ACUERDO de 24 de noviembre de 2016, del Consejo de Gobierno de la Universidad, por el que se aprueba la Política de Seguridad de la Información de la Universidad de Zaragoza.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, tiene por objeto establecer la Política de Seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos, informaciones y servicios utilizados en medios electrónicos que se gestionen en el ejercicio de sus competencias.

De conformidad con lo previsto en el artículo 11 del Real Decreto 3/2010, de 8 de enero, todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad.

Por todo ello el Consejo de Gobierno de la Universidad de Zaragoza en sesión celebrada el día 24 de noviembre de 2016, acuerda aprobar la siguiente.

Política de Seguridad de la Información

1. Entrada en vigor.

Texto aprobado el día 24 de noviembre de 2016, por el Consejo de Gobierno de la Universidad de Zaragoza.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. Introducción.

La Universidad de Zaragoza, en adelante UNIZAR, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos institucionales. En consecuencia, 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 a los servicios prestados.

Por ello, 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 y 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 la UNIZAR y su personal debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, conocer y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La UNIZAR 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 UNIZAR debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica.

2.1. Prevención.

La UNIZAR debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar 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 papeles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la UNIZAR debe:

csv: BOA20170201002

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

2.2. Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada 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 y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta.

La UNIZAR debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones, con respecto a incidentes detectados en áreas de la entidad, o en otros organismos relacionados con la UNIZAR.
- 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) reconocidos a nivel nacional: IRIS-CERT, CCN-CERT,….

2.4. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, la UNIZAR debe desarrollar planes de continuidad de los sistemas TIC, como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. Misión.

Según los Estatutos de la Universidad de Zaragoza, esta es una Institución con personalidad jurídica y patrimonio propio, que goza de autonomía académica, económica, financiera y de gobierno, de acuerdo con la Constitución y las leyes, para el ejercicio del servicio público de la educación superior mediante el estudio, la docencia y la investigación.

De forma estrechamente relacionada con el cumplimiento de esta misión, la UNIZAR desea manifestar la necesidad de una infraestructura TIC que prime y fomente el seguimiento de estándares, operativas abiertas y las mejores prácticas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos de la institución.

4. Alcance.

La UNIZAR establece la aplicación de la presente política de seguridad sobre todo el conjunto de sistemas de información, que permiten a la Universidad de Zaragoza prestar el servicio público de educación superior.

La presente política se aplicará a todos los servicios, sistemas y recursos TIC de la Universidad de Zaragoza. Son recursos TIC de la Universidad de Zaragoza todos los sistemas centrales y departamentales, puestos de trabajo, dispositivos, sistemas de almacenamiento, redes, aplicaciones (software) que sean de su propiedad.

Queda fuera de la presente, por tanto, equipos no inventariados a nombre de la Universidad de Zaragoza. No obstante, en el caso de que se acceda a la red corporativa mediante dichos equipos, quedarán sujetos a las obligaciones establecidas en la presente Política de Seguridad de la Información y normas e instrucciones de desarrollo.

La Política de Seguridad de la Información se aplica también a todas aquellas personas, indistintamente del colectivo al que pertenezcan, Centros, Departamentos, Institutos, entidades, unidades o servicios, sean internos o externos, que hagan uso de los recursos de las TIC de la Universidad de Zaragoza.

De forma más específica el ENS se aplica, inicialmente, sobre todos aquellos sistemas que presten servicios centralizados, prestados por el SICUZ y que se identifiquen como relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos, o con el acceso al procedimiento administrativo. Deberá analizarse la situación en el resto de la UNIZAR.

4.1. Servicio dentro del alcance.

A continuación se recoge una relación de los servicios incluidos en el alcance de aplicación del ENS:

- Sistema de Gestión Corporativo (ERP):
- Servicio de Gestión Académica.

csv: BOA20170201002

- Servicio de Gestión Económica.
- Servicio de Gestión de la Investigación.
- Servicio de Gestión de los Recursos Humanos.
- Sistema de Administración Electrónica:
- Servicio de Trámite y Registro Electrónico.
- Servicio de Archivo.
- Sistema de Docencia Virtual:
- Servicio de Docencia Virtual.
- Sistema de Servicios de Apoyo Universitario:
- Servicio de Biblioteca.
- Servicio de Atención al Usuario.

4.2. Ampliación del alcance.

Por último, se desea manifestar que adicionalmente, y aun entendiéndose que los siguientes servicios no se encuentran directamente en el alcance marcado por ENS, debido a su importancia en la comunidad universitaria, se acuerda extender el alcance a los siguientes:

- Sistema de Servicios de Apoyo Universitario.
- Servicio de Web Institucional.
- Servicio de Estadística para toma de Decisiones.

5. Declaración de la Política de Seguridad.

El propósito de esta Política de Seguridad de la Información es proteger la información y los servicios de la Universidad de Zaragoza. Es la política de esta entidad asegurar que:

- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad e integridad.
- 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.

La Universidad de Zaragoza implementará, mantendrá y realizará un seguimiento del cumplimiento del ENS.

6. Marco normativo.

Es de aplicación la legislación española en relación a protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, la UNIZAR podrá ser requerida por los órganos administrativos pertinentes, a proporcionar los registros electrónicos, o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco jurídico definido, entre otras, por las siguientes normas:

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- 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.
- Ley 39/2015, de 1 de octubre, del procedimiento administrativo común.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, así como por el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente dicha Ley, en aquellos artículos que continúen vigentes de conformidad con lo previsto en la disposición derogatoria única de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

7. Organización de la seguridad.

7.1. Comités: Funciones y responsabilidades.

El Comité de Seguridad TIC estará formado por:

- Secretario General.
- Gerente.
- Vicerrector o Adjunto al Rector con competencias en infraestructuras.
- Vicerrector o Adjunto al Rector con competencias en informática y comunicaciones.
- Máximo responsable técnico del Servicio de Informática y Comunicaciones.

csv: BOA20170201002

El Comité de Seguridad TIC estará presidido por el Secretario General y actuará como secretario el Gerente, teniendo como funciones:

- Convocar por orden del Presidente las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.

La Comisión se reunirá en sesión ordinaria al menos una vez al año, con el objeto de elaborar el informe, que remitirá al Consejo de Gobierno, y que coincidirá con la entrega de los indicadores para el Informe Nacional del Estado de Seguridad (INES). Podrá reunirse, igualmente, en sesión extraordinaria en cada ocasión en que los asuntos relacionados con sus competencias lo requiera. Las reuniones serán convocadas por la presidencia de la Comisión, ya sea por propia iniciativa, ya a petición de cualquiera de sus componentes, con una antelación mínima de 5 días hábiles en el caso de tratarse de una sesión ordinaria y de 48 horas cuando se trate de una sesión extraordinaria.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Divulgación de la política y normativa de seguridad de la UNIZAR.
- Aprobación de la normativa de seguridad de la UNIZAR.
- Revisión anual de la política de seguridad para que sea aprobada por el Consejo de Gobierno.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Promoción, supervisión y aprobación de las tareas de seguimiento del ENS:
- Tareas de adecuación.
- Análisis de Riesgos.
- Planes de mejora de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.
- Elaborar la estrategia de evolución de la Universidad de Zaragoza en lo que respecta a seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Monitorizar los principales riesgos residuales asumidos por la Universidad de Zaragoza y recomendar posibles actuaciones respecto de ellos.
- Coordinar los esfuerzos de las diferentes áreas universitarias 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.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

7.2. Roles: Funciones y responsabilidades.

Responsable de la información.

El Secretario General tendrá el rol de responsable de la información de la UNIZAR, ejerciendo las siguientes funciones:

- Establecimiento de los requisitos de la información en materia de seguridad. Buen uso, protección, integridad y confidencialidad.
- Determinar los niveles de seguridad de la información.
- Trabajo en colaboración con el responsable de seguridad y el de sistema en el mantenimiento de los sistemas catalogados según el anexo I del ENS.

Responsable de los servicios.

El Gerente tendrá el rol de responsable de los servicios de la UNIZAR, correspondiéndole las funciones siguientes:

- Establecimiento de los requisitos de los servicios en materia de seguridad, interoperabilidad, accesibilidad, disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Trabajo en colaboración con el responsable de seguridad y el de sistema, en el mantenimiento de los sistemas catalogados, según el anexo I del ENS.

Responsable de Seguridad.

El máximo responsable técnico del Servicio de Informática y Comunicaciones (en adelante, SICUZ) tendrá el rol de responsable de seguridad de la UNIZAR, con las funciones las siguientes:

csv: BOA20170201002

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC, en su ámbito de responsabilidad.

- Promover la formación y concienciación del SICUZ, dentro de su ámbito de responsabilidad.

- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y de los servicios prestados.

- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

- Apoyar y supervisar la investigación de los incidentes de seguridad, desde su notificación hasta su resolución.

- Elaborar el informe periódico de seguridad, incluyendo los incidentes más relevantes del periodo.

- Aprobar los procedimientos de seguridad elaborados por el Responsable del Sistema.

- Elaborar la normativa de seguridad de la entidad.

Responsable del Sistema TI.

El Comité de Seguridad TIC de la UNIZAR designa a los Directores de Área del SICUZ en el rol de responsables del Sistema de Información de la UNIZAR, teniendo por funciones, dentro de sus áreas de actuación, las siguientes:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y política de gestión del Sistema, estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.

- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.

- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema, durante las etapas de desarrollo, instalación y prueba del mismo.

- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.

- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.

- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.

- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.

- Determinar la categoría del Sistema según el procedimiento descrito en el anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el anexo II del ENS.

- Elaborar y aprobar la documentación de seguridad del Sistema.

- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.

- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).

- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.

- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

- Además, 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 seguridad, antes de ser ejecutada.

- Elaboración de los procedimientos de seguridad necesarios para la operativa en el Sistema.

Responsable de la Administración de Seguridad del Sistema (ASS).

El Comité de Seguridad TIC de la UNIZAR autorizará que, a criterio de la dirección del SICUZ, ésta designe a un técnico de informática en el rol de responsable de la ASS, cuyas funciones, dentro de sus áreas de actuación, serán las siguientes:

- Hacer seguimiento y colaborar en la implementación y mantenimiento de las medidas de seguridad, aplicables al Sistema de Información.

- Hacer seguimiento y colaborar en 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.

csv: BOA20170201002

- Hacer seguimiento y colaborar en la aplicación de los Procedimientos Operativos de Seguridad.
- Controlar 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.

7.3. Procedimiento de designación.

Acorde a los puestos reflejados en la Política de Seguridad.

7.4. Revisión de la Política de Seguridad.

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

8. Datos de carácter personal.

La UNIZAR realiza tratamientos en los que hace uso de datos de carácter personal. El Documento de Seguridad LOPD de la UNIZAR se puede encontrar impreso en papel, en las dependencias del SICUZ. Este documento recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de la UNIZAR 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.

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 cada dos años.
- 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.

10. Desarrollo de la Política de Seguridad.

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

La Política de Seguridad de la Información de la Universidad de Zaragoza estará disponible en la página web de la Universidad, a través de la siguiente dirección https://zaguan.unizar.es/record/58381.

11. Obligación del personal.

Todos los miembros de la UNIZAR tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

csv: BOA20170201002

Todos los miembros de la UNIZAR recibirán información de forma regular en materia de seguridad TIC. Se establecerá un programa de acciones de concienciación continua para atender a todos los miembros de la UNIZAR, 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, como si se trata de un cambio de puesto de trabajo, o de responsabilidades en el mismo.

12. Terceras partes.

Cuando la UNIZAR 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 UNIZAR 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 la normativa indicada, 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 indica 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 también la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Zaragoza, 24 de noviembre de 2016.— El Rector, José Antonio Mayoral Murillo.

csv: BOA20170201002