Política de seguridad de la información de la Fundación UVa

G _20_TIC_2026 Política de seguridad de la información

Versión 1	Redacción	Aprobación
Julio 2026	Director área TIC	Gerente

1.- Introducción

Este documento expone la Política de Seguridad de la Información de la FUNDACIÓN UNIVERSIDAD DE VALLADOLID M.P (en adelante, "Fundación"), como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco del Esquema Nacional de Seguridad (ENS).

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la Fundación. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

Esta Política constituye el documento de primer nivel del Sistema de Gestión de Seguridad de la Información (SGSI) de la Fundación. Recoge los principios, directrices y responsabilidades de carácter general, remitiéndose, allí donde procede, a las políticas específicas y procedimientos que desarrollan cada materia.

2.- Definiciones

- Sistema de Información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- SGSI: Sistema de Gestión de Seguridad de la Información que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información.
- Disponibilidad: es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- Integridad: la información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- Confidencialidad: la información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- Autenticidad: se debe asegurar la identidad u origen de la información.
- Trazabilidad: se debe asegurar para ciertos datos quién hizo qué y en qué

momento.

3.- Propósito

El propósito de esta Política de Seguridad de la Información es proteger los activos de información de la Fundación, asegurando la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, de acuerdo con los requerimientos del negocio y la legislación vigente.

Como documento marco del SGSI, esta Política establece principios y directrices generales y remite el desarrollo operativo, allí donde existe, a las políticas específicas y procedimientos correspondientes.

4.-Alcance

La presente Política se aplica a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la Fundación para los procesos descritos.

El personal sujeto a esta política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre y de si el usuario es empleado o no de la Fundación. Por lo tanto, también se aplica a cualquier tercera parte que tenga acceso a la información o los sistemas de la Fundación.

5.-Fundamentos de esta Política

En materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

- Seguridad como proceso integral

La seguridad debe entenderse como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. Se promoverá la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos para que ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

- Gestión de la seguridad basada en los riesgos

El análisis de los riesgos es parte esencial y continua del proceso de seguridad. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, con dichos riesgos a niveles aceptables, y se realizará mediante la aplicación de medidas de seguridad proporcionadas a la naturaleza de la información tratada y de los servicios a prestar.

- Prevención, detección, respuesta y conservación

La seguridad del sistema contempla medidas de prevención, detección y respuesta ante incidentes de seguridad, así como de conservación de la información y servicios en caso de que el incidente se produzca.

- Existencia de líneas de defensa

La Fundación implementa una estrategia de protección basada en múltiples capas (organizativas, físicas y lógicas), de modo que cuando una capa falle el sistema permita ganar tiempo para reaccionar, reducir la probabilidad de compromiso global y minimizar el impacto final.

- Vigilancia continua y reevaluación periódica

La vigilancia continua permite la detección de actividades o comportamientos anómalos y su oportuna respuesta. Las medidas de seguridad se evalúan y actualizan periódicamente, adecuándolas a la evolución de los riesgos.

- Diferenciación de responsabilidades

La Fundación organiza su seguridad mediante la designación de roles con responsabilidades claramente diferenciadas (Responsable de la Información, Responsable del Servicio, Responsable del Sistema, Responsable de Seguridad), recogidos en el apartado "Roles, Responsabilidades y Deberes".

6.- Requisitos de Seguridad

Esta Política establece los siguientes requisitos de carácter general:

- Organización del proceso de seguridad
- Análisis y gestión de los riesgos
- Gestión de personal, profesionalidad y formación
- Autorización y control de los accesos
- Adquisición de productos y contratación de servicios de seguridad
- Mínimo privilegio y seguridad desde el diseño
- Integridad y actualización del sistema
- Protección de la información almacenada y en tránsito
- Prevención ante sistemas de información interconectados
- Registro de actividad y detección de código dañino
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad
- Requisitos Legales y marco normativo

7.- Roles, Responsabilidades y Deberes

- Usuarios: Se define como usuario a cualquier individuo o sistema que accede a la información propiedad de la Fundación o gestionada por ella. Cada usuario responde por su conducta y por cualquier acción ejecutada bajo sus credenciales.

- Dirección: La Dirección está comprometida con esta Política y es consciente del valor de la información y del impacto que un incidente de seguridad puede producir. La Fundación es propietaria de los activos de información propios y la Dirección es responsable de los riesgos.

- Responsable de Seguridad: El Responsable de Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y los servicios, y supervisa la implantación de las medidas necesarias.

- Delegado de Protección de Datos: Conforme al RGPD y la LOPDGDD, el Delegado de Protección de Datos informa y asesora al Comité de Seguridad en materia de protección de datos y ofrece el asesoramiento jurídico solicitado en relación con dicha materia.

- Responsable del Sistema: El Responsable del Sistema desarrolla la forma concreta de implementar la seguridad en el sistema y supervisa la operación diaria, siguiendo las directrices del Responsable de Seguridad. Conforme al ENS, no puede coincidir con el Responsable de Seguridad.

- Comité de Seguridad de la Información: Compuesto por el Responsable de Seguridad, el Responsable del Sistema y la Dirección, se reúne al menos semestralmente para coordinar la seguridad de la información.

8.- Datos de carácter personal

La organización tratará los datos de carácter personal de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), garantizando en todo momento el respeto a los principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad.

En particular, únicamente se recogerán y tratarán datos personales cuando resulten adecuados, pertinentes y limitados a lo necesario en relación con las finalidades para las que sean tratados, debiendo estar dichas finalidades debidamente determinadas, explícitas y legitimadas conforme a alguna de las bases jurídicas previstas en la normativa aplicable.

Asimismo, la organización adoptará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas interesadas.

En este sentido, la organización integrará en sus procesos de gestión de la seguridad de la información las obligaciones derivadas de la normativa de protección de datos, incluyendo, entre otras, la identificación de la base legitimadora de los tratamientos, la realización de análisis de riesgos, la evaluación de impacto en protección de datos cuando proceda, y el mantenimiento del correspondiente registro de actividades de tratamiento.

- *Terceras Partes:*

Cuando la Fundación preste servicios a otros organismos o maneje información de terceros, se les hará partícipe de esta Política. La Fundación define y aprueba los canales para la coordinación, los procedimientos de actuación ante incidentes y el resto de actuaciones en materia de seguridad con otros organismos.

Cuando la Fundación utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política y de la normativa de seguridad aplicable. La tercera parte quedará sujeta a las obligaciones establecidas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias y se garantizará que el personal de terceros esté adecuadamente concienciado.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos 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.

- *Desarrollo del SGSI, Revisión y Auditorías:*

Esta Política y las normas de seguridad derivadas se adaptarán a la evolución de los sistemas, la tecnología, los cambios organizativos y la legislación vigente, alineadas con los estándares y mejores prácticas del ENS y prestando especial atención a las guías publicadas por el Centro Criptológico Nacional.

El Responsable de Seguridad revisará esta Política anualmente o cuando haya cambios significativos, sometiéndola de nuevo a aprobación por la Dirección. Las revisiones evaluarán la efectividad de la Política y los efectos de los cambios tecnológicos y de negocio. La Dirección será responsable de aprobar las modificaciones cuando se produzca un cambio que afecte a las situaciones de riesgo recogidas en este documento.

El SGSI se auditará al menos cada dos años en auditoría interna, conforme a un plan de auditorías desarrollado por el Responsable de Seguridad, que recogerá el alcance, los criterios, el equipo auditor, el calendario y los recursos necesarios. Las auditorías comprobarán el cumplimiento de esta Política, normativa y procedimientos derivados, así como la efectividad de los controles implantados. Los hallazgos darán lugar a acciones correctivas con responsable y plazo, cuyo seguimiento se tratará en el Comité de Seguridad.

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Francisco Javier Zaloña Saldaña - Gerente Fundación Uva	Firmado	07/07/2026 18:08:00	
URL de verificación	https://sede.uva.es/validador-documentos?code=vssmUEC1QId0y9HICXieqw%3D%3D			