

Política de Seguridad de la Información y de la Privacidad de los datos de carácter personal tratados



Control de versiones

Versión	Fecha	Autor	Revisor	Cambios
3.0	Septiembre 2024	Equipo Técnico Comité de Seguridad y Privacidad	Dirección Servicios Jurídicos	Revisión del representante legal

Aprobaciones

Órgano de gobierno	Entidad	Fecha	Firma
Dirección General	Fundació Esade	Septiembre 2023	Aprobado por Comité Ejecutivo

Índice

1.	Objeto del documento	P. 04
2.	Alcance	P. 04
3.	Marco normativo	P. 04
4.	Definiciones	P. 04
5.	Política de seguridad y privacidad de la información	P. 05
5.1	Objetivos de la política	P. 05
5.2	Alcance de la política	P. 06
5.3	Roles y responsabilidades.....	P. 06
5.4	Gestión del riesgo	P. 06
5.5	Formación y concienciación	P. 06
5.6	Auditoria	P. 07
5.7	Sanciones	P. 07
5.8	Validez y actualización	P. 07
5.9	Ratificación	P. 07

1. Objeto del documento

Este documento tiene por objeto facilitar las directivas y directrices que deben seguirse para proteger la información y la privacidad de los datos de carácter personal que gestiona Fundación Esade respecto a posibles incidentes y una amplia gama de amenazas de seguridad y privacidad, a fin de:

- Garantizar la seguridad de las operaciones realizadas, mediante sus Sistemas de Información.
- Minimizar los riesgos de daño a la información y su posible implicación con los datos de carácter personal.
- Asegurar el cumplimiento de los objetivos de la Organización.
- Asegurar el cumplimiento de la legislación vigente.

Fundación Esade tiene la voluntad de conseguir que los principios de Política de Seguridad y Privacidad de los datos de carácter personal tratados formen parte de la cultura de la Organización, para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información y la Privacidad en base a un estándar reconocido internacionalmente ISO27001 y su extensión para la gestión de la Privacidad ISO27701 (en adelante SIG).

2. Alcance

Todo el personal de Fundación Esade, incluyendo colaboradores, proveedores y la dirección, debe conocer y cumplir esta política.

Esta Política se desarrollará mediante normativa, procedimientos, instrucciones operativas, guías, manuales y todos aquellos instrumentos organizativos considerados útiles para alcanzar sus objetivos.

3. Marco normativo

Mediante esta política se da cobertura a los requisitos exigidos por la Norma ISO 27001 e ISO 27701, en su apartado N05.1

4. Definiciones

A los efectos de una correcta interpretación de la presente Política, se incluyen las siguientes definiciones:

- **Información:** Datos que poseen significado, en cualquier formato o soporte. Se refiere a toda comunicación o representación de conocimiento.
- **Datos de carácter personal:** Información que identifica o hace identificable a una persona.
- **Sistema de Información:** Se refiere a un conjunto de recursos relacionados y organizados para el tratamiento de información, según determinados procedimientos, tanto informáticos como manuales.

5. Política de seguridad y de la privacidad de los datos de carácter personal tratados

5.1 Objetivos de la política

El objetivo principal de la creación de esta Política de Seguridad y Privacidad de los datos de carácter personal tratados, por parte de la Dirección de Fundación Esade, es garantizar a los usuarios de sus servicios el acceso y tratamiento de la información de forma segura y respetando la privacidad con relación a los servicios que se requieren para el desempeño acordado entre las partes, así como evitar serias pérdidas o alteración de la información y accesos no autorizados a la misma;

- Que se desarrollen políticas, normativas, procedimientos y guías operativas para apoyar la Política de Seguridad y Privacidad de los datos de carácter personal tratados.
- Que se identifique la información que deba ser protegida.
- Que se establezca y mantenga la gestión del riesgo alineada con los requerimientos de la política del SIG y la estrategia de Fundación Esade
- Que se establezca una metodología para la apreciación y tratamiento del riesgo.
- Que se establezcan criterios con los que medir el nivel de cumplimiento del SIG.
- Que se revise el nivel de cumplimiento del SIG.
- Que se corrijan las no conformidades mediante la implementación de acciones correctivas.
- Que el personal reciba formación y concienciación sobre la seguridad y privacidad de la información.
- Que todo el personal sea informado sobre la obligación de cumplimiento de la Política de Seguridad y Privacidad de los datos de carácter personal tratados.
- La asignación de los recursos necesarios para gestionar el SIG.
- La identificación y cumplimiento de todos los requerimientos legales, regulatorios y contractuales.
- Que se identifiquen y analicen las implicaciones de seguridad de la información y de la privacidad de los datos de carácter personal respecto a los requerimientos de negocio.
- Que se mida el grado de madurez del propio sistema de gestión de la seguridad de la información y de la privacidad.
- Que se realice la mejora continua sobre el SIG.

Se establece un marco para la consecución de los objetivos de seguridad y privacidad de la información de Fundación Esade. Dichos objetivos se alcanzarán a través de una serie de medidas organizativas y de normas concretas y claramente definidas.

Los principios que deben respetarse, en base a las dimensiones básicas de la seguridad y privacidad, son los siguientes:

- Confidencialidad: propiedad por la cual únicamente puede acceder a la información gestionada por Fundación Esade quién esté autorizado para ello, previa identificación, en el momento y por los medios habilitados.
- Integridad: propiedad que garantiza la validez, exactitud y completitud de la información gestionada por Fundación Esade, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación y permitiendo que sea modificada únicamente por quién esté autorizado para ello.
- Disponibilidad: propiedad de ser accesible y utilizable en los intervalos acordados. La información gestionada por Fundación Esade es accesible y utilizable por los clientes y usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- Privacidad: proteger la privacidad de la información personal de los estudiantes, profesores y personal administrativo que gestiona Fundación Esade así como colaboradores externos, asegurando que se cumplan las leyes y regulaciones aplicables en todo momento.

- Legalidad vigente: Cumplir con la legislación vigente

La dirección de Fundación Esade se compromete a poner todos los recursos necesarios para abordar con éxito la consecución de dichos objetivos. Así como llevar a cabo de forma periódica, la revisión y seguimiento de estos.

5.2 Alcance de la política

El alcance de la Política de Seguridad y de la Privacidad de los datos de carácter personal tratados, coincide con el alcance del SIG:

“Sistemas de Información y privacidad relacionados con los servicios TI que dan cobertura a los procesos de formación, investigación y de debate social de Fundación Esade según la última declaración de aplicabilidad”.

Esta ha sido aprobada por la Dirección General y se ha comunicado dentro de la organización y está disponible para las partes interesadas en la Web corporativa.

5.3 Roles y responsabilidades

Fundación Esade ha definido los roles y responsabilidades de las personas involucradas en la gestión de la seguridad y privacidad de la información personal en la universidad, desde la alta dirección hasta el personal de apoyo:

- La Dirección General de Fundación Esade es la responsable de aprobar la presente política.
- El CSO es el responsable de mantener la presente política.

5.4 Gestión del riesgo

El Sistema de Gestión de la Seguridad y Privacidad de la Información (SIG) en Fundación Esade, se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente pueden afectar a la seguridad y privacidad de la información de los servicios prestados, consistente en:

- Identificar las amenazas, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad y privacidad de la información.
- Analizar el riesgo, en base a la consecuencia de materializarse la amenaza y de la probabilidad de ocurrencia.
- Evaluar el riesgo, según un nivel previamente establecido y aprobado de riesgo ampliamente aceptable, tolerable e inaceptable.
- Tratar el riesgo inaceptable, mediante los controles o salvaguardas adecuadas.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

5.5 Formación y concienciación

Desde Fundación Esade y con el fin de apoyar las partes interesadas y acompañarlas en su crecimiento personal para mejorar la Seguridad y Privacidad se dispone de un plan de formación en Seguridad y Privacidad, así como de píldoras de concienciación.

5.6 Auditoría

La Dirección General de Fundación Esade garantiza y verifica, mediante auditorías internas y externas, el grado de cumplimiento de las directrices de esta Política y que éstas son operadas e implementadas correctamente, responsabilizándose del cumplimiento de las medidas correctivas que hayan podido determinarse con el fin de mantener la mejora continua.

5.7 Sanciones

El incumplimiento de esta Política de Seguridad y de la Privacidad de los datos de carácter personal tratados y demás normativas y procedimientos que la desarrollan tendrá como consecuencia la aplicación de sanciones, conforme a la magnitud y características del aspecto no cumplido, de acuerdo con la legislación laboral vigente.

5.8 Validez y actualización

Esta política es efectiva desde el momento de su publicación y se revisa como mínimo una vez al año.

El objetivo de las revisiones periódicas es adecuarla a los cambios en el contexto de la organización, con atención a las cuestiones externas e internas, analizándose las incidencias acaecidas de seguridad y privacidad de la información y las no conformidades encontradas en el SIG. Todo ello armonizado con los resultados de los diferentes procesos de apreciación del riesgo.

Al revisar la Política también se revisará todas las Normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios relevantes que pudieran acontecer a nivel organizacional, de nuevos servicios o de infraestructura.

Fundación Esade, dispone de una clasificación de la información y se protege según su importancia y sensibilidad.

El Comité de Seguridad y de Privacidad debe garantizar que todo el personal involucrado en el SIG conoce esta política, sus objetivos y procesos, a través de su divulgación, acciones formativas y acciones de concienciación.

También debe garantizar la distribución de los documentos que aplican a cada nivel, de acuerdo con los diferentes roles definidos en la compañía

5.9 Ratificación

Don Daniel Abel Monteiro Palhare Traça en representación de Fundación Esade acepta plenamente el contenido de esta Política y se compromete a aplicarla.

Do Good.
Do Better.

esade

www.esade.edu