procedimientos de seguridad que forman parte del mapa normativo cuando no sean competencia del Comité y poner en conocimiento de éste las modificaciones realizadas.

Responsabilidades del Responsable del Sistema

El Responsable del Sistema desarrollará, operará y mantendrá el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios, definiendo la topología y la gestión del sistema, pudiendo detener el acceso a información o la prestación de servicios si detecta deficiencias graves de seguridad. Debe integrar las medidas específicas de seguridad en el marco general de seguridad, asesorar sobre la categoría del sistema, participar en los planes de mejora y continuidad y, en su caso, ejercer funciones de administración de seguridad del sistema, tales como la gestión y configuración de hardware y software de seguridad, la gestión de autorizaciones, la aprobación de cambios de configuración, la supervisión de instalaciones y la monitorización del estado de seguridad e incidencias. Podrá designar responsables de sistema delegados y delegar funciones concretas cuando la complejidad lo justifique.

Delegado de Protección de Datos

El Delegado de Protección de Datos tiene como funciones informar y asesorar a la Universidad y a los usuarios que se ocupen del tratamiento de las obligaciones en materia de protección de datos, supervisar el cumplimiento de la normativa y políticas internas, ofrecer asesoramiento sobre evaluaciones de impacto, cooperar con la Agencia Española de Protección de Datos actuando como punto de contacto y desempeñar sus funciones atendiendo a los riesgos asociados a las operaciones de tratamiento. Debe recabar información sobre las actividades de tratamiento, analizar la conformidad, asesorar y emitir recomendaciones, supervisar el registro de operaciones, asesorar sobre protección de datos desde el diseño y por defecto, sobre evaluaciones de impacto, priorizar actividades según riesgo y aconsejar sobre auditorías, formación y recursos.

Comité de Seguridad TIC (COMSEGTIC)

El Comité de Seguridad TIC tiene como atribuciones mantenerse informado de la normativa de certificación de conformidad con el ENS, de las entidades de certificación acreditadas y esquemas de certificación, proponer directrices y recomendaciones, coordinar esfuerzos en materia de seguridad para asegurar coherencia y evitar duplicidades, atender las inquietudes de la organización informando regularmente a la dirección, resolver conflictos de responsabilidad entre responsables o departamentos, asesorar en materia de seguridad cuando se requiera,

revisar la Política de Seguridad antes de su aprobación por el Consejo de Gobierno y aprobar la normativa de uso de medios electrónicos y el mapa de normativa y procedimientos de seguridad para la implantación del ENS. Durante el proyecto de adecuación al ENS se reunirá al menos trimestralmente; una vez alcanzada la certificación, al menos dos veces al año, pudiendo aumentar la frecuencia según necesidades. Las reuniones se convocarán por su Presidencia y las decisiones se adoptarán por consenso de los miembros permanentes.

Oficina de Seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la Oficina de Seguridad TIC, cuyas competencias abarcan la adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en interconexiones y conectividad y otras funciones relacionadas. Estará dirigida por un Director de la Oficina de Seguridad TIC, nombrado por el Comité y que actuará como enlace con él, siendo el Responsable de Seguridad o su delegado, y contará con un Secretario designado por el Comité y con los administradores especialistas de seguridad que se estimen necesarios. Entre sus funciones están la gestión y operativa de la seguridad del proyecto de adecuación, implantación y gestión de la conformidad ENS, la redacción y presentación de propuestas al Comité, la promoción de la mejora continua del sistema de gestión de la seguridad mediante la elaboración y revisión de la Política y la normativa de seguridad, la verificación de procedimientos, la planificación de formación y sensibilización, la definición de requisitos de formación de administradores y usuarios, la propuesta de planes de mejora con su dotación presupuestaria, el seguimiento de riesgos residuales y la promoción de auditorías periódicas ENS y RGPD. El Director convocará las reuniones de la Oficina, que podrá trabajar en pleno o en grupos de trabajo específicos, elevando sus propuestas al Comité de Seguridad TIC.