POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundació General de la Universitat de València

VNIVERSITAT DE VALÈNCIA
Fundació General

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 14 de septiembre de 2020 por la Vicepresidencia Ejecutiva de la FUNDACIÓ GENERAL DE LA UNIVERSITAT DE VALÈNCIA. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

La Fundació General de la Universitat de València (FGUV) 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 los departamentos deben 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, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La organización 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 organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

2.1. Prevención

La organización 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 roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la organización debe:

- Tener autorizado 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, se deben monitorizar las operaciones 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 organización debe:

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

2.4. Recuperación

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

3. ALCANCE

Esta política se aplica a todos los sistemas TIC y a todos los miembros de la organización.

4. MISIÓN

La FGUV, de conformidad con lo dispuesto en el artículo 7 de sus *Estatutos*, *tiene la misión fundamental de cooperar en el cumplimiento de los fines de la Universitat de València*. Ésta es una tarea que realiza mediante el encargo de gestión efectuado por la Universitat de València, que desarrolla a través de tres grandes áreas de actuación (Cultura y formación, Servicios Universitarios y Solidaridad) y de sus servicios generales.

La experiencia y conocimiento del entorno sociocultural, formativo y docente, así como del ámbito de la cooperación universitaria al desarrollo, proporcionan a la FGUV las herramientas necesarias para configurarse como un puente, entre la Universitat de València y la sociedad, de transferencia, divulgación, difusión, democratización cultural, formación y solidaridad.

5. NORMATIVA

La principal normativa aplicable a la FGUV es la siguiente:

- LEY 8/1998, de 9 de diciembre, de la Generalitat Valenciana, de Fundaciones de la Comunidad Valenciana
- DECRETO 68/2011, de 27 de mayo, del Consell, por el que se aprueba el Reglamento de Fundaciones de la Comunitat Valenciana
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- 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 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Ley 53/1984, de 26 de diciembre, de incompatibilidades del personal al servicio de las Administraciones Públicas.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comité

La Seguridad de la Información y de TIC (STIC) estará coordinada por el **Comité de Seguridad** y estará formado por:

- Cristóbal Suria en su condición de Gerente
- Rafael Cebrià en su condición de Responsable del departamento de administración
- Elena Vila en su condición de Responsable del departamento jurídico
- Paula Iranzo en su condición de técnica del departamento jurídico
- Salvador Garcia en su condición de técnico del departamento de informática
- Javier Plaza en su condición de Delegado de Protección de datos de la Universitat de València y sus fundaciones dependientes o persona en quien delegue

El **Responsable de Seguridad** actúa como **Secretario del Comité de Seguridad.** Como tal, tendrá las siguientes funciones:

- Convoca las reuniones del Comité de Seguridad.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Es el responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad reportará a la Vicepresidencia Ejecutiva

Deberá obtener regularmente el asesoramiento técnico o externo pertinente para la toma de decisiones y se asesorará en los temas sobre los cuáles haya de decidir o emitir una opinión.

6.2. Roles: Funciones y responsabilidades

1. **RESPONSABLE DE LA INFORMACIÓN**

El rol de **Responsable de la Información**, debido a la naturaleza, tamaño y recursos disponibles de la organización recae en el Comité de Seguridad. Si procediera, se detallará el nombramiento de **Responsables Delegados de Seguridad** y las funciones que les son delegadas.

Funciones del Responsable de la Información:

a. Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.

2. **RESPONSABLE DEL SERVICIO**

El **Comité de Seguridad** asume el rol de **Responsable del Servicio** y se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, destacándose los aspectos de seguridad física (seguridad de las instalaciones), seguridad de la información, Compliance (seguridad y conformidad legal) y planes de contingencia.

Funciones del Responsable del Servicio:

a. Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
b. Coordina todas las funciones de seguridad de la Organización.
c. Vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
d. Vela por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
e. Aprobación de las políticas de seguridad.
f. Aprobación previa de la implementación de las medidas técnicas del sistema.

3. RESPONSABLE DE LA SEGURIDAD

El **responsable de la Seguridad (del ENS)** que recae en Salvador Garcia Pertegaz, es la persona designada por la dirección de la organización, según el procedimiento establecido en este documento en el apartado procedimientos de designación.

Funciones del Responsable de Seguridad:

Debe planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho adecuadamente.

Las funciones esenciales del Responsable de la Seguridad son:

a. Determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y del servicio.
b. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información.
c. Promover la formación y concienciación en materia de seguridad de la información.
d. Actuar como Secretario del Comité de Seguridad.

4. RESPONSABLE DEL SISTEMA

El **Responsable del Sistema** que recae en Alfonso Chiner Fernández**,** se encarga de la parte operativa del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad

Funciones del Responsable del Sistema:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.

b. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

6.3. Procedimientos de designación

El cumplimiento de las responsabilidades y funciones definidas en esta política de seguridad se determina por la definición de diferentes roles que se han vinculado a ellas. Será competencia de la Vicepresidencia Ejecutiva designar la persona, comité o entidad que adoptará un rol determinado, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

6.4. Política de Seguridad de la Información

Será misión del Comité de Seguridad 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 la Vicepresidencia Ejecutiva, y difundida por Gerencia para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

La FGUV trata datos de carácter personal. El documento de seguridad al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de la FGUV 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.

8. GESTIÓN DE RIESGOS

La organización deberá realizar un análisis de riesgos de todos los sistemas, 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 establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad en diferentes materias:

- Normas de uso personal de los recursos informáticos y telemáticos de la Universitat de València
- Análisis de riesgos realizados
- Evaluaciones de impacto
- Normativa 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 organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible en la intranet.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de la FGUV 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.

Todos los miembros de la FGUV asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la FGUV, 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.

11. TERCERAS PARTES

Cuando la FGUV 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la FGUV 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 atañe 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.

ANTONIO| ARIÑO| VILLARROYA

Firmado digitalmente por ANTONIO|ARIÑO| VILLARROYA
Fecha: 2020.09.16 12:58:51 +02'00'