

**Annex.**

**Requeriments de seguretat per proveïdors de serveis informàtics**



**Índex**

1. Objecte del document 3

2. Requeriments 3

ID 1. Política de Seguretat 3

ID 2. Certificació de ISO27001 3

ID 3. Procediment de revisió de la Política de Seguretat 3

ID 4. Evidència de la difusió de la Política de Seguretat 3

ID 10. Evidència de la difusió de la Normativa de Seguretat 3

ID 11. Procediments de Seguretat 3

ID 13. Evidència de la difusió dels Procediments de Seguretat o de la possibilitat d’accés per part dels usuaris. 4

ID 40. Document d'Identificació del Control d'Accés al sistema 4

ID 43. Procediment d'Autenticació del Sistema 4

ID 46. Document de Requeriments d'Accés al sistema 4

ID 50. Eina corporativa específica per a la gestió dels usuaris propis 4

ID 54. Procediment de Gestió de Drets d'Accés al Sistema 4

ID 62 Evidència de què l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions 5

ID 63. Acord de confidencialitat on es fa constar el lliurament de l'identificador 5

ID 64. Evidència de l'últim usuari propi donat de baixa 5

ID 67. Procediment d'Accés en Local 5

ID 107. Evidència què es disposa d'antivirus als sistemes d'informació 5

ID 111. Evidència de què el programa antivirus es troba actualitzat 6

ID 172. Evidències de la difusió del contingut del Pla de Conscienciació 6

ID 174. Evidències de la difusió del contingut del Pla de Formació 6

ID 241. Document on s'indica el mecanisme d'autenticació i identificació 6

ID 244. Procediment per a l'elaboració i execució del pla de proves de l'aplicació 6

ID 273. Procediment de configuració segura del correu. 6

ID 276. Evidència de l'eina monitoratge dels elements de seguretat 6

ID 330. Normativa documentada que especifica els deures i obligacions del personal contractat a través d'un tercer. 6

ID 460. Protocol d'actuació envers l'incompliment de les obligacions per part del personal tercer 7

# Objecte del document

El present document defineix els controls que hauria de fer front una empresa adjudicatària de serveis informàtics en cas d’auditoria de l’ENS de nivell BAIX.

# Requeriments

## ID 1. Política de Seguretat

Es disposa d'una Política de Seguretat que inclou:

1- Objectius de l'organització

2- Marc legal i regulador

3- Rols relacionats amb la seguretat, així com les seves responsabilitats i procediment de designació.

4- Estructura del comitè de gestió i coordinació de seguretat.

5- Criteri per a la classificació de la documentació.

6- Referència a la legislació aplicable en matèria de tractaments de dades de caràcter personal.

7- La Política de Seguretat ha de ser un document en paper o suport electrònic.

8- La Política de Seguretat inclou l'especificació del termini i condicions de la seva revisió i que ha d'estar aprovada per un òrgan superior.

9- La Política de Seguretat inclou un apartat específic de gestió dels usuaris i els seus privilegis, així com la persona responsable.

10- La Política de Seguretat inclou un apartat específic indicant els responsables de la informació gestionada pel sistema.

## ID 2. Certificació de ISO27001

Certificat vigent conforme l'organització està certificada en la ISO27001.

## ID 3. Procediment de revisió de la Política de Seguretat

Document contenint el Procediment de revisió i aprovació de la Política de Seguretat o en el seu defecte, apartat de la Política de Seguretat on s'especifiqui el període de revisió i aprovació.

## ID 4. Evidència de la difusió de la Política de Seguretat

Evidència de què la Política de Seguretat és accessible pel personal afectat a la Intranet, pàgina web, portal, repositori o ha estat distribuïda a tots els usuaris dels quals són responsables mitjançant del correu electrònic.

## ID 10. Evidència de la difusió de la Normativa de Seguretat

Evidència que la Normativa de Seguretat - ja sigui pròpia o s'empri el Marc Normatiu de l’Agència de Ciberseguretat de Catalunya - està disponible a la Intranet, pàgina web, portal, repositori, llibreria o a qualsevol altre mitjà accessible per a tots els usuaris implicats o bé que els ha estat distribuïda a través del correu electrònic.

## ID 11. Procediments de Seguretat

Es disposa de Procediments de Seguretat per a la realització de les tasques rutinàries.

Aquests han d'incloure com a mínim:

1- Com portar a terme les tasques habituals.

2- Qui ha de fer cada tasca.

3- Com identificar i reportar comportaments anòmals.

## ID 13. Evidència de la difusió dels Procediments de Seguretat o de la possibilitat d’accés per part dels usuaris.

Evidència de que els Procediments de Seguretat - siguin propis o s'emprin els del Marc Normatiu de l’Agència de Ciberseguretat de Catalunya - estan disponibles a la Intranet, pàgina web, portal, repositori, llibreria o a qualsevol altre mitjà accessible per a tots els usuaris implicats.

## ID 40. Document d'Identificació del Control d'Accés al sistema

Es disposa d'un procediment formalitzat de gestió d'usuaris degudament aprovat i actualitzat que s'indiqui:

- Com es realitza la gestió dels usuaris i dels seus privilegis així com la persona responsable de la gestió dels usuaris.

- Que els identificadors dels usuaris han de ser nominals i no es poden compartir.

- El període de retenció dels usuaris.

## ID 43. Procediment d'Autenticació del Sistema

Es disposa d'un procediment degudament aprovat i actualitzat on es descriuen els mecanismes d'autenticació dels usuaris o s'especifica dins del procediment formalitzat de gestió d'usuaris els següents punts:

1- Es detalla els sistemes d'autenticació dels usuaris amb l'obligació de tenir almenys un factor d'autenticació.

2- Es detalla i s'obté l'evidència de que l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions.

3- S'explica com gestionar les baixes d'usuaris i el lligam amb RRHH que permeti avisar als responsables de gestió d'usuaris del canvi en les relacions amb aquests.

4- S'indica que es facin servir almenys dos factors d'autenticació en els sistemes categoritzats com a nivell mig i alt.

5- En el cas que es facin servir tokens, que aquests utilitzen un algoritme autoritzat pel CCN, per exemple AES.

## ID 46. Document de Requeriments d'Accés al sistema

Es disposa d'un procediment formalitzat de gestió d'usuaris degudament aprovat i actualitzat que s'indiqui:

- Com es realitza la gestió dels usuaris i dels seus privilegis així com la persona responsable de la gestió dels usuaris.

- Que els identificadors dels usuaris han de ser nominals i no es poden compartir.

- El període de retenció dels usuaris.

## ID 50. Eina corporativa específica per a la gestió dels usuaris propis

Es disposa d'una eina corporativa específica per a la gestió dels usuaris.

## ID 54. Procediment de Gestió de Drets d'Accés al Sistema

Es disposa d'un procediment o s'inclou dins del procediment formalitzat d'usuaris del sistema els següents punts:

- S'assignarà el rol adequat a cada usuari amb els mínims privilegis possibles i revisant-se els mateixos periòdicament.

- S'inclourà la relació entre els permisos que ha de tenir cada usuari en funció del seu rol.

- S'especificarà quins son els responsables dels recursos dels sistemes (físics i lògics) i qui té la responsabilitat delegada de concedir, alterar o anul·lar l'accés als mateixos.

## ID 62 Evidència de què l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions

Es disposa de l'evidència que demostra que els nous usuaris confirmen la recepció de l'identificador, coneixen i accepten les obligacions. Aquesta evidència pot prendre diverses formes:

1- Evidència de que en crear el seu identificador s'informa l'usuari per correu electrònic, i en accedir per primer cop ha d'acceptar els drets i deures d'accés a l'aplicatiu.

2- Que el personal d'un proveïdor signi un document d'obligacions el primer dia, així com un acord de confidencialitat i queda constància del lliurament de l'identificador.

3- Que en la part inferior de la pantalla d'accés s'indiquin els termes i condicions, pel que els usuaris estan implícitament acceptant-les per accedir al sistema.

## ID 63. Acord de confidencialitat on es fa constar el lliurament de l'identificador

Es disposa del document contenint l'Acord de Confidencialitat signat per l'usuari fent constar la recepció del seu identificador. Ha d'existir un registre de cada usuari confirmant la recepció de l'identificador.

## ID 64. Evidència de l'últim usuari propi donat de baixa

Es disposa de l'evidència mostrant la baixa d'un usuari amb la data efectiva de la baixa.

## ID 67. Procediment d'Accés en Local

Es disposa d'un Procediment d'Accés en Local què especifiqui que:

1- Els sistemes abans d'entrar en explotació o els ja existents han estat configurats de forma que no revelin informació del sistema abans d'un accés autoritzat.

2- Els diàlegs d'accés (al lloc de treball, dins les pròpies instal·lacions de l'organització, al servidor, al domini de xarxa, etc.) no revelin informació sobre el sistema al qual s'està accedint.

3- Faci constar que s'ha d'informar sempre els usuaris de les seves obligacions un cop han accedit dins el sistema.

4- S'ha d'informar a l'usuari del seu darrer accés al sistema.

5- Defineixi uns horaris en què és possible la connexió al sistema i altres en què no ho és.

6- No es pot accedir al sistema fora de les hores autoritzades.

7- Indiqui punts de renovació d'autenticació durant la sessió d'un usuari.

## ID 107. Evidència què es disposa d'antivirus als sistemes d'informació

Es disposa de l'evidència de l'ús de mecanismes de prevenció davant de codi perjudicial (antivirus) per a tots els equips (Servidors i llocs de treball) del sistema i també en les maquetes, així com de la seva configuració.

## ID 111. Evidència de què el programa antivirus es troba actualitzat

Es disposa de l'evidència que les opcions de configuració aplicades als antivirus són les recomanades pels fabricants (p.ex. Anàlisi d'execució de programes, anàlisi de correu entrant i sortint, bloqueig automàtic de codi nociu, etc.), així com les referents a la freqüència d'actualització.

## ID 172. Evidències de la difusió del contingut del Pla de Conscienciació

Es disposa d'evidència de la difusió del contingut del pla de conscienciació (en la intranet o per algun altre mitjà es llancen missatges de conscienciació (p.ex. correus, comunicats interns,…)).

## ID 174. Evidències de la difusió del contingut del Pla de Formació

Es disposa d'evidència amb la difusió del contingut del pla de formació en els darrers 3 anys.

## ID 241. Document on s'indica el mecanisme d'autenticació i identificació

Es disposa d'una política o normativa documentada respecte al disseny d'un sistema que contempli els mecanismes d'identificació i autenticació i a més contempla els mecanismes de protecció de la informació tractada.

Així mateix no ha de ser possible accedir a informació del sistema que pugui ser utilitzada per a l'escalada de privilegis, ni executar accions fent-se passar per un altre usuari, etc.

## ID 244. Procediment per a l'elaboració i execució del pla de proves de l'aplicació

Es disposa d'un procediment d'Acceptació i Posada en Servei de Protecció de les Aplicacions Informàtiques. Abans de passar a producció s’ha de comprovar el funcionament correcte de l’aplicació. S’ha de comprovar que:

1- Es compleixen els criteris d’acceptació en matèria de seguretat.

2- No es deteriora la seguretat d’altres components del servei.

3- Les proves s’han de fer en un entorn aïllat (preproducció).

4- Les proves d’acceptació no s’han de fer amb dades reals, llevat que s’asseguri el nivell de seguretat corresponent.

5- Es realitzen anàlisis de vulnerabilitats.

6- Es realitzen anàlisis de coherència i codi font.

## ID 273. Procediment de configuració segura del correu.

Es disposa d'un procediment el qual es detalla com es configura el correu per tal de disposar d'un sistema segur.

## ID 276. Evidència de l'eina monitoratge dels elements de seguretat

Es disposa de l'evidència en la qual s'observa que es disposa d'una eina per monitoritzar els elements de seguretat com ara els virus o l'spam degudament configurat i mantingut.

## ID 330. Normativa documentada que especifica els deures i obligacions del personal contractat a través d'un tercer.

Es disposa de normativa on s'especifiquen els deures i obligacions del personal contractat a través d'un tercer.

## ID 460. Protocol d'actuació envers l'incompliment de les obligacions per part del personal tercer

Es disposa d'un procediment que defineix la resolució d'incidents relacionats amb l'incompliment de les obligacions per part del personal del tercer, a més d'identificar a la persona de contacte amb el tercer per a la resolució d'aquest tipus d'incidents.