

Política de seguretat

Aprovat per: Responsable de seguretat

Data: 13/6/2025

Canvis sobre l'anterior versió: ([històric de canvis](#))

0. Introducció

Aquest document és la Política de Seguretat de la Informació i dels Serveis a IThinkUPC. Defineix els seus objectius i l'estructura que la formen. Aquesta política ha estat establerta per la Direcció i ha de ser seguida a nivell individual per cada treballador. Té en compte els requeriments legals existents, les necessitats de l'empresa, dels propietaris i dels clients.

Aquesta política ha estat **aprovada** per la **Direcció** d'IThinkUPC.

1. Objectius

La política de seguretat d'IThinkUPC té com a finalitat garantir la **confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat** de la **informació** i dels **serveis** que gestiona. Es fonamenta en un sistema de gestió basat en la **legalitat vigent** (veure l'[annex X](#)) per conèixer el detall de la legislació aplicable) i l'acompliment de la **norma [ISO 27001](#)** i de l'Esquema Nacional de Seguretat (**ENS**).

Per garantir la seguretat de la informació, a IThinkUPC s'adopten mesures de seguretat tècniques i mesures organitzatives proporcionals als riscos. Els objectius de la política de seguretat de la informació són:

1. Garantir la prestació dels serveis amb una protecció adequada d'acord amb els requisits i expectatives de les parts interessades.
2. Millorar l'eficiència dels processos relatius a la prestació dels serveis sense pèrdua dels nivells de seguretat exigits.
3. Complir la legislació vigent relativa a la seguretat i privacitat de la informació.

Aquests objectius es concreten en els següents aspectes:

- **Compliment normatiu**, ja que la política ha d'estar alineada amb la **legislació** aplicable i amb les **regulacions i obligacions contractuals** directament relacionades amb la seguretat i privacitat de la informació.
- **Protecció dels actius**, és a dir, tot allò que és important per a l'organització. Es crea un marc normatiu que determina com IThinkUPC protegeix els seus recursos.
- **Conscienciació** dels empleats d'IThinkUPC de la **importància** de la informació a la qual té accés, els **riscos de seguretat** que els poden afectar ,i sobre la manera de **minimitzar** les seves **conseqüències** o la **freqüència** en la que es presenten aquests incidents.
- Creació d'un **entorn** on aplicar **mesures i pràctiques de seguretat**. També ajuda a determinar la conducta que han de seguir les persones que treballen a IThinkUPC, mitjançant la definició de **funcions, responsabilitats i obligacions**.

2. Obligacions dels empleats

IThinkUPC proporciona recursos informàtics (estacions de treball, connexió a la xarxa de comunicacions, correu electrònic, repositori de fitxers i impressores, entre d'altres) als seus treballadors per al desenvolupament de la seva activitat laboral. Els **empleats es comprometen** a utilitzar de **manera correcta els recursos i actius informàtics**, i la **informació** d'IThinkUPC **exclusivament** per a **tasques** relacionades amb la **seva feina**, i **queda prohibit explícitament qualsevol ús comercial i/o privat no autoritzat**. A més, els **empleats** tenen l'**obligació** de **protegir** aquests recursos i la **informació** que poden allotjar contra l'**accés no autoritzat** mitjançant **mesures de prevenció i identificació ràpida d'incidències**, de **limitació de pèrdues** i de **restauració**. Per decidir el grau de protecció s'han d'aplicar els següents criteris:

- La classificació definida dels actius d'informació. (veure detall a l'[annex 3](#))
- L'acompliment de les disposicions legals sobre seguretat de la informació.
- L'acompliment de les obligacions contractuals sobre seguretat de la informació.

En el cas de **desenvolupadors d'aplicacions**, han d'assegurar que aquestes aplicacions inclouen els **controls necessaris per complir els objectius de seguretat de la informació** establerts per aquesta política de seguretat de la informació.

El **Departament de Recursos Humans** és l'encarregat de **divulgar** aquesta política entre el personal, i **conscienciar** als treballadors de la **importància** i de **les repercussions del seu incompliment**.

Al final d'aquest document s'inclou una relació d'annexos amb tota la informació que desenvolupa aquesta política.

3. Comunicació d'incidències

Tots els treballadors d'IThinkUPC, inclòs el **personal contractat d'empreses externes**, tenen l'**obligació** de **comunicar** qualsevol **irregularitat** o **incident** en el compliment de la política i procediments de **seguretat de la informació i serveis** de l'empresa, ja sigui en la seva pròpia operativa o en l'operativa que es realitza en altres àmbits.

La comunicació es realitzarà pels canals habituals d'**ATIC**, indicant **totes les dades necessàries** per a la correcta verificació i resolució de la incidència.

En el cas d'**incidències** que es consideri que necessiten un **tractament especial**, es poden utilitzar altres **canals més privats** (per exemple; presencialment, telefònicament o mitjançant correu electrònic al Responsable del Servei o Responsable de Seguretat). En aquests casos, les dades del denunciant es mantindran reservades i únicament seran utilitzades pel/s administrador/s de seguretat de la informació i/o RRHH en cas de requerir-se informació addicional per a la seva verificació.

4. Organització de la seguretat

A IThinkUPC s'estableixen diferents rols per vetllar per la seguretat de la informació, tant la pròpia com la custodiada.

4.1. Comitè de Seguretat de la informació

El Comitè de Seguretat de la informació és el responsable de **redactar** i **proposar** a la **Direcció** d'IThinkUPC les **polítiques** i **procediments** de seguretat de la informació, així com les seves posteriors modificacions.

4.2. Responsable de la Seguretat de la informació

El Responsable de la Seguretat de la informació és el responsable de totes les **activitats** relacionades amb la seguretat de la informació. Qualsevol delegació de responsabilitat en un altre haurà d'estar documentada i serà informada al Comitè de Seguretat de la informació. Entre les seves tasques destaca la **coordinació del coneixement sobre temes de seguretat de la informació** a l'empresa per assegurar que les accions que es duguin terme siguin coherents. També proporciona consells i ajuda a la presa de decisions a la resta del personal.

4.3. Fòrum de Seguretat de la informació

El Fòrum de Seguretat de la informació és el grup de persones de l'empresa que **assessora** a nivell tècnic al Comitè de Seguretat de la informació i al Responsable de Seguretat de la informació en totes les qüestions relatives a la seguretat de la informació.

4.4. Responsable del servei

És el **gestor** designat per IThinkUPC per **garantir la correcta prestació del servei** d'acord amb les necessitats dels clients i l'operativa definides. Coopera estretament amb el Responsable de Seguretat per vetllar per la correcta aplicació de la Política de Seguretat.

Les seves responsabilitats són:

- **Classificació de la informació** en els **nivells** preestablerts segons el grau de criticat de la seva confidencialitat, integritat i disponibilitat.
- **Definició de les mesures de protecció** que cal aplicar associades al servei.
- **Definició de les regles d'accés a les dades.**
- **Coordinació de les incidències de seguretat** tant amb els interlocutors definits com en el Responsable de Seguretat.
- El Responsable del Servei es responsable de la **gestió del risc** i el **manteniment de la informació** relativa a la gestió dels **riscos**.

El detall de cadascun d'aquests rols es pot consultar a l'[annex II](#).

5. Classificació dels actius d'informació

Són considerats **actius** de la **informació** tots aquells **components** o **funcionalitats** que, juntament amb els recursos informàtics, componen un **Sistema d'Informació**.

La seguretat de la informació està definida per cinc conceptes aplicats a la informació:

- **Confidencialitat:** protecció dels actius d'informació contra accessos o divulgació no autoritzats.
- **Integritat:** garantia de l'exactitud dels actius d'informació contra alteració, pèrdua o destrucció, ja sigui de forma accidental o fraudulenta.
- **Disponibilitat:** per assegurar que els recursos informàtics i els actius d'informació puguin ser utilitzats en la forma i temps requerits, i recuperats en cas de desastre.
- **Autenticitat:** capacitat de garantir que l'origen de la informació és el que es diu i no ha estat modificat des de la seva creació o transmissió.
- **Traçabilitat:** capacitat que permet identificar i seguir els moviments i canvis de la informació al llarg del temps.

Per mantenir una protecció adequada, aquests actius seran **inventariats** i **classificats**, i se'ls assignarà un Propietari i un Responsable del servei, que són les persones responsables en última instància del seu bon funcionament i de la seva seguretat de la informació.

Aquests criteris es detallen al document III dels procediments operatius enumerats al final d'aquest document: "[Classificació i control d'actius](#)".

6. Enumeració dels annexos de seguretat de la informació

La Política de Seguretat completa es troba al present document. Com a complement, es disposa d'un conjunt d'annexos que determinen i concreten els apartats de la política.

- Organització de la seguretat de la informació ([Document II](#))
- Classificació i control d'actius ([Document III](#))
- Seguretat de la informació vinculada al personal ([Document IV](#))
- Seguretat física de la informació ([Document V](#))
- Comunicacions i gestió de l'explotació ([Document VI](#))
- Control d'accés ([Document VII](#))
- Desenvolupament i manteniment ([Document VIII](#))
- Pla de Continuïtat ([Document IX](#))
- Conformitat ([Document X](#))

Aquests annexos es complementen amb altres documents, tecnologies, equips, programari, etc. i que focalitzen l'operativa de cada cas específic.