# Política de seguretat de la informació i de privacitat de les dades de caràcter personal tractades

**Control de versions**

| Versió | Data | Autor | Revisió | Canvis produïts |
|---|---|---|---|---|
| 2.0 | Setembre 2023 | Equip Tècnic<br>Comitè de Seguretat i Privacitat | Direcció de Serveis Jurídics | Revisió de l'abast |

**Aprovacions**

| Òrgan de govern | Entitat | Data | Signatura |
|---|---|---|---|
| Direcció General | Fundació Esade | Setembre 2023 | Aprovat per Comitè Executiu |

# Índex

## 1.1 Objecte del document

Aquest document té per objecte facilitar les directives i les directrius que s'han de seguir per protegir la informació i la privacitat de les dades de caràcter personal que gestiona la Fundació Esade respecte a possibles incidents i a una gran varietat d'amenaces de seguretat i privacitat, a fi de:

→ Garantir la seguretat de les operacions realitzades a través dels seus sistemes d'informació.

→ Minimitzar els riscos de dany a la informació i la seva possible implicació amb les dades de caràcter personal.

→ Assegurar el compliment dels objectius de l'organització.

→ Assegurar el compliment de la legislació vigent.

La Fundació Esade té la voluntat d'aconseguir que els principis de la Política de seguretat i privacitat de la informació formin part de la cultura de l'organització. Per això, ha implementat un Sistema de Gestió de la seguretat de la Informació i la Privacitat basat en un estàndard reconegut internacionalment, la ISO27001, i la seva extensió per a la gestió de la privacitat, la ISO27701 (en endavant, SIG).

## 2. Abast

Tot el personal de la Fundació Esade, inclosos els col·laboradors, els proveïdors i la direcció, ha de conèixer i complir aquesta política.

Aquesta política es desenvoluparà per mitjà de normativa, procediments, instruccions operatives, guies, manuals i tots els instruments organitzatius que es considerin útils per tal d'assolir els seus objectius.

## 3. Marc normatiu

Mitjançant aquesta política, es dona cobertura als requisits exigits per les normes ISO 27001 i ISO 27701, a l'apartat N05.1

## 4. Definicions

Per tal d'interpretar correctament aquesta política, s'inclouen les definicions següents:

→ Informació: Dades que tenen significat, en qualsevol format o suport. Es refereix a tota comunicació o representació de coneixement.

→ Dades de caràcter personal: Informació que identifica una persona o la fa identificable.

→ Sistema d'informació: Es refereix a un conjunt de recursos relacionats i organitzats per al tractament de la informació, segons determinats procediments, tant informàtics com manuals.

# 5. Política de seguretat i privacitat de les dades de caràcter personal tractades

## 5.1 Objectius de la política

L'objectiu principal de l'elaboració d'aquesta Política de seguretat i privacitat de les dades de caràcter personal tractades per part de la Direcció de la Fundació Esade és garantir als usuaris dels seus serveis l'accés i el tractament de la informació de manera segura i respectant la privacitat amb relació als serveis que es requereixen per a l'acompliment acordat entre les parts, i evitar-ne pèrdues greus o l'alteració de la informació i accessos no autoritzats a aquesta:

- → Que es desenvolupin polítiques, normatives, procediments i guies operatives per donar suport a la Política de seguretat i privacitat de les dades de caràcter personal tractades
- → Que s'identifiqui la informació que hagi de ser protegida.
- → Que s'estableixi i es mantingui alineada la gestió del risc amb els requisits de la política del SIG i l'estratègia de la Fundació Esade.
- → Que s'estableixi una metodologia per a l'apreciació i el tractament del risc.
- → Que s'estableixin uns criteris amb els quals mesurar el nivell de compliment del SIG.
- → Que es revisi el nivell de compliment del SIG.
- → Que es corregeixin les no conformitats amb la implementació d'accions correctives.
- → Que el personal rebi formació i conscienciació sobre la seguretat i privacitat de la informació.
- → Que tot el personal sigui informat sobre l'obligació de compliment de la Política de seguretat i privacitat de la informació.
- → L'assignació dels recursos necessaris per gestionar el SIG.
- → La identificació i el compliment de tots els requisits legals, reguladors i contractuals.
- → Que s'identifiquin i s'analitzin les implicacions de seguretat de la informació i de la privacitat de les dades de caràcter personal respecte a les exigències del negoci.
- → Que es mesuri el grau de maduresa del propi sistema de gestió de la seguretat de la informació i de la privacitat.
- → Que es faci una millora contínua del SIG.

S'estableix un marc per a l'assoliment dels objectius de seguretat i privacitat de la informació de la Fundació Esade. Aquests objectius s'assoliran a través d'una sèrie de mesures organitzatives i de normes concretes i clarament definides.

Els principis que s'han de respectar, sobre la base de les dimensions bàsiques de seguretat i privacitat, són els següents:

- → Confidencialitat: Propietat en virtut de la qual només pot accedir a la informació gestionada per la Fundació Esade qui estigui autoritzat a fer-ho, amb identificació prèvia, en el moment i pels mitjans habilitats.
- → Integritat: Propietat que garanteix la validesa, l'exactitud i la completesa de la informació gestionada per la Fundació Esade, essent el seu contingut el que hagin facilitat els afectats, sense cap tipus de manipulació, informació que només podrà ser modificada per qui estigui autoritzat a fer-ho.
- → Disponibilitat: Propietat de ser accessible i utilitzable en els intervals acordats. La informació gestionada per la Fundació Esade és accessible i utilitzable pels clients i pels usuaris autoritzats i identificats en tot moment, i la seva pròpia persistència queda garantida davant de qualsevol eventualitat prevista.
- → Privacitat: Protegir la privacitat de la informació personal dels estudiants, del professorat i del personal administratiu que gestiona la Fundació Esade, així com dels col·laboradors externs, assegurant que es compleixin les lleis i les regulacions aplicables en tot moment.
- → Legalitat vigent: Complir amb la legislació vigent.

La direcció de la Fundació Esade es compromet a posar tots els recursos necessaris per abordar amb èxit l'assoliment d'aquests objectius i a fer-ne, de manera periòdica, la revisió i el seguiment.

## 5.2 Abast de la política

L'abast de la Política de seguretat i privacitat de la informació coincideix amb l'abast del SIG:

"Sistemes d'informació i privacitat relacionats amb els serveis TI que donen cobertura als processos de formació, de recerca i de debat social de la Fundació Esade, segons la darrera declaració d'aplicabilitat."

Aquest ha estat aprovat per la Direcció General i s'ha comunicat dins de l'organització i està a disposició de les parts interessades a la web corporativa.

## 5.3 Rols i responsabilitats

La Fundació Esade ha definit els rols i les responsabilitats de les persones implicades en la gestió de la seguretat i la privacitat de la informació personal a la universitat, des de l'alta direcció fins al personal de suport:

→ La Direcció General de la Fundació Esade és la responsable d'aprovar aquesta política.
→ El CSO és el responsable de mantenir aquesta política.

## 5.4 Gestió del risc

El Sistema Integrat de Gestió de la Seguretat i la Privacitat de la Informació (SIG) de la Fundació Esade s'articula mitjançant un procés general d'apreciació i tractament del risc, que potencialment pot afectar la seguretat i la privacitat de la informació dels serveis prestats, consistent a:

→ Identificar les amenaces, que aprofitaran vulnerabilitats dels sistemes d'informació que suporten o dels quals depèn la seguretat i la privacitat de la informació.
→ Analitzar el risc, sobre la base de la conseqüència de materialitzar-se l'amenaça i de la probabilitat d'ocurrència.
→ Avaluar el risc, segons un nivell de risc prèviament establert i aprovat, àmpliament acceptable, tolerable i inacceptable.
→ Tractar el risc inacceptable amb els controls o les salvaguardes adequats.

Aquest procés és cíclic i s'ha de fer de manera periòdica, com a mínim una vegada a l'any. Per a cada risc identificat, s'assignarà un propietari, i en una mateixa persona o comitè poden recaure múltiples responsabilitats.

## 5.5 Formació i conscienciació

A fi de donar suport a les parts interessades i acompanyar-les en el seu creixement personal amb vista a millorar la seguretat i la privacitat, la Fundació Esade disposa d'un pla de formació en seguretat i privacitat, i de píndoles de conscienciació.

## 5.6 Auditoria

La Direcció General de la Fundació Esade garanteix i verifica, amb auditories internes i externes, el grau de compliment de les directrius d'aquesta política i que aquestes siguin operades i implementades correctament, i es responsabilitza de complir les mesures correctives que s'hagin pogut determinar a fi de mantenir-ne la millora contínua.

## 5.7 Sancions

L'incompliment d'aquesta Política de seguretat i privacitat de la informació i d'altres normatives i procediments que la desenvolupen tindrà com a conseqüència l'aplicació de sancions, segons la magnitud i les característiques de l'aspecte no complert, d'acord amb la legislació laboral vigent.

## 5.8 Validesa i actualització

Aquesta política és efectiva des del moment de la seva publicació i es revisa, com a mínim una vegada a l'any.

L'objectiu de les revisions periòdiques és adequar-la als canvis en el context de l'organització, fent atenció a les qüestions externes i internes, analitzant les incidències esdevingudes en matèria de seguretat i privacitat de la informació i les no conformitats trobades en el SIG, tot això harmonitzat amb els resultats dels diferents processos d'apreciació del risc.

En revisar la política, també es revisaran totes les normes i altres documents que la desenvolupen, seguint un procés d'actualització periòdica que estarà subjecte als canvis rellevants que es puguin produir a l'organització, de nous serveis o d'infraestructures.

La Fundació Esade disposa d'una classificació de la informació i la protegeix segons la seva importància i sensibilitat. El Comitè de Seguretat i de Privacitat ha de garantir que tot el personal involucrat en el SIG coneix aquesta política, els seus objectius i processos, fent-ne divulgació, accions formatives i accions de conscienciació.

També ha de garantir la distribució dels documents que són d'aplicació a cada nivell, d'acord amb els diferents rols definits a l'empresa.

## 5.9 Ratificació

Xavier Mendoza Mayordomo, en representació de la Fundació Esade, accepta plenament el contingut d'aquesta política i es compromet a aplicar-la.

Do Good.
Do Better.

esade

www.esade.edu