

# 1001 - Política de seguretat



Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain)

(+34) 973 282 300 · [info@lleida.net](mailto:info@lleida.net)

## Control Documental

Data	Versió	Modificacions	Autor
19/12/2014	1.0	Creació	Manel Cervera Díaz
04/01/2016	1.1	Revisió i Actualització	Manel Cervera Díaz
16/03/2016	1.2	Separació dels objectius del document	Manel Cervera Díaz
02/12/2016	1.3	Revisió i Actualització	Jordi Ramon
22/12/2017	1.4	Revisió	Jordi Ramon
23/07/2018	1.5	Actualització del llinar de risc acceptat i actualització de la confidencialitat	Jordi Ramon
09/11/2018	1.6	Alineació amb serveis de l'abast, actualització normativa afecta, substitució compromís d'obtenció per manteniment de l'SGSI	Eva Pané
20/12/2018	1.7	Previsió de la comunicació dels incidents de seguretat. Actualització del compliment normatiu de protecció de dades	Eva Pané
17/12/2019	1.8	Referència a la Política de Privadesa i al concepte de privadesa en el disseny en el desenvolupament d'aplicacions. Referència a l'aprovació d'aquesta política per part del Comitè de seguretat i la seva publicació a la web de Lleida.net	Eva Pané
29/05/2020	1.9	S'afegeixen referències específiques al control d'accés i a la seguretat física.	Eva Pané
22/02/2021	1.10	Actualitzada referència normativa de serveis de confiança	Eva Pané

## Llista de distribució

Departaments
Lleida.net

## Classificació i estatus del document

<b>Classificació del document</b>	Públic
-----------------------------------	--------

<b>Status del document</b>	Aprovat
----------------------------	---------

## Documents referenciats

Documents
3001 - Gestió del repositori de documents
1008 - Objectius de Lleida.net
2005 - Seguretat en el desenvolupament d'aplicacions
DP-1001 Política de Privadesa

# yy Lleida.net

## Índex

Control Documental .....	1
Llista de distribució.....	1
Classificació i estatus del document .....	1
Documents referenciats .....	1
1 Introducció.....	4
1.1 Objectiu .....	4
1.2 Àmbit d'aplicació .....	4
1.3 Distribució.....	4
1.4 Revisió.....	4
2 Política de seguretat de la informació .....	5
2.1 Responsabilitat.....	5
2.2 Seguretat de la informació .....	5
2.3 Actius d'informació .....	5
2.4 Objectius de Lleida.net.....	5
2.5 Directrius de la Política de Seguretat.....	6
2.6 Cos Normatiu de Seguretat de la Informació .....	6
2.7 Anàlisis i Gestió de Riscs .....	7
2.8 Risc residual acceptat .....	7
2.9 Violacions de la Política i procés disciplinari.....	7
2.10 Compliment legal i estatutari .....	7
2.11 Conscienciació i Formació en Seguretat de la Informació.....	8
2.12 Incidents de seguretat.....	8
2.13 Privadesa .....	8
3 Mapa de clàusules de la ISO 27001:2013 .....	9
4 Mapa de controls de la ISO 27002:2013 .....	9

## **1 Introducció**

### **1.1 Objectiu4**

La present política té com a objectiu establir el compromís de la Direcció de Lleida.net, representada pel seu Steering Committee, sobre la seguretat de la informació i la protecció d'actius d'informació necessaris per al desenvolupament de les funcions descrites a l'abast, permetent així, l'assoliment dels seus objectius.

Aquest compromís es materialitza mitjançant la implantació i el manteniment d'un Sistema de Gestió de la Seguretat de la Informació (SGSI) en conformitat amb l'estàndard internacional ISO/IEC 27001:2013.

### **1.2 Àmbit d'aplicació**

Tots els membres de Lleida.net, així com totes les terceres parts identificades a l'abast del Sistema de Gestió de la Seguretat de la Informació (SGSI).

### **1.3 Distribució 4**

Aprovada per l'Steering Committe de Lleida.net, aquesta Política ha de ser accessible a totes les persones incloses a la llista de distribució especificada al control documental, mitjançant els canals adequats, establertes al procediment 3001 - Gestió del repositori de documentació.

### **1.4 Revisió**

La present Política de Seguretat, serà revisada i aprovada anualment per part de l'Steering Committee de Lleida.net. Tanmateix, si hi hagués canvis rellevants per a l'Organització, ja siguin aquests de tipus operatiu, legal, regulador, o contractual, es procedirà a la seva revisió sempre que es consideri necessari, assegurant així que la Política roman adaptada en tot moment.

## 2 Política de seguretat de la informació

Lleida.net es compromet a protegir tots els actius sota la seva responsabilitat mitjançant les mesures que siguin necessàries, sempre garantint el compliment de les diferents normatives i lleis aplicables. Per aquest motiu un objectiu estratègic de negoci de Lleida.net és la certificació ISO 27001:2013 per a la gestió dels processos de notificació i contractació electrònica, solucions SMS i validació de dades.

Amb l'objectiu de complir amb la ISO 27001:2013 Lleida.net es compromet a:

Mantenir un Sistema de Gestió de la Seguretat de la Informació (SGSI) que inclou els processos, recursos, procediments, tecnologies i eines necessàries per a garantir la confidencialitat, integritat i disponibilitat dels actius d'informació i dels actius tecnològics que donen suport a Lleida.net. En especial als processos inclosos a l'abast.

### 2.1 Responsabilitat

El compliment de la present Política de Seguretat és responsabilitat de tot el personal de Lleida.net, així com del personal extern d'aquest, inclòs a l'abast del Sistema de Gestió de la Seguretat de la Informació. La Direcció de Lleida.net espera que tot el personal, tant intern com extern, estigui familiaritzat amb la present Política de Seguretat.

### 2.2 Seguretat de la informació

El terme "Seguretat de la Informació" es refereix a la protecció dels actius d'informació contra la revelació, modificació o destrucció no autoritzada, sigui ocasionada de forma accidental o intencionada. Els atributs de seguretat associats als actius d'informació són:

- **Confidencialitat:** Propietat per la qual la informació no es posa a disposició o es transmet a individus, entitats o processos no autoritzats.
- **Integritat:** Propietat de salvaguardar l'exactitud i completesa dels actius d'informació
- **Disponibilitat:** Propietat de ser accessible i utilitzable per a una entitat autoritzada

### 2.3 Actius d'informació

Els actius d'informació a les quals la present Política fa referència, inclouen qualsevol informació suportada en format físic (paper, contractes, targetes de visita, etc.) o correu electrònic (servidors, portàtils, telèfons mòbils, etc.) i que Lleida.net requereix per al desenvolupament de les seves funcions i de la consecució dels seus objectius estratègics i operatius.

### 2.4 Objectius de Lleida.net

La present Política pretén establir les directrius necessàries pel que fa a Seguretat de la Informació, les quals són considerades per la Direcció de Lleida.net com un requisit imprescindible per a la consecució dels objectius estratègics i operatius. Aquests poden consultar-se en el document 1008 - Objectius de Lleida.net.

## 2.5 Directrius de la Política de Seguretat

La Direcció de Lleida.net considera que la consecució dels objectius del grup es troba subjecta a l'acompliment de diversos requeriments encaminats a garantir la seguretat de la informació dins de l'Organització. D'aquesta manera, es considera que la Seguretat de la Informació ha de ser una prioritat per a l'organització i per a això, la present Política estableix les següents directrius:

- La informació de la qual Lleida.net és propietari i/o dipositari ha de ser únicament accessible per a les persones degudament autoritzades, pertanyin o no a l'Organització
- La present Política de Seguretat, així com la resta de cos Normatiu de l'SGSI (procediments, guies, etc.) haurà de ser accessible per a tots els membres de Lleida.net dins de l'abast de l'SGSI, així com el personal aliè a la mateixa que es relaciona amb aquest a través d'algun dels seus processos
- L'Organització ha de complir amb tots aquells requeriments legals, reguladors i estatutaris que li siguin d'aplicació, així com els requeriments contractuals
- La confidencialitat de la informació s'ha de garantir en tot moment
- La integritat de la informació ha d'assegurar a través de tots els processos que la gestionen, processen i emmagatzemen
- La disponibilitat de la informació s'ha de garantir mitjançant les adequades mesures de seguretat i continuïtat del negoci
- Tot el personal dins l'abast de l'SGSI de Lleida.net, haurà de disposar de l'adequada formació i conscienciació en matèria de Seguretat de la Informació
- Tot incident o debilitat que pugui comprometre o hagi compromès la confidencialitat, integritat i/o disponibilitat de la informació, ha de ser registrat i analitzat per aplicar les corresponents mesures correctives i/o preventives. Així mateix es comunicaran a les parts interessades en els terminis corresponents.
- Tot membre de Lleida.net dins de l'abast de l'SGSI, tan pertanyent a l'Steering Committee com al Grup Operatiu, és responsable d'implementar, mantenir i millorar la present Política, així com de vetllar pel compliment de la mateixa
- Tot membre de Lleida.net dins de l'abast de l'SGSI és responsable de garantir l'adequada implementació, manteniment i millora de l'SGSI, així com la seva conformitat amb l'estàndard ISO/IEC 27001: 2013

Els rols afectes a les directrius de la Política de Seguretat s'estableixen en el Reglament 2001 - Responsabilitats SGSI Lleida.net

## 2.6 Cos Normatiu de Seguretat de la Informació

Com a part d'aquesta política s'ha generat documentació que fa referència a Normatives i Procediments que apliquen als processos descrits a l'abast de l'SGSI. Aquesta documentació

serà distribuïda pels canals adequats d'acord amb la necessitat del coneixement, a totes les parts interessades.

## **2.7 Anàlisi i Gestió de Riscs**

La Seguretat de la Informació és controlada i monitorada per la Direcció de Lleida.net mitjançant el marc d'Anàlisi i Gestió de Riscos establert dins de l'SGSI. Aquest marc permet a la Direcció de Lleida.net avaluar el grau de control intern al voltant dels actius d'informació mitjançant l'ús d'una metodologia d'anàlisi de riscos que proveeixi de resultats objectius, mesurables i reproduïbles.

## **2.8 Risc residual acceptat**

La Direcció de Lleida.net, assumint que la mitigació completa de qualsevol risc no és assolible, estableix que el nivell de risc residual associat a qualsevol dels actius d'informació inclosos en l'abast de l'SGSI, no haurà de ser superior al nivell 6 (sobre una escala de 25). Per a la Direcció de Lleida.net, aquest nivell representa el llindar de risc residual el cost de mitigació del qual és més gran que la pèrdua incorreguda en cas de materialització d'aquest. En cas que el risc residual associat a qualsevol dels actius d'informació superi el nivell de risc acceptat, la Direcció de Lleida.net avaluarà les alternatives de mitigació d'aquest risc i proporcionarà els recursos necessaris per a situar-lo per sota del nivell de risc residual acceptat.

## **2.9 Violacions de la Política i procés disciplinari**

Qualsevol excepció a la present Política de Seguretat haurà de ser registrada i informada a la Direcció de Lleida.net. Així mateix, qualsevol violació de la mateixa pot resultar en l'aplicació de les accions disciplinàries corresponents d'acord amb la legislació aplicable.

És responsabilitat de tots els membres de Lleida.net notificar a la Direcció de qualsevol esdeveniment o situació que pogués suposar l'incompliment d'alguna de les directrius definides per la present Política.

## **2.10 Compliment legal i estatutari**

La present Política estableix la necessitat de complir amb tots aquells requeriments legislatius, normatius i contractuals que li siguin d'aplicació a Lleida.net i els actius d'informació gestionats. En aquest sentit, la Direcció de Lleida.net es compromet a dotar els recursos necessaris per a complir tota legislació i regulació aplicable a l'activitat de Lleida.net i estableix la responsabilitat de l'esmentat compliment sobre tots els seus membres.

En aquest sentit, es vetllarà pel compliment de tota legislació i regulació aplicable, la qual contempla principalment els següents aspectes:

- Legislació relacionada amb la protecció de dades de caràcter personal:
  - Reglament (UE) 2016/679 del Parlament Europeu i del Consell del 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46 / CE (GDPR)



- Llei Orgànica 3/2018, del 5 de desembre, protecció de dades personals i garantia dels drets digitals.
- Reial Decret 1720/2007, del 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, del 13 de desembre, de protecció de dades de caràcter personal
- Llei de Serveis de la Societat de la Informació (LSSI):
  - Llei 34/2002 de l'11 de juliol de serveis de la societat de la informació i comerç electrònic
- Legislació relacionada amb els serveis de confiança:
  - Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell del 23 de juliol de 2014 relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la qual es deroga la Directiva 1999/93 / CE
  - Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Legislació relacionada amb les telecomunicacions:
  - Llei 9/2014 del 9 de maig de Telecomunicacions

Així mateix, s'haurà d'assegurar el compliment de qualsevol altra legislació o normativa aplicable.

### **2.11 Conscienciació i Formació en Seguretat de la Informació**

Tots els membres de Lleida.net han de disposar de la formació adequada per al desenvolupament de les seves funcions. Així mateix, s'ha d'assegurar l'adequada conscienciació dels membres de Lleida.net en termes de Seguretat de la Informació i bones pràctiques.

Així mateix, els membres de Lleida.net han de disposar d'accés i coneixement de les actualitzacions regulars de la present Política i la resta del Cos Normatiu i Documental de l'SGSI.

### **2.12 Incidents de seguretat**

Un incident de seguretat consisteix en qualsevol esdeveniment que pogués comprometre la confidencialitat, integritat i/o disponibilitat de la informació, així com afectar la consecució dels objectius de Lleida.net.

La present Política estableix l'obligació i responsabilitat de tots els membres de Lleida.net, així com a terceres parts incloses en l'abast de l'SGSI, de la identificació i notificació als gestors de Lleida.net de qualsevol incident que pogués comprometre la seguretat dels actius d'informació de Lleida.net, així com de qualsevol situació que pogués suposar una no conformitat amb els procediments de l'SGSI i l'estàndard ISO / IEC 27001: 2013.

### **2.13 Privadesa 8**

El compromís amb la privacitat de les dades tractades que hagi de tractar Lleida.net es reflecteix en la Política de Privadesa (DP 1001- Política de Privacitat) disponible al públic a través del web corporatiu.

Així mateix, l'organització aplicarà el principi de privacitat en el desenvolupament d'aplicacions desenvolupat el 2005 - Seguretat en el desenvolupament i manteniment d'aplicacions.

### 2.14 Control d'accessos

Lleida.net pren mesures per garantir la seguretat de la informació mitjançant el control de l'accés lògic i físic a aquesta, els recursos de processament de la informació i els processos de negoci que han de ser controlats sobre la base dels requisits de negoci, mitjançant l'establiment de les directrius a seguir per a la gestió de l'accés als sistemes, així com els rols i responsabilitats dels usuaris i els controls definits.

### 2.15 Seguretat física

S'han de prendre mesures per a la gestió de la seguretat física a les diferents instal·lacions de Lleida.net, a través de l'establiment de protocols d'accés a les instal·lacions per als diferents rols que hagin d'accedir, amb distinció de les zones que siguin especialment securitzades i la definició dels usos acceptables en els llocs de treball

**La present Política de Seguretat ha estat aprovada pel Comitè de Seguretat de Lleida.net i entra en vigor el mateix dia de la publicació a la pàgina principal del web de Lleida.net.**

## 3 Mapa de clàusules de la ISO 27001:2013

Clàusules ISO 27001:2013
5.1 - Leadership and commitment
5.2 - Policy

## 4 Mapa de controls de la ISO 27002:2013

Control ISO 27002:2013
5.1.1 - Policies for information security
5.1.2 - Review of the policies for information security