POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

1 Aprobación y Entrada en Vigor

Mediante Acuerdo del Consejo de Gobierno de 12 de junio de 2018, se aprobó la Política de Seguridad de la Información de la Universidad Internacional de Andalucía.

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 Internacional de Andalucía depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que la Universidad Internacional de Andalucía y todo su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (Real Decreto 3/2010), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La Universidad Internacional de Andalucía 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 entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1 Prevención

La Universidad Internacional de Andalucía 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 implementará las medidas mínimas de seguridad

determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Universidad Internacional de Andalucía debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 Respuesta

La Universidad Internacional de Andalucía:

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

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Universidad Internacional de Andalucía desarrollará planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación en aquellos servicios en que sea necesario.

3 Alcance

Esta política de seguridad será de obligado cumplimiento para todos los miembros de la Universidad Internacional de Andalucía, siendo aplicable a todos los activos empleados por el mismo en la prestación de los servicios a los ciudadanos, a otras administraciones, así como para su propia gestión y funcionamiento.

4 Misión

Universidad Pública del Sistema Universitario Andaluz, de posgrado, comprometida con el progreso sostenible de su entorno, con vocación internacional y de cooperación solidaria, especialmente con América Latina y el Magreb, que responde con calidad, innovación, agilidad y flexibilidad a los retos emergentes de la sociedad en los diferentes campos de las ciencias, la tecnología, la cultura y las artes.

5 Marco normativo

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

- De ámbito Europeo:
    - Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas del mercado interior (Idas) y normas de ejecución.
    - 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.
    - Directiva (UE) 2016/1148 del Parlamento Europeo y el Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
    - Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.
- De ámbito Estatal:
    - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
    - Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
    - 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 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- 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 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- 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.
- Resolución de 7 de octubre de 2016 de la Secretaría de estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de Informe de Estado de Seguridad.
- Resolución de 13 de octubre de 2016 de la Secretaría de estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- 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.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- De ámbito Autonómico:
    - Decreto Legislativo 1/2013, de 8 de enero, por el que se aprueba el Texto Refundido de la Ley Andaluza de Universidades.
    - Ley 1/2014 de 24 de junio de Andaluza de Transparencia Pública de Andalucía
- De ámbito Interno:
    - Estatutos de la Universidad Internacional de Andalucía. decreto 236/2011, de 12 de julio.
    - Normativa de registro de la Universidad Internacional de Andalucía. BOJA 16/3/2018.
    - Otras normas que en la actualidad o en el futuro, de carácter general o interno, resulten de aplicación a la Universidad en el marco de esta Política de Seguridad.

6 Organización de la Seguridad

La implantación de la Política de Seguridad en la Universidad Internacional de Andalucía requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsable del Servicio

c) Responsable de la Información

d) Responsable de Seguridad de la Información

e) Delegado de Protección de Datos

f) Responsable del Sistema

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

6.1 Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el órgano de gestión interna al que compete la Seguridad de la Información en la UNIA.

Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

El Comité de Seguridad de la Información recabará información y auxilio de todas las áreas de la Universidad cuando así lo considere necesario. Todas las áreas, servicios y unidades de la Universidad Internacional de Andalucía están obligadas a informar y prestar apoyo al Comité de Seguridad de la Información cuando éste lo requiera.

El Comité de Seguridad de la Información tiene las siguientes funciones y responsabilidades:

- Elaborar la estrategia de evolución de la Universidad Internacional de Andalucía en lo que respecta a la seguridad de la información. Identificar, revisar y proponer objetivos estratégicos en materia de seguridad de la información.
- Informar del estado de la seguridad de la información a los Órganos de Gobierno de la Universidad.
- Proponer al Consejo de Gobierno la aprobación de la política de seguridad de la información.
- Proponer al Rector la aprobación de las modificaciones sobre la política de seguridad.
- Proponer al Rector la aprobación de las normativas y reglamentos de seguridad relacionados con la aplicación del ENS.
- Proponer las iniciativas principales para mejorar la gestión de la seguridad de la información, incluyendo la divulgación de la política y normativas de seguridad.
- Coordinar la adopción de acciones y medidas encaminadas a la adaptación de la Universidad Internacional de Andalucía al Esquema Nacional de Seguridad.
- Asegurar la disponibilidad de los recursos necesarios para llevar a cabo los planes de acción relacionados con la seguridad de la información o priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Proponer la designación de los responsables encargados de la aplicación y supervisión de las medidas de seguridad.
- Aprobación de los procedimientos de seguridad de la UNIA cuando así lo solicite el Responsable de Seguridad.
- Realizar una revisión anual del contenido de la Política de Seguridad y una propuesta de actualización cuando sea necesario.
- Resolver los conflictos entre los diferentes responsables.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:

- Grado de cumplimiento del plan de adecuación.
- Revisión de los resultados obtenidos en las diferentes actualizaciones del análisis de riesgos y los niveles de riesgo alcanzados.
- Resultados de las auditorías bienales que se realicen y otros informes asociados a la idoneidad de los controles de seguridad implantados, identificando las causas origen de las excepciones que pudieran existir y proponiendo acciones de mejora.

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

- Convocar 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.

6.2 Responsable de la Información

Tiene las siguientes funciones y responsabilidades:

- Establecer los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que es responsable.
- Valorar para cada información contemplada en el análisis de riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Trabajar en colaboración con el Responsable de Seguridad y el de Sistema en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

6.3 Responsable del Servicio

Tiene las siguientes funciones y responsabilidades:

- Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información.
- Valorar para cada servicio contemplado en el análisis de riesgos las diferentes

dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).

- Trabajar en colaboración con el Responsable de Seguridad y el de Sistema en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

6.4 Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en el ámbito de cumplimiento del ENS.
- Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos prestados por la Universidad según el criterio de valoración establecido por el artículo 43 del ENS.
- Realizar o instar la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Universidad en materia de seguridad.
- Supervisar el estado de seguridad del sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.
- Elaborar la normativa de seguridad.
- Promover la formación y concienciación del personal de la Universidad y en especial, del personal del Servicio Informático involucrado en las labores de gestión de los sistemas de información que dan soporte a los procesos de Administración Electrónica de la Universidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.

- Aprobar los procedimientos de seguridad elaborados por los Responsables de los Sistemas cuando en virtud del contenido definido no requieran la revisión y aprobación del Comité de Seguridad.
- Elaborar como secretario del Comité los siguientes informes periódicos:
    - Resumen consolidado de las actuaciones llevadas a cabo y en curso dentro del desarrollo del Plan de adecuación del ENS aprobado.
    - Resumen consolidado de los incidentes de seguridad registrados desde la última reunión del Comité.
    - Valoración del estado de la seguridad de los sistemas de información afectados por el ENS y la evolución de los niveles de riesgo a los que están expuestos.
    - Resumen consolidado de los procedimientos de seguridad aprobados por el Responsable de Seguridad desde la última reunión del Comité.

6.5 Delegado de Protección de Datos

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

6.6 Responsable del Sistema

Es responsable de asegurar la ejecución de medidas para asegurar los activos y servicios de los sistemas de información, que soportan la actividad de la Universidad Internacional de Andalucía, de acuerdo a los objetivos de la organización.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la tipología y los procedimientos 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.
- Establecer planes de contingencia y los procesos de análisis y gestión de riesgos en el Sistema.
- 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 la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, efectuar la comunicación al Responsable de Seguridad o a quién éste determine

7 Procedimientos de designación

Se designan las siguientes responsabilidades:

- Responsable de la Información: Secretaría General
- Responsable del Servicio: Gerencia
- Responsable de Seguridad: designada por el Rector.
- Delegado de Protección de Datos: designada por el Rector.
- Responsable del Sistema: Dirección del Área TIC.

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por el Rector a propuesta del Comité de Seguridad TIC.

8 Revisión de la Política de Seguridad de la Información

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

9 Datos de Carácter Personal

La Universidad Internacional de Andalucía 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.

10 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 de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información 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.

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 Internacional de Andalucía en materia de protección de datos de carácter personal.

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 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 URL:

www.unia.es/seguridad-de-la-informacion

12 Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de la Universidad Internacional de Andalucía 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 Internacional de Andalucía 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 Internacional de Andalucía recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Universidad Internacional de Andalucía, 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

13 Terceras partes

Cuando la Universidad Internacional de Andalucía preste servicios a otros organismos o manejen 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad Internacional de Andalucía utilice servicios de terceros o cedan 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.