POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundació Universitat-Empresa de València - ADEIT

Febrero 2025

Historial de cambios		
Versión	**Fecha**	**Descripción del cambio**
0.1 a 1.2	Marzo 2020 a Febrero 2023	Diferentes versiones desde primer borrador para discusión en marzo de 2020, añadiendo responsabilidades y funciones, marco regulatorio, política de seguridad de la UV, composición del comité TIC, análisis de riesgos, modificación según RD311/2022
1.2	Septiembre 2022	Revisión en reunión 30 de septiembre y aprobación para paso a final de año a aprobación por parte del Patronato de ADEIT
20230216	Febrero 2023	Se revisa la parte de categorización, índice, se añade algunos de los requisitos que faltaban (gestión de incidentes o funcionalidad mínima, por ejemplo).
20250220	Febrero de 2025	Se revisan y actualizan algunos apartados por cuestión de matiz, adaptación, mejora o cambios poco significativos

Última revisión y aprobación		
1.1	Responsable de Seguridad	Vicente L. Francés
V20230216	Responsable de Seguridad	Vicente L. Francés
V20230327	Aprobación por el Comité TIC para su aprobación definitiva por el Patronato de la Fundación en fecha 30 de marzo de 2023	Comité de Seguridad TIC
V20230327	Aprobación por el Patronato de la Fundación en fecha 30 de marzo de 2023	Patronato de la Fundación
V20250220	Revisión y actualización para aprobación por el Comité de seguridad TIC en fecha 26 de febrero de 2025	Vicente L. Francés, Mar Nieto, Gabriel Roger
V20250220	Aprobación por el Comité de seguridad TIC el 26 de febrero de 2025	Comité de Seguridad TIC
V20250220	Aprobación por la Comisión Ejecutiva y Patronato de la Fundación en fecha 10 de marzo de 2025	Comisión Ejecutiva y Patronato de la Fundación

Este documento debe estar disponible en el web del ADEIT una vez presentado y aprobado por la Comisión Ejecutiva y Patronato de ADEIT.

Índice

1. Aprobación y entrada en vigor

Texto aprobado por el Comité de seguridad TIC de la Fundación en fecha 26 de febrero de 2025.

Texto aprobado por la Comisión Ejecutiva y Patronato en fecha 10 de marzo de 2025.

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

2. Introducción

La Fundación Universidad-Empresa de la Universitat de València (Consell Social de la Universitat de València. Estudi General de València), de la Comunitat Valenciana, Medio Propio de la Universitat de València (en adelante "**la Fundación**" o "**ADEIT**") es una organización, con personalidad jurídica propia, promovida por el Consell Social de la Universitat de València en 1989, cuyo objetivo es, por un lado, que la sociedad aproveche las capacidades de la Universidad y, por otro, servir de cauce para trasmitir a la Universidad las necesidades e inquietudes de la sociedad en general y las de los sectores productivos en particular.

Para ello, ADEIT fomenta el desarrollo de actividades conjuntas en todos aquellos campos que favorezcan el intercambio de conocimientos y que, como consecuencia, impulsen el desarrollo y progreso económico.

3. Objetivos y misión de ADEIT

Los principales ejes de actuación son los siguientes:

- Formación, especialización y reciclaje de universitarios y profesionales.
- Prácticas de estudiantes universitarios en entidades y empresas. Asesoramiento para la búsqueda de empleo o la creación de empresas.
- Difusión de la cultura emprendedora.
- Apoyo a la innovación y a la transferencia de tecnología y conocimiento.

La misión de ADEIT es:

- Promover y fomentar las relaciones entre la Universitat de València y el entorno empresarial y profesional, facilitando el intercambio de las necesidades y conocimientos entre ambas.

La visión de ADEIT es:

- Ser reconocida como un referente nacional e internacional por su capacidad de generación de modelos y herramientas de cooperación entre la Universidad y la empresa, convirtiéndose en un agente clave en actividades de innovación, formación, empleo y emprendimiento de la Universitat de València.

Los valores de ADEIT son

- Visión global de la Universitat de València
- Integración y coordinación de servicios
- Satisfacción del cliente
- Gestión eficaz y eficiente
- Innovación y mejora continua
- Sostenibilidad y adaptación al cambio
- Compromiso con los grupos de interés
- Conocimiento y especialización
- Profesionalidad
- Confianza e imagen

4. Principios Básicos de Seguridad

Los principios básicos de seguridad actuales , sin perjuicio de ser modificados en el futuro, son:

a. Organización e implantación del proceso de seguridad.
b. Análisis y gestión de los riesgos.
c. Gestión de personal.
d. Profesionalidad.
e. Autorización y control de los accesos.
f. Protección de las instalaciones.
g. Adquisición de productos de seguridad y contratación de servicios de seguridad.
h. Mínimo privilegio.
i. Integridad y actualización del sistema.
j. Protección de la información almacenada y en tránsito.
k. Prevención ante otros sistemas de información interconectados.
l. Registro de la actividad y detección de código dañino.
m. Incidentes de seguridad.
n. Continuidad de la actividad.
o. Mejora continua del proceso de seguridad.

5. Prevención de riesgos

Las tareas que realizará ADEIT en relación con prevención son:

- Estudiar el impacto y posibles riesgos de nuevos sistemas o servicios antes de autorizar su implantación y puesta en marcha.
- Evaluar periódicamente la seguridad.
- Solicitar de forma periódica a terceros la evaluación de seguridad.

6. Detección de anomalías

ADEIT deberá monitorizar sus sistemas y servicios de forma continua para detectar anomalías en los niveles de prestación de servicios y actuar en consecuencia al artículo 9 del ENS (Esquema Nacional de Seguridad).

Cada 2 años, al menos, se realizará una auditoría interna.

7. Respuesta ante incidentes

Las tareas que realizará ADEIT en relación con la respuesta son:

- Establecer mecanismos para responder a los incidentes de seguridad.
- Establecer un punto de contacto para las comunicaciones con respecto a incidentes de seguridad.
- ADEIT utilizará la herramienta INES del CCN para el intercambio de información relacionada con los incidentes de seguridad.

8. Recuperación de sistemas

Para garantizar la disponibilidad de los servicios críticos para ADEIT, se ha desarrollado un plan de continuidad de los sistemas TIC en el que se proporciona toda la información suficiente para recuperar los sistemas en el tiempo garantizado.

9. Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)

El **alcance** del SGSI son los servicios que ADEIT provee y la información que los sustenta.

Los **servicios incluidos** en el alcance del SGSI de ADEIT que tienen que cumplir con el ENS son:

[SE 01] Títulos Propios UV

[SE 02] Servicios e-Learning

[SE 03] Becas de formación profesional prácticas (BFPP)

[SE 04] Gestión Económico-Administrativa

[SE 05] Gestión de RRHH

[SE 06] Prácticas de Empresa

[SE 07] Espacios. Edificio. Aulas

[SE 09] Gestión de ideas de emprendimiento

[SE 10] Servicios en la Web

[SE 11] Congresos y cursos

La **información** en el alcance del SGSI de ADEIT que tiene que cumplir con el ENS es:

[AD_IN_01] Profesores Universidad UV

[AD_IN_02] Profesionales externos

[AD_IN_03] Datos de Títulos Propios UV/ Guías docentes

[AD_IN_04] Carga docente de Títulos Propios UV/ Tarifas Profesores

[AD_IN_05] Alumnos Títulos Propios UV con información de pagos

[AD_IN_06] Actas de Títulos Propios UV

[AD_IN_07] Títulos expedidos de Títulos Propios UV

[AD_IN_08] Datos de cursos Aula Virtual

[AD_IN_09] Video vigilancia

[AD_IN_10] Inscritos congresos/cursos con información de pagos

[AD_IN_11] Estudiante / Titulados UV

[AD_IN_12] Entidades / Empresas

[AD_IN_13] Clientes / Proveedores

[AD_IN_15] Personal de ADEIT

[AD_IN_17] Datos de oferta formativa de prácticas / becas

10. Categorización

La **categoría** del sistema de ORGANIZACIÓN es de **NIVEL MEDIO** como se puede ver en el documento de Categorización del sistema "ADEIT-CategorizacionDelSistema". Dicha valoración ha sido realizada por el Responsable de Seguridad.

Este Nivel se ha obtenido a partir de la valoración CITAD (en cuanto al daño de un impacto en las dimensiones de seguridad: Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad) de información y servicios mencionados en el apartado anterior, realizada por sus responsables.

11. Marco normativo o regulatorio

La normativa aplicable a ADEIT es:

- 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 (RGPD).
- Ley 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales (LOPD y GDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que señala en su art. 17.3 que los medios o soportes en que se almacenen documentos , deberán contar con las medidas de seguridad que establece el Esquema Nacional de Seguridad, que garanticen una serie de principios (como integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados); y, establece también, en su art. 27.3 que las Administraciones Públicas deberán cumplir con el Esquema Nacional de Seguridad para garantizar la identidad y contenido de las copias electrónicas o en papel, es decir, el carácter de copias auténticas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- 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. Disposición Adicional Primera y por remisión, artículos 52 a 55 y 59.
- Estatuto de los Trabajadores.
- Convenio Colectivo de Oficinas y Despachos de la provincia de Valencia.
- Instrucciones técnicas de seguridad, esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema Nacional de Seguridad, según establece en su disposición adicional segunda el Real Decreto 311/2022:
    1. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe de Estado de la Seguridad.
    2. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
    3. Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
    4. Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

12. Organización de la seguridad

12.1. Funciones del Comité de Seguridad TIC

Siguiendo el artículo 10 del ENS se definen los siguientes roles que formarán el Comité de Seguridad TIC de ADEIT.

Las funciones del Comité de Seguridad TIC son:

- Elaborar y revisar periódicamente la política de seguridad de la información para que sea aprobada por el Patronato de ADEIT.
- Aprobar y divulgar la Normativa de Seguridad de ADEIT.
- Promover la mejora continua de la gestión de la seguridad de la información de ADEIT.
- Coordinar los esfuerzos en materia de seguridad de la información con la Universitat de València.
- Evaluar los principales riesgos residuales para ADEIT y recomendar posibles actuaciones respecto de estos riesgos.
- Evaluar el cumplimiento de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones. En particular, velar por la coordinación en las áreas de seguridad en gestión de incidentes con la Universitat de València.
- Promover la realización de auditorías periódicas y evaluar el cumplimiento de las obligaciones de ADEIT en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad de acuerdo con los recursos disponibles.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación hasta su puesta en operación. En particular, velar por la creación y utilización de servicios horizontales que reduzcan duplicados y secunden un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que pueda haber entre los diferentes responsables y/o departamentos del ADEIT y pasar a dirección aquellos casos en que no tenga suficiente autoridad para decidir.
- Evaluar las necesidades de recursos requeridos para el cumplimiento de los planes de actuación derivados de la aplicación de la política de seguridad.
- Promover la formación y concienciación de todos los trabajadores en materia de seguridad de la información y ciberincidentes.
- Elaborar un informe anual sobre el estado de la seguridad de ADEIT.

12.2. Composición del Comité TIC

El Comité TIC de Seguridad estará formado por los siguientes roles:

- El Responsable de la Seguridad.
- El Responsable de los Servicios e Información.
- El Delegado de Protección de Datos.

- El Administrador de Seguridad o Responsable de Sistemas.

En las actas del Comité de Seguridad TIC están relacionados los miembros de este comité y sus funciones.

12.2.1. Un Responsable de la Seguridad

El Responsable de Seguridad será único para todo ADEIT, que tendrá responsabilidad sobre los parámetros y controles del Anexo I del ENS, incluyendo los siguientes deberes y responsabilidades:

- Mantener la seguridad de la información usada y de los servicios prestados por los sistemas TIC.
- Realizar las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del ADEIT en materia de seguridad.
- Determinación de las decisiones de seguridad para satisfacer las necesidades de cada uno de los servicios.
- Supervisar regularmente, junto con el responsable de sistemas, la seguridad de las infraestructuras y sistemas de ADEIT e informar a los responsables de los servicios correspondientes.
- Recopilar información de vulnerabilidades o amenazas detectadas e informar sobre brechas de seguridad.
- Promover la formación y concienciación del personal del ADEIT en relación con la seguridad en el uso de los sistemas TIC.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información usada y los servicios prestados.
- Aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Verificar los informes de monitorización y auditoría del estado de la seguridad de los sistemas.
- Fomentar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el Comité TIC de Seguridad incluyendo los incidentes más importantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por los responsables de los sistemas cuando en virtud de su contenido no requiera la aprobación del Comité TIC de Seguridad.
- Proponer la redacción de la normativa de seguridad del ADEIT que se considere necesaria formalizar.
- Determinar la categorización de los sistemas y los requisitos de seguridad con carácter previo a la entrada de un nuevo servicio.

El Responsable de Seguridad será propuesto por la dirección de ADEIT. Una vez aprobado y bajo el cumplimiento de una serie de requisitos (cómo el que asuma las responsabilidades y deberes anteriormente expuestos) será designado como Responsable de Seguridad que tendrá independencia de los miembros del Consejo. Nunca deberá ejercer otros roles de seguridad, cómo el de la LOPD/GDPR o el de Responsable de sistemas, por segmentación de funciones y para lograr que sea independiente de lo que debe pedir responsabilidades a otras personas de ADEIT.

Para su renovación, deberá ser reunido el Comité TIC que valorará ésta utilizando criterios objetivos.

12.2.2. Un Responsable de los Servicios e Información

El Responsable de Servicios e Información estará encargado de:

- Trabajar en colaboración con el responsable de seguridad y el responsable de sistemas.
- Recopilar necesidades de seguridad de cada uno de los jefes de departamentos o responsables de los servicios proporcionados por el ADEIT.
- Determinar los requisitos de seguridad de los parámetros del Anexo I del ENS para cada uno de los servicios de ADEIT que deberán ser posteriormente tratados por el responsable de seguridad e implementados por el responsable de sistemas.
- Especificar las condiciones de seguridad en el ciclo de vida de los servicios de los que son responsables, incluyendo los controles que fueran necesarios.
- Valorar las consecuencias e impactos relativos a seguridad en relación con la protección de sus activos y cumplimiento de sus obligaciones de servicio, que incidirá en la categorización de cada uno de los servicios proporcionados con respecto a la seguridad.
- Informar sobre posibles vulnerabilidades o amenazas detectadas al responsable de seguridad y al responsable de sistemas.
- Cada responsable del servicio o/y de la información deberá determinar cuál es el nivel del servicio de acuerdo con cómo afectaría un incidente al servicio considerando las dimensiones de seguridad (Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad). Estas valoraciones son las que se han usado para determinar la categoría del sistema.

El responsable de servicios e información será **propuesto** por los miembros del Comité de Seguridad TIC y aceptado por el consenso de todos sus miembros. Una vez aprobado y bajo el cumplimiento de una serie de requisitos (cómo el que asuma las responsabilidades y deberes anteriormente expuestos) será designado como responsable de servicios e información que tendrá independencia de los miembros del Comité de Seguridad TIC.

Para su renovación, deberá ser reunido el Comité TIC que valorará ésta utilizando criterios objetivos

12.2.3. Delegado/a de la Protección de Datos (DPD)

Es la persona encargada de realizar las funciones relacionadas con la normativa reguladora de protección de datos (RGPD y LOPD). Esta persona es la que ostenta la responsabilidad de Delegado de Protección de Datos de la Universitat de València.

Su designación y renovación será el de la propia Universitat de València de la cual ADEIT es medio propio.

12.2.4. Administrador de Seguridad o Responsable de Sistemas

El Administrador de Seguridad o Responsable de Sistemas realizará las siguientes funciones:

- La operación de los servicios y sistemas de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- La realización de tareas de control, monitorización y detección de problemas de seguridad incluyendo auditorías internas.
- Definir las configuraciones básicas tanto hardware como software de los puestos de trabajo y administrar los accesos a la red corporativa.
- Comprobar la profesionalidad de los miembros del departamento de sistemas, comprobando que la seguridad de los sistemas esté atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.
- Velar por el funcionamiento correcto del sistema durante todo su ciclo de vida, de sus especificaciones e instalaciones, e incorporar los requisitos de seguridad necesarios para la operativa del sistema.
- Definir la tipología y la política de gestión del sistema y establece los criterios de uso y los servicios están disponibles.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.
- Proponer al responsable de seguridad los cambios que afecten a la seguridad del sistema.
- Decidir las medidas de seguridad que se aplicarán a los proveedores de componentes del sistema durante las etapas de desarrollo, instalación y prueba.
- Implantar y controlar las medidas específicas de seguridad del sistema y comprobar que se integran adecuadamente dentro del marco general de seguridad.
- Aprobar toda la modificación sustancial de la configuración de cualquier elemento del sistema que afecte a la seguridad y la disponibilidad de los servicios.
- Llevar a cabo el proceso de revisión periódica del análisis de gestión de riesgos en el sistema.
- Investigar los incidentes de seguridad que afecten al sistema y en su caso, comunicar al responsable de seguridad o a quién éste determine.

- Comunicar la información relativa a ciberincidentes producidos en ADEIT al CCN a través de la herramienta INES en los plazos establecidos para ello.
- Establecer planes de contingencia y emergencia.

Todos estos perfiles (el responsable de seguridad, el responsable de los servicios e información, el DPD y el responsable de sistemas) forman el Comité TIC de Seguridad de la Información de ADEIT.

En general, siguiendo la guía de CCN STIC-801 de responsabilidades, se diferenciarán tres grandes bloques de responsabilidades:

- La responsabilidad legal, que corresponde a la dirección del ADEIT y a los responsables de los tratamientos.
- La supervisión, que corresponde al responsable de seguridad y al DPD.
- La operación del sistema o servicio, que corresponde al responsable de cada uno de los servicios proporcionados por ADEIT.

13. Profesionalidad

Los responsables mencionados anteriormente deberán poder demostrar:

- Formación en seguridad.
- Experiencia profesional, experiencia en seguridad.
- Tener roles parecidos (el Responsable de Seguridad será quien sea el responsable de cumplimiento del ENS y la LOPD).
- El auditor debe estar certificado como tal o en su defecto de la ISO 27001 o CISA u otros certificados similares.
- Deben ser profesionales que con diligencia gestionen la seguridad de la organización.

14. Política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de ésta. La Política será aprobada por la Comisión Ejecutiva y el Patronato, y difundida por el Comité de Seguridad TIC para que la conozcan todas las partes afectadas.

Así mismo, el Comité de Seguridad TIC aprobará la normativa de seguridad de los sistemas de información de ADEIT y la dará a conocer internamente a los trabajadores de ADEIT pudiéndose publicar en la web de ADEIT.

El cumplimiento de las responsabilidades definidas en esta política de seguridad está determinado por el acceso a los diferentes cargos que se vinculan a esas responsabilidades.

15. Datos de carácter personal

ADEIT trata datos de carácter personal sometidos al RGPD Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecto al tratamiento de datos de carácter personal y a la libre circulación de estos datos, así como a la LOPD y GDD Ley Orgánica 3/2018 de protección de datos personales y garantía de derechos digitales

El documento de Registro de Actividades del Tratamiento RAT, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de ADEIT 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 RAT.

Las medidas técnicas y organizativas de seguridad están adaptándose al estado de la técnica, los costes de aplicación y la naturaleza, ámbito, objetivo, contexto y finalidad del tratamiento, así como a riesgos de probabilidad e impacto variable de los derechos de las personas físicas.

16. 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.

Los responsables de cada uno de los procesos para el establecimiento del ENS en ADEIT, incluyendo la gestión de riesgos serán los siguientes:

1. Los responsables de cada uno de los servicios serán responsables de categorizar la información y servicios de acuerdo con los niveles marcados por las guías ENS. Esta categorización proporcionará automáticamente la categoría del sistema de información.
2. El responsable de seguridad determinará la declaración de aplicabilidad teniendo en cuenta los mínimos requeridos en las medidas de seguridad dispuestas en el Anexo II del ENS y las medidas adicionales o compensatorias que se estimen oportunas.
3. El responsable de seguridad realizará el pertinente análisis de riesgos.
4. El administrador de seguridad se encargará de aplicar las medidas acordadas y monitorizará los sistemas pudiendo requerir auditorías internas o/y externas.
5. Los responsables de cada uno de los servicios deberán aceptar el riesgo residual y en su caso proponer medidas de mejora.

La gestión de riesgos está definida en el procedimiento de ADEIT PS-01 Análisis y Gestión de Riesgos.

17. Desarrollo de la política de seguridad de la información

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.

Otros documentos que complementan esta política de seguridad son:

- La normativa de seguridad del uso de sistemas de la información de ADEIT.
- Los procedimientos de seguridad de sistemas de la información de ADEIT.
- Los procesos de autorización de sistemas de la información de ADEIT.

La política de seguridad está disponible en la página web de ADEIT.

18. Obligaciones del personal de ADEIT

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

Todos los miembros de ADEIT atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años y además se establecerá un programa de concienciación continua para atender a todos los miembros de ADEIT, en particular a los de nueva incorporación mediante información digital como folletos, mensajes, tutoriales o newsletter.

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.

19. Terceras partes

Cuando ADEIT 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 ADEIT 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 de seguridad, 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.

Los proveedores que contrate ADEIT deben cumplir con el ENS, o demostrar que tienen medidas de seguridad equivalentes en los servicios que entreguen a ADEIT.

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.

20. Autorización y control de accesos

La autorización y control de accesos debe realizarse cómo se detalla en el procedimiento Control de accesos.

21. Adquisición de Productos

Se realiza según el procedimiento PS03 de Contratación de servicios TIC dependiendo del tipo de producto adquirido.

Primará, más allá de que cumpla con los requisitos, en los productos de seguridad que tenga un certificado de seguridad con el reconocimiento más amplio posible (europeo, internacional, etc.)

Se evitará productos de código abierto, software libre o de una fuente desconocida.

Se complementan estas directrices con el documento de ADEIT - Procesos de autorización de sistemas de la información.

22. Protección de las instalaciones

Las instalaciones están física y lógicamente protegidas, no se permiten personas ajenas a ADEIT que no estén autorizadas, y cámaras en las entradas y salida. Y las zonas no accesibles están cerradas o con acceso controlado por el personal de la propia Fundación según se indica en el procedimiento PS113 para el Control de accesos a las instalaciones de la Fundación.

23. Integridad y actualización del sistema

El sistema SGSI está en continua actualización de sus activos, los responsables de Seguridad y de Sistemas deben estar actualizando los procesos y las medidas y controles, así como otros productos de trabajo de la seguridad (Responsable de Seguridad) así como los sistemas (Responsable de Sistemas), de tal forma que se garantice su integridad

24. Seguridad por Defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto, según el ENS (lo que aplica para ADEIT):

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se realizará limpieza o se inhabilitaran de funcionalidades que no se utilicen para tal efecto. Se darán los permisos y accesos necesarios para las funciones requeridas por las personas.

Todo sistema debe cumplir con estas directrices.

25. Protección de la información almacenada y en tránsito

Toda información almacenada y en tránsito deberá estar según su clasificación y su categoría de la forma más segura posible (encriptada).

No se autoriza que aquella información clasificada como restringida o confidencial (uso Oficial) sea reproducida, copiada, transferida de ninguna forma sin la autorización adecuada. El resto de información se considera no clasificada o de uso Público

Más información en los procedimientos internos relativos al Art22-Protección de la información almacenada y en tránsito.

26. Prevención ante otros sistemas de información interconectados

Existen sistemas de información interconectados externos, esencialmente los de la Universitat de València y otros con otras universidades, se deberá garantizar la seguridad de estos, de la conexión y si es posible exigir que cumplan con la seguridad al menos al mismo nivel que ADEIT.

Entre los sistemas de ADEIT, antes de interconectar un sistema nuevo con los existentes se deberá probar en modo pre-explotación con simulacros antes de conectar estos.

27. Monitorización de la seguridad, registro de actividad y detención del código dañino

La monitorización del SGSI se basa en el procedimiento de ADEIT - PS10 Monitorización de Seguridad..

Se tendrá un registro de todas las actividades de todos los usuarios, se les informará de su última sesión, se les bloqueará si hay inactividad el terminal, si pasa más tiempo se les cerrará la sesión.

28. Mínima funcionalidad

Se darán a las personas acceso y recursos que representen lo mínimo que se requiere para poder realizar el trabajo (ver 24.b)

Se verificará que los equipos que se entreguen a los usuarios tengan sólo acceso y sólo instalado lo que necesitan para realizar su trabajo.

29. Continuidad

Se realizará en todo momento una valoración del impacto (BIA), para saber los RTO (tiempo de máximo de interrupción) y RPO (tiempo desde la última copia de seguridad) de los servicios que la organización ofrece. La Fundación dispone de un procedimiento específico, PS06 Plan de Continuidad

30. Mejora continua

El Comité de Seguridad TIC de la Fundación tiene establecido un plan de mejoras que se va validando en sus reuniones periódicas para las posibles mejoras de la seguridad y de nuestro SGSI.

En el seguimiento de todas las actualizaciones y mejoras que se van llevando a cabo se utiliza la metodología PDCA y realizan a través de la aplicación compartida https://alfresco.adeituv.es

31. Gestión de Incidentes

Se usará el procedimiento de ADEIT - PS05 de Gestión de Incidencias. En este sentido los incidentes son identificados y gestionan hasta su cierre.

32. Glosario y acrónimos

SGSI Sistema de Gestión de Seguridad de la Información

ENS Esquema Nacional de Seguridad

RAT Registro de Actividades de Tratamiento de datos

BIA Análisis de Impacto en el Negocio

RTO **(Recovery Time Objective)** Tiempo máximo de Interrupción del sistema / servicio

RPO **(Recovery Point Objective)** Tiempo transcurrido desde la última copia de seguridad