AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA | Generalitat de Catalunya

CLASSIFICACIÓ
SENSIBLE
GENERALITAT DE CATALUNYA

AQUEST FULL NO HA DE SEPARAR-SE DEL DOCUMENT QUE L'ACOMPANYA

INFORMACIÓ IMPORTANT DEL DOCUMENT

Si vostè és usuari d'aquesta informació:

- ✓ **El contingut adjunt mai s'hauria de conèixer fora de l'àmbit d'actuació de la Generalitat de Catalunya i els seus proveïdors estrictament vinculats.**
- ✓ **El document ha d'estar custodiat en un recinte tancat.**
- ✓ **En cas que l'origen de l'enviament sigui una bústia genèrica, cal indicar sempre el nom de l'emissor.**
- ✓ **L'enviament d'aquesta informació per correu electrònic cal fer-la, sempre que sigui possible, de forma xifrada. En el cas que no es pugui xifrar, caldrà protegir el document amb contrasenya.**
- ✓ **No està autoritzat enviar el contingut del document adjunt a bústies no pertanyents a l'àmbit de la Generalitat de Catalunya o els seus proveïdors.**
- ✓ **L'enviament per correu postal es farà en sobre tancat, sense etiquetes externes que indiquin el nivell de classificació, i mitjançant serveis de missatgeria reconeguts per l'entitat emissora.**
- ✓ **S'ha de garantir que la informació adjunta estigui fora de l'abast de tercers no autoritzats.**
- ✓ **En el cas de transmissió de la informació a través de converses (presencials, telefòniques, videoconferències, etc.), cal extremar les mesures per a que només personal usuari de la informació pugui tenir accés a la mateixa, evitant llocs públics o llocs compartits.**
- ✓ **En la divulgació d'aquesta informació se n'ha de garantir la integritat per evitar la modificació per part d'un tercer no autoritzat.**
- ✓ **En l'emmagatzematge d'aquesta informació, se n'ha de garantir que la informació queda fóra de l'abast de tercers no autoritzats, evitant llocs exposats obertament.**
- ✓ **L'accés a aquesta informació s'ha de limitar a personal autoritzat, establint les mesures de protecció necessàries per garantir-ho (tant en format paper com en format electrònic).**
- ✓ **S'ha d'evitar l'exposició accidental o no intencionada de la informació a persones no usuàries de la informació.**
- ✓ **Els documents impresos s'han de recollir al moment, i no s'han de deixar ni oblidar a la safata de la impressora.**
- ✓ **En cas de ser necessària la destrucció de la informació, cal utilitzar un procediment que en garanteixi una eliminació efectiva. Si el format és paper, cal utilitzar destructora que impedeixi la seva recuperació o lectura. Si es tracta d'un format digital, caldrà executar un esborrat lògic segur. En tots dos casos, caldrà registrar-ne la destrucció.**
- ✓

sensible

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Esborrany d'Informe d'Auditoria de Compliment de l'Esquema Nacional de Seguretat (ENS) Fase III Consorci Administració Oberta de Catalunya

Novembre 2020

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Fitxa del document

Títol	Esborrany d'Informe d'Auditoria de Compliment de l'ENS Fase III Consorci Administració Oberta de Catalunya
Fitxer físic	Agència de Ciberseguretat de Catalunya - Esborrany d'Informe d'Auditoria de Compliment de l'ENS Fase III - CAOC_v1.docx.

Versió	Redactat per	Revisat per	Aprovat per	Data aprovació
1	Servei d'Auditoria	Àrea de Compliment Normatiu	Agència de Ciberseguretat de Catalunya	13/11/2020

Registre de canvis			
Versió	**Pàgines**	**Data de modificació**	**Motiu del canvi**
1.0	39	13/11/2020	Esborrany d'Informe d'Auditoria

Entitat Auditada: **Consorci Administració Oberta de Catalunya (CAOC)**
Entitat Auditora: **Agència de Ciberseguretat de Catalunya**

ÍNDEX

01 INTRODUCCIÓ I ANTECEDENTS

L'Esquema Nacional de Seguretat (en endavant, ENS) té com a objecte, en l'àmbit de les Administracions Públiques, l'establiment d'una política de seguretat en la utilització de mitjans electrònics, que permeti l'adequada protecció de la informació.

L'ENS es va definir en la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics (actualment derogada per la Llei 39/2015). El seu text es va desenvolupar posteriorment, mitjançant el Reial Decret 3/2010 (en endavant, RD 3/2010), de 8 de gener, on va quedar regulat en l'àmbit de l'Administració Electrònica, és a dir, a la seguretat dels sistemes d'informació del Sector Públic. Més tard, aquesta legislació va patir una modificació mitjançant el Reial Decret 951/2015 (en endavant, RD 951/2015), del 23 d'octubre.

La finalitat de l'ENS és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures que garanteixen la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, permetent als ciutadans i a les Administracions Públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans.

Així, mitjançant aquesta legislació s'assegura que els sistemes d'informació prestaran els seus serveis i custodiaran la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control i sense que la informació pugui arribar al coneixement de persones no autoritzades. Per això, es desenvoluparà i perfeccionarà al llarg del temps l'evolució de la tecnologia, els nous estàndards internacionals sobre seguretat i auditoria i la consolidació de les infraestructures que li serveixen de suport, mantenint-se actualitzat de manera permanent.

L'ENS estableix el requisit de verificar mitjançant una auditoria que els sistemes d'informació de l'Administració Electrònica compleixen amb les mesures de seguretat incloses en l'Annex II del RD 3/2010 i en el RD 951/2015 quan aquests estan classificats amb un nivell de criticitat mitjà o alt.

En aquest sentit, l'Agència de Ciberseguretat de Catalunya, com a entitat encarregada, entre d'altres funcions, de planificar, gestionar i controlar la seguretat de les TIC de l'Administració de la Generalitat i del seu sector públic en virtut de la Llei 15/2017, del 25 de juliol, de l'Agència de Ciberseguretat de Catalunya, els seus estatuts i l'Acord del Govern pel qual s'aprova el contracte programa entre l'Administració de la Generalitat de Catalunya, mitjançant el Departament de Polítiques Digitals i Administració Pública, i la Fundació Centre de Seguretat de la Informació de Catalunya per als anys 2019-2022, de 5 de Febrer de 2019, portarà a terme una auditoria de l'ENS en els sistemes que estan sota la seva responsabilitat. Aquest procés es realitza mitjançant diferents fases on s'auditen sistemes de cada un dels departaments de la Generalitat de Catalunya.

Per a la fase actual d'auditoria, la Fase III, l'Agència de Ciberseguretat de Catalunya ha inclòs dins l'abast un subconjunt dels sistemes d'informació de la Generalitat de Catalunya en funció dels següents criteris:

1. Suporten processos crítics, segons la definició de SIC (Sistema d'Informació Crític).
2. Representen a tots els Departaments que integren la Generalitat de Catalunya, bé perquè són responsables d'un procés suportat per algun dels sistemes seleccionats o el sistema és transversal.
3. Involucren a la majoria dels prestadors de serveis del Centre de Telecomunicacions i Tecnologies de la Informació (en endavant, CTTI).
4. Comparteixen sinergies tecnològiques amb sistemes auditats a les Fases I i II.

En el present document es detallen els resultats de l'auditoria del sistema d'informació del CAOC inclòs a la Fase III d'aquest procés d'auditoria de l'ENS.

02 OBJECTIU I ABAST

L'objectiu d'aquest informe és expressar una opinió sobre el grau de compliment i nivell de maduresa per part de l'entitat auditada de les mesures de seguretat estipulades en l'Annex II del RD 3/2010 i les modificacions publicades a la Disposició Addicional quarta del RD 951/2015.

L'opinió reflectida en el mateix es refereix exclusivament al grau de compliment i nivell de maduresa en data 27 d'agost de 2020.

La conformitat dels sistemes d'informació amb tots els requisits establerts en l'Annex II del RD 3/2010 s'ha obtingut mitjançant l'avaluació de les evidències proporcionades per tots els actors implicats en l'auditoria i que es detallen més endavant a la *Taula 1. Actors implicats i categorització del sistema*. Les mateixes en cap cas s'han obtingut directament per part de l'equip d'auditoria. En aquest sentit, el Servei d'Auditoria no és responsable de les anomalies en els resultats presentats en aquest informe que poguessin haver-se ocasionat per la informació no confiable facilitada per alguna de les fonts.

Dins l'abast d'aquesta auditoria s'inclou el **sistema *Extranet de les Administracions Públiques de Catalunya*** (en endavant, EACAT) que és gestionada des del Consorci Administració Oberta de Catalunya. Aquest portal estableix un canal bidireccional de comunicació segur entre administracions, que permet la tramesa de documentació electrònica, basada en formularis i intercanvi automatitzat de dades, amb seguretat tècnica i jurídica mitjançant l'ús de la signatura electrònica i de registres telemàtics.

L'EACAT està format per dues plataformes unides amb un únic sistema d'identificació:

- EACAT-TR: On es troba localitzada la Base de Dades.
- EACAT-PL: On es troba localitzat el frontal web.

Els usuaris que fan ús de l'aplicació en la seva operativa (en endavant, usuaris de l'aplicació) són usuaris de les diferents administracions públiques catalanes i altres organismes i institucions que estiguin adherits a l'EACAT. Addicionalment, a cadascun dels ens esmentats anteriorment es designa un/s responsable/s de la configuració funcional del sistema (en endavant, usuaris gestors).

Els usuaris gestors i els usuaris de l'aplicació poden accedir a l'EACAT mitjançant:

- Usuari i contrasenya, propi del sistema.
- Certificat (amb validació del mòdul PSIS).
- GICAR.

Per aquest sistema s'han avaluat els aspectes de seguretat de l'aplicació web, les mesures aplicables del lloc de treball dels usuaris del CAOC, les bases de dades que intervenen i els controls de seguretat associats a la infraestructura dels servidors i comunicacions que donen suport al sistema.

Pel fet que l'operativa dels usuaris gestors i dels usuaris de l'aplicació del sistema no requereix l'ús de suports d'informació, només s'han analitzat les mesures de protecció dels suports d'informació aplicades pel prestador de serveis de CPD.

A continuació, es mostra el detall dels actors implicats en l'administració i el manteniment del sistema EACAT, el nivell de seguretat global del mateix i la categorització de cadascuna de les dimensions de seguretat segons la classificació realitzada pel CAOC:

		Actors implicats						Categorització					
Sistema d'informació	**ORG**	**CPD**	**APP**	**LLT**	**COM**	**CORREU**	**SAU**	**D**	**A**	**I**	**C**	**T**	**Global sistema**
EACAT	CAOC	Mediacloud-NTT	Open-trends	Intern	NTT	Opentrends	LT1-Everis	Baix	Baix	Baix	Baix	Baix	Baix
Extranet de les Administracions Públiques de Catalunya (EACAT)		**DPT/ORG:** Departament / Organisme responsable **CPD:** Centre de Processament de Dades **APP:** Aplicació **LLT:** Lloc de Treball **COM:** Comunicacions **CORREU:** Correu electrònic **SAU:** Servei d'Atenció a l'Usuari						**D:** Disponibilitat **A:** Autenticitat **I:** Integritat **C:** Confidencialitat **T:** Traçabilitat					

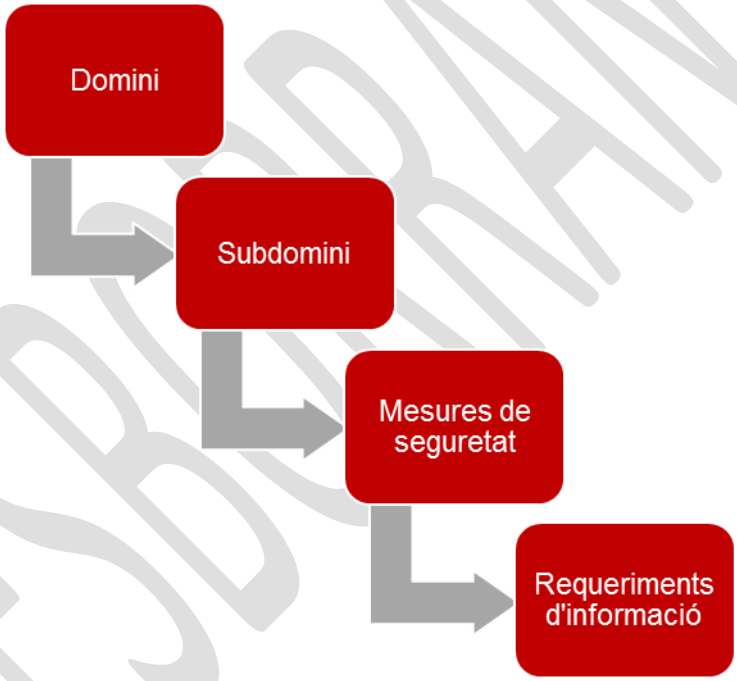
Taula 1. Actors implicats i categorització del sistema

03 DEFINICIÓ DELS DOMINIS I SUBDOMINIS DE L'ENS

Les mesures de seguretat que es troben definides a l'Annex II de l'ENS es troben agrupades en els següents **tres dominis** i per cadascun d'ells en diversos subdominis de seguretat**:**

- **Marc organitzatiu** que està format pel conjunt de mesures relacionades amb l'organització global de la seguretat.
- **Marc operacional** que està format per les mesures que s'han d'adoptar per protegir l'operació dels sistemes d'informació.
- **Mesures de protecció** que està format pel conjunt de mesures que se centren a protegir actius concrets, segons la seva naturalesa i la qualitat exigida pel nivell de seguretat.

A partir d'aquestes mesures de seguretat, s'han establert un conjunt de requeriments d'informació per poder realitzar la present auditoria.



Il·lustració 1. Estructura de l'Esquema Nacional de Seguretat

A continuació, s'exposen les principals característiques dels diferents subdominis:

- ***Marc organitzatiu:***

1. **Marc organitzatiu**: Es tracten les mesures relacionades amb l'organització global de la seguretat, com la definició d'una política de seguretat, amb l'establiment d'un conjunt d'estàndards que descriguin la forma en la qual s'han de dur a terme determinades activitats, les responsabilitats i autoritzacions en l'ús de les TIC.

   Aquests aspectes són requerits tant a l'Organisme responsable del sistema, com a tots els prestadors de serveis.

- ***Marc operacional:***

2. **Planificació:** Es tracten totes aquelles mesures relacionades amb disposar d'una anàlisi de risc, amb la gestió de l'arquitectura de seguretat i amb la gestió d'adquisició, de capacitat i dimensionament de nous components.

   Aquests aspectes són requerits tant a l'Organisme responsable del sistema, com als prestadors de serveis de CPD i d'Aplicacions.

3. **Control d'accés:** Es tracten el conjunt de mesures relacionades amb la gestió dels usuaris, així com dels seus drets d'accés. Així mateix, es fa especial èmfasi en disposar d'una segregació òptima de les funcions i tasques dels usuaris.

   En aquest cas les mesures apliquen tant pel control dels usuaris gestors com pels usuaris de l'aplicació, així com pels usuaris del prestador de serveis CPD, que administren les bases de dades i les infraestructures (en endavant, usuaris administradors) que donen suport al sistema auditat.

4. **Explotació:** Es tracten com a mesures destacables les següents: mesures de seguretat relacionades amb la gestió de la configuració dels sistemes, mesures respecte a la gestió de canvis i dels incidents de seguretat i també en relació als registres de les activitats dels usuaris.

   Aquests aspectes són requerits tant a l'Organisme responsable del sistema, com a tots els prestadors de serveis.

5. **Serveis externs:** Fa referència als Acords de Nivell de Servei (en endavant, ANS) definits amb els prestadors de serveis i els mecanismes establerts per vetllar pel compliment de les seves obligacions de servei.

   Aquest subdomini no aplica al sistema EACAT ja que el sistema està categoritzats com a nivell baix.

6. **Continuïtat del servei:** Es tracten les següents mesures de seguretat: una anàlisi d'impacte que permeti identificar els requeriments de disponibilitat del servei i un pla de continuïtat que estableixi les accions a executar en cas d'interrupció dels serveis prestats amb els mitjans habituals.

   Aquest subdomini no aplica al sistema EACAT ja que el sistema està categoritzats com a nivell baix.

7. **Monitorització del sistema:** Es focalitza en la necessitat d'establir eines de detecció o prevenció d'intrusió i també de disposar d'un sistema de mètriques que permeti conèixer el grau d'implantació de les mesures de seguretat i el nombre d'incidents identificats i el temps utilitzat per resoldre'ls.

   Aquests aspectes són requerits tant a l'Organisme responsable del sistema com al prestador de serveis de CPD.

❖ ***Mesures de protecció:***

8. **Protecció de les instal·lacions i infraestructures:** Es tracten el conjunt de mesures de seguretat física i continuïtat que és necessari disposar als centres de processament de dades.

   Aquests aspectes són requerits al prestador de serveis de CPD.

9. **Gestió del personal:** Es centra en el conjunt de mesures de seguretat i continuïtat relacionades amb la gestió del personal, com ara, les accions de conscienciació i formació portades a terme en matèria de seguretat de la informació.

   Aquests aspectes són requerits tant a l'Organisme responsable del sistema, com als prestadors de serveis de CPD, d'Aplicacions i del SAU.

10. **Protecció dels equips:** S'exposen les diferents mesures de seguretat i continuïtat que cal implementar a les estacions de treball.

    Pel sistema analitzat, s'han analitzat les mesures de seguretat de les estacions de treball dels usuaris gestors i usuaris de l'aplicació de l'EACAT.

11. **Protecció de les comunicacions:** S'enfoca a les mesures de seguretat i continuïtat relatives a les comunicacions mitjançant, entre d'altres, l'establiment d'un perímetre segur i d'una segregació de xarxes adequada.

    Aquests aspectes són requerits al prestador de serveis de Comunicacions.

12. **Protecció dels suports d'informació:** Es fa referència a les mesures de seguretat que permeten protegir els suports d'informació durant tot el seu cicle de vida.

En aquest cas, ja que l'operativa dels usuaris gestors i dels usuaris de l'aplicació no requereix l'ús de suports d'informació, només s'han analitzat les mesures de protecció aplicades pel prestador de serveis de CPD.

13. **Protecció de les aplicacions informàtiques:** Es tracten totes aquelles mesures de seguretat que és necessari establir durant el desenvolupament i posada en producció d'una aplicació.

    Aquests aspectes són requerits al prestador de serveis d'Aplicacions.

14. **Protecció de la informació:** Hi ha establertes un conjunt de mesures de seguretat i continuïtat, entre les quals, destaquen les mesures relatives a les dades de caràcter personal, la utilització de la signatura electrònica, el xifrat de la informació o les mesures relacionades amb les còpies de seguretat.

    Aquests aspectes són requerits tant a l'Organisme responsable del sistema, com als prestadors de serveis de CPD i de Comunicacions.

15. **Protecció dels serveis:** Es tracten les mesures de seguretat i continuïtat relacionades amb la protecció del correu electrònic, de les aplicacions web i protecció davant la denegació de servei.

    Aquests aspectes són requerits als prestadors de serveis de CPD, d'Aplicacions, de Correu i de Comunicacions.

04 METODOLOGIA I TREBALL REALITZAT

El treball realitzat s'ha dut a terme mitjançant el marc metodològic que es detalla a continuació.

Il·lustració 2. Marc metodològic de l'Esquema Nacional de Seguretat

4.1 FASE 0 - PLANIFICACIÓ

Aquesta fase, que s'ha desenvolupat durant el mes de juliol de 2019 ha consistit a planificar la present auditoria i a definir el seu objectiu i abast.

4.2 FASE 1 - PRESA DE REQUERIMENTS

La següent fase s'ha desenvolupat des del setembre fins al desembre de 2019. Aquesta ha consistit en el següent:

4.2.1 Identificació dels controls i actors implicats

Per tal de seleccionar les mesures de seguretat que apliquen als diferents actors i al sistema d'informació definit a l'abast d'aquesta auditoria, s'han dut a terme les següents activitats:

- S'han identificat i analitzat els controls de l'ENS que apliquen als sistemes auditats, tenint en compte les seves característiques i categorització.
- S'han identificat els actors implicats i s'han assignat les mesures de seguretat de l'ENS segons les funcions desenvolupades per cadascun d'ells.

4.2.2 **Requeriments d'informació**

Les activitats que s'han realitzat amb la finalitat de sol·licitar els requeriments d'informació necessaris per a la realització de la present auditoria es detallen a continuació:

- S'han analitzat les evidències necessàries a fi de detectar aquelles que són transversals a tots els sistemes i/o a tots els Departaments/Organismes per tal de minimitzar el volum de qüestions a formular.
- S'han elaborat qüestionaris de sol·licitud d'evidències de les diferents mesures de seguretat segons l'aplicabilitat d'aquestes. Aquests qüestionaris han estat adaptats:
  - En funció de l'interlocutor que havia de donar resposta als requeriments plantejats.
  - S'han tingut en compte les evidencies ja rebudes a les fases anteriors i s'ha revisat la seva vigència a fi de no demanar-les de nou.
- Respecte als interlocutors dels Departaments/Organismes de la Generalitat de Catalunya, s'han dut a terme diverses reunions presencials amb l'objectiu de realitzar la petició de les evidències i obtenir les respostes als requeriments plantejats. Les evidències en cap cas s'han obtingut directament per part de l'equip d'auditoria.
- En relació als prestadors de serveis, s'ha determinat realitzar la sol·licitud d'evidències per correu electrònic i la recollida d'aquestes mitjançant repositoris corporatius o del propi prestador. En cas necessari s'han realitzat reunions per tal de facilitar la tasca de recollida d'evidències. Les evidències en cap cas s'han obtingut directament per part de l'equip d'auditoria.

4.3 FASE 2 - DOCUMENTACIÓ

Aquesta fase s'ha desenvolupat des del mes de març fins a finals d'agost de 2020 i ha consistit en el següent:

4.3.1 **Anàlisi d'evidències**

Les tasques dutes a terme per poder realitzar l'anàlisi de les evidències sol·licitades, han estat les següents:

- S'ha desenvolupat i implementat un programa de treball per tal de poder realitzar el seguiment i l'anàlisi de les evidències requerides en els qüestionaris.
- S'ha analitzat la informació rebuda per tal de validar-ne cadascuna de les mesures de seguretat establertes a l'apartat *4.2.1 Identificació dels controls i actors implicats.*
- Durant l'anàlisi de les evidències obtingudes en la present auditoria i, en particular, respecte als requeriments del domini Marc Organitzatiu, s'ha tingut en consideració el Marc Normatiu de Seguretat de la informació de la Generalitat de Catalunya (en endavant, Marc Normatiu), així com la Instrucció d'Ús de les TIC 3/2018.
- S'ha determinat el grau de compliment de les mesures de seguretat de l'Annex II de l'ENS, a partir de les següents perspectives: la definició de procediments documentats i l'execució de procediments de forma operativa.

- En els casos en què ha estat necessari, s'han demanat aclariments als interlocutors amb la finalitat d'avaluar adequadament el resultat de les mesures de seguretat.

4.3.2 **Resultats**

L'auditoria mostra el grau de compliment, grau de fiabilitat i nivell de maduresa agrupats per subdomini.

4.3.2.1 ***Grau de compliment***

El grau de compliment de les mesures de seguretat incloses a l'Annex II de l'ENS respecte al sistema d'informació definit a l'abast d'aquesta auditoria, es determina tenint en compte:

- El conjunt de requeriments que donaran compliment a cada mesura de seguretat.
- El compliment de cada requeriment (100% si compleix, 50% si compleix parcialment i 0% si no compleix).
- El pes de cada requeriment (assignat segons la seva criticitat entre 1 i 5, on 5 és la criticitat màxima).

4.3.2.2 ***Grau de fiabilitat***

D'acord amb la metodologia, les evidències que finalment no han estat obtingudes s'han considerat en el càlcul del grau de compliment com a incompliments. Per aquest motiu, s'ha establert el paràmetre fiabilitat com el grau d'evidències obtingudes respecte a les sol·licitades, amb l'objectiu de tenir present en quina mesura les evidències no obtingudes podrien arribar a millorar el grau de compliment.

4.3.2.3 ***Càlcul del nivell de maduresa***

S'ha determinat el nivell de maduresa[1] a partir de la següent taula en la qual es defineixen les equivalències entre el grau de compliment i el nivell de maduresa.

Grau de compliment	Nivell de maduresa	Significat	Descripció
0 - 9%	0	Inexistent	Aquesta mesura no està sent aplicada en aquest moment.
10 - 49%	1	Inicial / ad hoc	Quan l'organització no proporciona un entorn estable. L'èxit o fracàs del procés depèn de la competència i bona voluntat de les persones, però és difícil preveure la reacció davant d'una situació d'emergència.
50 - 79%	2	Repetible, però intuïtiu	Quan hi ha un mínim de planificació que, acompanyada de la bona voluntat de les persones proporciona una pauta a seguir en situacions que es donen de manera recurrent. És impredictible el resultat si es donen circumstàncies noves.
80 - 89%	3	Procés definit	Es disposa un catàleg de processos que es manté actualitzat. Aquests processos garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2, i que es gestiona al nivell 3.
90 - 99%	4	Gestionat i mesurable	Quan es disposa d'un sistema de mesures i mètriques per conèixer l'acompliment (eficàcia i eficiència) dels processos. La Direcció és capaç d'establir objectius qualitatius a assolir i disposa de mitjans per valorar si s'han assolit i en quina mesura.
100%	5	Optimitzat	En aquest nivell, l'organització és capaç de millorar l'acompliment dels sistemes a partir d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.

Taula 2. Equivalència entre el grau de compliment i el nivell de maduresa.

[1] **'Guía de Seguridad (CCN-STIC 804) - Esquema Nacional de Seguridad - Guía de implantación'.**

4.3.2.4 ***Interpretació dels resultats***

Els resultats obtinguts en la present auditoria es mostren segons les següents perspectives:

- **Compliment del Sistema:** Inclou els resultats agregats i per subdomini del compliment i la fiabilitat de les evidències rebudes del sistema auditat a la Fase III de l'ENS.
- **Maduresa del Sistema:** Recull el nivell de maduresa agregat i per subdomini de cadascun del sistema auditat a la Fase III de l'ENS.

4.3.2.5 ***Debilitats i recomanacions***

A través dels resultats obtinguts s'han identificat unes observacions i elaborat unes recomanacions on es detallen els incompliments parcials o totals de la present auditoria.

A l'apartat *6.2 Debilitats i recomanacions detectades en l'auditoria ENS de la Fase III* es detallen les observacions i recomanacions pertinents, que conjuntament amb *l'Annex I Quadre de recomanacions per dominis de l'ENS* del present document, donen una visió més clara de les debilitats i recomanacions del sistema auditat.

4.4 FASE 3 - TANCAMENT

Aquesta fase, que s'ha desenvolupat des de mitjan abril fins a principis de novembre del 2020, ha consistit en l'elaboració el present informe a partir dels resultats obtinguts en aquesta auditoria.

05 RESUM EXECUTIU

En funció del treball realitzat i dels resultats obtinguts en el mateix, d'acord amb l'abast de la present auditoria descrit a l'apartat *2. Objectiu i abast*, es determina que el **grau de compliment** de les mesures de seguretat previstes pels Reglaments de desplegament de l'ENS per part del sistema auditat és del **80,27%,** el que suposa un **nivell de maduresa** de **3 sobre 5.** El **nivell de compliment és un càlcul quantitatiu** que no té en compte la criticitat de les mesures ni el seu impacte i, per tant, un alt nivell de compliment no té perquè implicar un alt nivell de seguretat.

A continuació es detallen els subdominis que han obtingut un **millor grau de compliment**, així com els aspectes més rellevants que han originat aquest resultat:

- Respecte al subdomini de ***Protecció de les Instal·lacions i Infraestructures***, el grau de compliment assolit ha estat del 100,0%. En aquest cas, és important destacar que el prestador de serveis de CPD Mediacloud-NTT disposa de les mesures de seguretat físiques requerides, com són, els mecanismes de control d'accés, el correcte condicionament dels locals i subministrament d'energia elèctrica, les mesures necessàries per al compliment de les normatives industrials relatives a la protecció contra incendis i el registre detallat de qualsevol entrada i sortida d'equipament.
- En quant al subdomini de ***Protecció dels suports d'informació***, s'ha obtingut un grau de compliment del 95,7%. S'ha identificat que el prestador de serveis de CPD Mediacloud-NTT disposa dels procediments i els aplica correctament, als mecanismes criptogràfics utilitzats i mesures de custòdia, transport i destrucció dels suports. Malgrat això, s'ha identificat que no es disposa d'un procediment per comparar els registres de les sortides amb les arribades i aixecar les alarmes pertinents quan es detecti algun incident.
- En relació al subdomini de ***Planificació***, s'ha obtingut un grau de compliment del 88,8%. S'ha identificat que pel sistema auditat, el CAOC disposa de mecanismes pel seguiment de la seguretat, com són documentacions d'arquitectura, i una correcta gestió de dimensionament i capacitat. A més, s'ha identificat que es disposa d'una anàlisi de riscos del sistema auditat actualitzada i aprovada durant l'últim any. Addicionalment, es disposa d'un procediment que indica la necessitat de revisió, seguiment i aprovació regular de l'anàlisi de riscos del sistema, com a mínim anual. Tot i això, s'ha identificat que no disposa d'un procés formal per planificar l'adquisició de nous components del sistema.
- Respecte al subdomini de ***Protecció de la Informació***, s'ha obtingut un grau de compliment del 87,8%. S'ha identificat que es realitza correctament el tractament de dades de caràcter personal i la qualificació de la informació del sistema mitjançant un procediment documentat. D'altra banda, s'observa que es realitza una correcta gestió de les còpies de seguretat. Tanmateix, el CAOC no disposa d'un procediment de signatura electrònica per identificar els documents que requereixen capacitat probatòria segons la Llei del Procediment Administratiu.

D'altra banda, també és necessari remarcar els següents dominis en els quals s'ha obtingut un nivell de **compliment relativament inferior** respecte a la resta de subdominis analitzats:

- Pel que fa al subdomini de ***Protecció dels equips***, s'ha assolit un grau de compliment del 49,8%. S'ha identificat que el CAOC realitza operativament mesures de protecció dels equips portàtils i disposa d'un procediment documentat on s'indiquen les mesures que s'han de complir per realitzar un accés remot al sistema. Així mateix, la configuració del bloqueig de la pantalla dels equips compleix amb el Marc Normatiu i es disposa de mecanismes de detecció que permetin saber si l'equip ha estat manipulat. D'altra banda, pel que fa al lloc de treball, tot i disposar d'un inventari dels equips, no es realitzen revisions periòdiques d'aquest i no es disposa d'un procediment de les mesures de protecció dels equips on es reculli la responsabilitat de revisar periòdicament la possessió de cada portàtil per la persona que consta a l'inventari.
- Pel que fa al subdomini de ***Monitorització del sistema,*** s'ha obtingut un grau de compliment del 55,6%. Tot i que es disposa d'una anàlisi de riscos del servei EACAT incloent els indicadors de risc, així com un diagnòstic de seguretat realitzat per l'Agència, no s'han definit els indicadors per mesurar la seguretat i el rendiment del sistema.
- Respecte al subdomini de ***Control d'accés***, s'ha assolit un grau de compliment del 60,5%. S'ha identificat que pel que fa al CAOC, no es disposa d'un procediment formalitzat de gestió d'usuaris. A més, en quant al CAOC i al prestador de serveis d'aplicació Opentrends, amb la informació proporcionada no es pot assegurar que es realitzin revisions dels usuaris gestors i de l'aplicació, així com tampoc es disposi d'un procediment de revisió on es comprovi que els usuaris donats de baixa han estat bloquejats o eliminats complint amb el període de retenció establert per procediment. Així mateix, hi ha usuaris gestors i de l'aplicació amb més d'un rol assignat sense identificadors singulars per a cadascun dels casos i a més, amb la informació proporcionada, no es pot assegurar que s'inhabilitin els permisos dels usuaris quan aquests deixen l'organització. Addicionalment, aquests usuaris no es bloquegen després del període d'inactivitat fixat per procediment. Tanmateix, no es pot assegurar que s'informi als usuaris de les seves obligacions un cop han accedit dins el sistema. Per altra banda, no es disposa d'un procediment de gestió de drets d'accés al sistema. A més, pel que fa al mecanisme d'accés que utilitza el sistema auditat, s'ha identificat que hi ha paràmetres que difereixen dels controls definits dins del Marc Normatiu. Pel que fa el prestador de serveis de CPD Mediacloud-NTT, s'ha identificat que els usuaris administradors són genèrics i no s'observa que els usuaris tinguin assignats un únic rol o perfil. Addicionalment, amb la informació proporcionada, no es pot assegurar que els comptes d'usuaris administradors s'inhabilitin tant bon punt els usuaris deixen l'organització i no es pot assegurar que els comptes d'usuaris administradors compleixin amb el període de retenció establert per procediment. Per altra banda, s'ha identificat que no es revisen els usuaris administradors del sistema de forma periòdica.

A l'apartat *6. Resultats de la Fase III de l'Auditoria de l'ENS al Consorci Administració Oberta de Catalunya* es detallen els incompliments totals o parcials identificats en la present auditoria, així com les recomanacions pertinents.

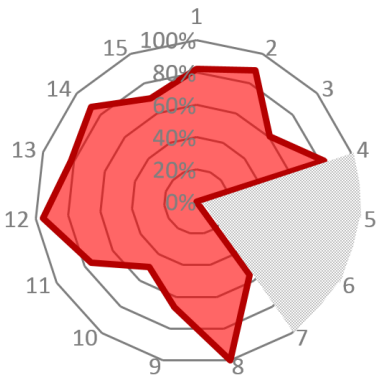
06 RESULTATS DE LA FASE III DE L'AUDITORIA DE L'ENS AL CONSORCI ADMINISTRACIÓ OBERTA DE CATALUNYA

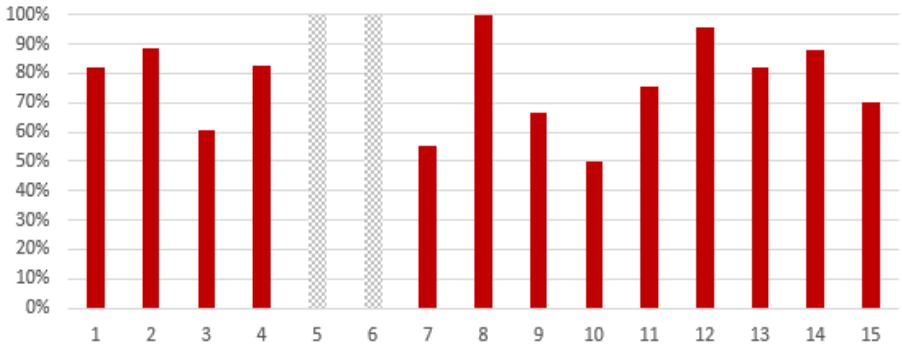
6.1 ANÀLISI DEL COMPLIMENT I MADURESA DEL SISTEMA AUDITAT A LA FASE III DE L'ENS

Sistema EACAT	**Extranet de les Administracions Públiques de la Generalitat de Catalunya**	**80,3%**	**96,9%**

Marc organitzatiu		Compliment	Fiabilitat
1	Marc organitzatiu	82,1%	95,2%
Marc operacional		**Compliment**	**Fiabilitat**
2	Planificació	88,8%	100,0%
3	Control d'accés	60,5%	100,0%
4	Explotació	82,7%	96,4%
5	Serveis externs	No aplica	No aplica
6	Continuïtat del servei	No aplica	No aplica
7	Monitorització del sistema	55,6%	55,6%
Mesures de protecció		**Compliment**	**Fiabilitat**
8	Protecció de les instal·lacions i infraestructures	100%	100,0%
9	Gestió del personal	66,5%	85,9%
10	Protecció dels equips	49,8%	100,0%
11	Protecció de les comunicacions	75,3%	100,0%
12	Protecció dels suports d'informació	95,7%	100,0%
13	Protecció de les aplicacions informàtiques	81,8%	100,0%
14	Protecció de la informació	87,8%	100,0%
15	Protecció dels serveis	70,0%	93,1%

A continuació, es mostra de forma gràfica i per subdomini el grau de compliment del sistema.

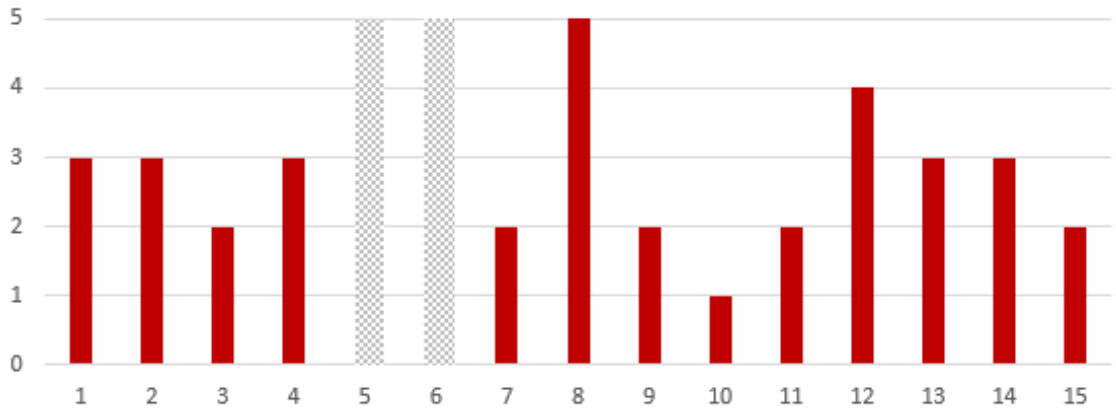




Sistema EACAT	Extranet de les Administracions Públiques de la Generalitat de Catalunya	3

Marc organitzatiu		Maduresa
1	Marc organitzatiu	3
Marc operacional		**Maduresa**
2	Planificació	3
3	Control d'accés	2
4	Explotació	3
5	Serveis externs	No aplica
6	Continuïtat del servei	No aplica
7	Monitorització del sistema	2
Mesures de protecció		**Maduresa**
8	Protecció de les instal·lacions i infraestructures	5
9	Gestió del personal	2
10	Protecció dels equips	1
11	Protecció de les comunicacions	2
12	Protecció dels suports d'informació	4
13	Protecció de les aplicacions informàtiques	3
14	Protecció de la informació	3
15	Protecció dels serveis	2

A continuació, es mostra de forma gràfica i per subdomini el nivell de maduresa del sistema.



6.2 DEBILITATS I RECOMANACIONS DETECTADES EN L'AUDITORIA ENS DE LA FASE III

R.01: Política de seguretat

Subdomini	Marc organitzatiu
Mesures	org.2; org.3; org.4
Sistemes afectats	EACAT

Observacions

Pel que fa al CAOC i al prestador de serveis de comunicacions NTT, no disposen d'un procés formal per a les autoritzacions respecte als sistemes d'informació que inclogui:

- Un procés formal d'autorització d'utilització d'instal·lacions habituals i alternatives.
- Un procés formal d'autorització d'entrada d'equips en producció, en particular, equips que involucrin criptografia.
- Un procés formal d'autorització d'establiment d'enllaços de comunicacions amb altres sistemes.
- Un procés formal d'autorització d'utilització de mitjans de comunicació, habituals i alternatius.

Addicionalment, el prestador de serveis de comunicacions NTT no disposa d'un procés formal d'autorització d'entrada d'aplicacions en producció.

Pel que fa al prestador de serveis d'aplicació Opentrends, amb la informació proporcionada no es pot assegurar que es disposi dels procediments interns de seguretat actualitzats. Addicionalment, tot i disposar d'una normativa de seguretat pròpia, amb la informació proporcionada no es pot assegurar que estigui disponible per tots els usuaris implicats.

A més, pel que fa als prestadors de serveis d'aplicació Opentrends, de comunicacions NTT i el propi lloc de treball, amb la informació proporcionada no es pot assegurar que es disposi d'una normativa de seguretat actualitzada ni que se'n faci difusió.

Recomanacions

Pel que fa al CAOC i al prestador de serveis NTT, han d'establir un procés formal d'autoritzacions que cobreixi tots els elements del sistema d'informació:

- Utilització d'instal·lacions, habituals i alternatives.
- Entrada d'equips en producció, en particular, equips que involucrin criptografia.
- Establiment d'enllaços de comunicacions amb altres sistemes.
- Utilització de mitjans de comunicació, habituals i alternatius.

Addicionalment, el prestador de serveis de comunicacions NTT ha de disposar d'un procés formal d'autorització d'entrada d'aplicacions en producció.

Pel que fa al prestador de serveis d'aplicació Opentrends, ha de disposar de documentació que detalli de forma clara i precisa:

- Com portar a terme les tasques habituals.
- Qui ha de fer cada tasca.
- Com identificar i reportar comportaments anòmals.

A més, pel que fan els prestadors de serveis d'aplicació Opentrends, de comunicacions NTT i el propi lloc de treball, han de disposar d'una Normativa de Seguretat que descrigui:

- L'ús correcte d'equips, serveis i instal·lacions.
- El que es considera ús indegut.
- La responsabilitat del personal respecte del compliment o violació d'aquestes normes: drets, deures i mesures disciplinàries d'acord amb la legislació vigent.

Addicionalment, s'ha de fer difusió de la Normativa de Seguretat als usuaris.

R.02: Procediment de gestió d'incidents de seguretat

Subdomini	Marc organitzatiu
Mesures	org.3
Sistemes afectats	EACAT

Observacions

Pel que fa al CAOC, s'ha identificat que tot i que es realitza una gestió operativa dels incidents de seguretat, no es disposa d'un procediment formalitzat de gestió d'incidents de seguretat aprovat.

Recomanacions

El CAOC ha de disposar d'un procediment intern de notificació, registre i gestió d'incidències actualitzat.

R.03: Comunicacions i serveis en xarxa

Subdomini	Marc organitzatiu; Protecció de les comunicacions; Protecció dels serveis
Mesures	org.3; mp.com.3.1; mp.s.1; mp.s.2.1
Sistema afectat	EACAT

Observacions

En quant al prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, amb la informació proporcionada no es pot assegurar la implantació de regles del tallafoc per evitar atacs de WebProxy's o DNS Caché. Per altra banda, s'ha identificat que es disposa d'usuaris administradors genèrics i a més, amb la informació proporcionada no es pot assegurar que s'assignin els usuaris a grups específics i disposin d'uns permisos delimitats, de forma que es previnguin els intents d'escalat de privilegis.

Pel que fa al prestador de serveis d'aplicació Opentrends, pel sistema EACAT, la informació de les cookies no s'emmagatzema xifrada, no protegint de forma adequada els atacs de manipulació de cookies. Addicionalment, no disposen de mecanismes que evitin atacs de manipulació d'URL, injecció de codi, escalat de privilegis i "cross-site-scripting", en definitiva no es disposa d'una correcta protecció contra atacs d'injecció de codi.

Pel que fa al prestador de serveis de correu Opentrends, tot i que fa ús d'un antivirus als servidors de correu, amb la informació proporcionada no es pot assegurar que aquest es trobi actualitzat i que la seva configuració és la recomanada pel fabricant. Addicionalment, amb la informació proporcionada no es pot assegurar que es disposi d'una política, normativa o estàndard documentada que especifiqui la protecció de l'encaminament de missatges i establiment de connexions. A més, amb la informació proporcionada, no es pot assegurar que es monitoritzin i es protegeixin enfront elements de seguretat, com ara els virus o spam.

En quant al prestador de serveis de comunicacions NTT, no disposa d'una política o normativa documentada que obligui a assegurar l'autenticitat de l'altre extrem d'un canal de comunicació abans d'intercanviar cap informació. Així mateix, no disposa de política o normativa documentada que especifiqui l'ús de mecanismes per a la prevenció i detecció d'atacs actius. A més, no disposa de procediments de transmissió de dades per xarxes públiques.

Recomanacions

En quant al prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, ha d'implantar regles del tallafoc o disposar d'una eina especialitzada que eviti atacs de WebProxy's o DNS Caché. Per altra banda, s'han de retirar els usuaris administradors genèrics amb contrasenyes per defecte i a més, s'ha de garantir que els usuaris es troben assignats a un grup determinat i que disposen d'uns permisos delimitats, de forma que es previnguin els intents d'escalat de privilegis.

Pel que fa al sistema d'informació EACAT, el prestador de serveis d'aplicació Opentrends:

- S'ha d'emmagatzemar la informació de les cookies de forma xifrada.
- S'han de prevenir atacs de manipulació d'URL.

- S'han d'aplicar els següents mecanismes de seguretat contra atacs d'injecció de codi:
  - Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en particular prenent mesures en els següents aspectes:
  - S'evitarà que el servidor ofereixi accés als documents per vies alternatives al protocol determinat.
  - Es previndran atacs de manipulació de fragments d'informació que s'emmagatzema en el disc dur del visitant d'una pàgina web a través del seu navegador, a petició del servidor de la pàgina, conegut en terminologia anglesa com a "cookies".
- Es previndran intents d'escalat de privilegis.
- Es previndran atacs de "cross site scripting".

Pel que fa al prestador de serveis de correu Opentrends, s'ha de disposar d'un procediment documentat que especifiqui la protecció de l'encaminament de missatges i l'establiment de connexions, aquest ha de contemplar els següent punts:

- La informació distribuïda per mitjà de correu electrònic s'ha de protegir, tant en el cos dels missatges com en els annexos.
- S'ha de protegir la informació d'encaminament de missatges i establiment de connexions.
- S'ha de protegir l'organització contra els problemes que es materialitzen per mitjà del correu electrònic, en concret:
  - Correu no sol·licitat, en l'expressió anglesa «spam».
  - Programes perjudicials, constituïts per virus, cucs, troians, espies, o altres de naturalesa anàloga.
  - Codi mòbil de tipus «applet».
- S'han d'establir normes d'ús del correu electrònic per part del personal determinat. Aquestes normes d'ús han de contenir:
  - Limitacions a l'ús com a suport de comunicacions privades.
  - Activitats de conscienciació i formació relatives a l'ús del correu electrònic.

En quant al prestador de serveis de comunicacions NTT, ha de disposar d'una política o normativa documentada que:

- Asseguri l'autenticitat de l'altre extrem d'un canal de comunicació abans d'intercanviar informació.
- Previngui atacs actius, i garantir que almenys es detectaran i s'activaran els procediments previstos de tractament de l'incident. Es consideren atacs actius:
  - L'alteració de la informació en trànsit.
  - La injecció d'informació espúria.
  - El segrest de la sessió per una tercera part.
- Accepti qualsevol mecanisme d'autenticació dels que prevegi la normativa aplicable.

Per últim, ha de disposar d'un procediment de transmissió de dades per xarxes públiques, que incorpori les mesures que s'hauran de portar per poder protegir la transmissió de dades a través de xarxes d'operadors de telecomunicacions (transmissió per Internet, el que implica enviament de correus electrònics, intercanvi de dades a través de FTP o plataformes web).

R.04: Protecció de les dades

Subdomini	Marc organitzatiu
Mesures	org.4
Sistemes afectats	EACAT
Observacions	
Pel que fa al CAOC, no disposa d'un procés formal per a les autoritzacions respecte al tractament d'informació fora de les instal·lacions de l'Organisme.	
Recomanacions	
El CAOC, ha de disposar d'un procés formal d'autoritzacions en relació al tractament d'informació fora de les instal·lacions de l'Organisme, disposant d'un formulari de sol·licitud de l'autorització que hauria d'atorgar la persona designada dins de l'Organisme.	

R.05: Gestió dels suports d'informació

Subdomini	Marc organitzatiu; Protecció dels suports d'informació
Mesures	org.4; mp.si.4
Sistemes afectats	EACAT
Observacions	
Pel que fa al CAOC, s'ha identificat que no existeix un procés formal per a les autoritzacions respecte a la utilització i a la sortida d'equips mòbils (com per exemple, ordinadors portàtils, PDAs o altres de naturalesa anàloga). Per altra banda, pel que fa el prestador de serveis de CPD Mediacloud-NTT, no es realitza el registre d'entrada i sortida dels suports d'informació.	
Recomanacions	
A més, el CAOC, ha de disposar d'un procés formal d'autoritzacions en relació a la utilització i sortida d'equips mòbils, disposant d'un formulari de sol·licitud de l'autorització que hauria d'atorgar la persona designada dins de l'Organisme. Pel que fa el prestador de serveis de CPD Mediacloud-NTT, en relació als suports d'informació tant en suport electrònic com no electrònic, ha de disposar i implantar un registre i d'un procediment de transport dels suports on es detalli el registre d'entrada i sortida dels mateixos. Aquest registre ha d'identificar el transportista que lliura el suport i el transportista que el trasllada. Addicionalment, s'ha d'implantar un procediment rutinari que compari els registres d'entrades i sortides i dispari les alarmes pertinents quan es detecti un incident.	

R.06: Adquisició i devolució d'actius

Subdomini	Planificació
Mesures	op.pl.3
Sistema afectat	EACAT
Observacions	
Pel que fa al CAOC, no disposa d'un procediment d'adquisició de nous components del sistema.	
Recomanacions	
Pel que fa al CAOC, ha d'establir un procés formal per planificar l'adquisició de nous components del sistema, procés que: • Ha d'atendre les conclusions de l'anàlisi de riscos. • Ha de ser conforme a l'arquitectura de seguretat escollida. • Ha de preveure les necessitats tècniques, de formació i de finançament de forma conjunta.	

R.07: Control d'accés lògic

Subdomini	Control d'accés
Mesures	op.acc.1; op.acc.2; op.acc.4; op.acc.5.1; op.acc.6.1
Sistema afectat	EACAT

Observacions

Pel que fa al CAOC, tot i que es fa de manera operativa, no es disposa d'un procediment formalitzat de gestió d'usuaris. A més, en quant al CAOC i al prestador de serveis d'aplicació Opentrends, amb la informació proporcionada no es pot assegurar que es realitzin revisions dels usuaris gestors i de l'aplicació, així com tampoc que es disposi d'un procediment de revisió on es comprovi que els usuaris donats de baixa de l'organització han estat bloquejats o eliminats, i que s'inhabilitin els usuaris gestors i de l'aplicació que finalitzen la relació amb les funcions de cada sistema, complint amb el període de retenció dels usuaris definit per procediment. Així mateix, pel sistema auditat, en quant als usuaris gestors i de l'aplicació, s'ha identificat que es disposa d'usuaris genèrics i aquests no estan associats a un únic rol o perfil. Addicionalment, els usuaris gestors i de l'aplicació no signen un document d'obligacions tot deixant constància del seu identificador.

Per altra banda, tot i que es realitza de manera operativa, no es disposa d'un procediment de gestió de drets d'accés al sistema on s'indiqui qui és el responsable dels recursos i de l'autorització tant dels usuaris gestors com dels usuaris de l'aplicació, i que contingui els requeriments d'accés al sistema. Així mateix, pel que fa al mecanisme d'accés que utilitza el sistema auditat, s'ha identificat que hi ha paràmetres configurats que difereixen dels controls definits dins del Marc Normatiu.

Pel que fa el prestador de serveis de CPD Mediacloud-NTT, pel sistema EACAT:

- S'ha identificat que els usuaris administradors son usuaris genèrics i no s'observa que els usuaris tinguin assignats un únic rol o perfil.
- Amb la informació proporcionada, no es pot assegurar que els comptes d'usuaris administradors s'inhabilitin tant bon punt els usuaris deixen l'organització.
- Amb la informació proporcionada, no es pot assegurar que els comptes d'usuaris administradors compleixin amb el període de retenció establert per procediment.
- No es revisen periòdicament els usuaris administradors del sistema.

Recomanacions

Pel que fa al CAOC, ha de disposar 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. En cas que hi hagi usuaris no nominals hi ha d'haver una relació unívoca entre l'usuari i un propietari de la compte.
- Que els usuaris s'han de retenir durant el període necessari per atendre les necessitats de traçabilitat dels registres d'activitat que hi estan associats.

Addicionalment, pel que fa al CAOC i al prestador de serveis d'aplicació Opentrends s'ha de disposar i implantar un procediment de revisió dels usuaris gestors i de l'aplicació de forma periòdica i realitzar informes de revisió dels mateixos, i a més, que aquest indiqui que els usuaris donats de baixa de l'organització s'han de bloquejar o eliminar, complint amb el període de retenció de traces establert. Per altra banda, s'han de retirar els usuaris genèrics amb contrasenyes per defecte i a més, hi ha d'haver una relació unívoca entre rol i perfil d'usuari. Així mateix, els usuaris gestors i de l'aplicació han de reconèixer que han rebut les credencials d'accés i que coneixen i accepten les obligacions que impliquen la seva recepció, en particular, el deure de custòdia diligent, protecció de la seva confidencialitat i informació immediata en cas de pèrdua.

Per altra banda, s'ha de disposar d'un procediment documentat que contingui els requeriments d'accés als sistemes pels usuaris gestors i els usuaris de l'aplicació, on s'especifiqui el següent:

- Els recursos dels sistemes s'han de protegir amb algun mecanisme que n'impedeixi la utilització, llevat de les entitats que gaudeixin de drets d'accés suficients.
- Els drets d'accés de cada recurs s'han d'establir segons les decisions de la persona responsable del recurs i s'han d'atenir a la política i la normativa de seguretat dels sistemes, on s'ha d'indicar qui són aquests responsables.

Pel que fa al sistema EACAT, s'han d'adaptar els paràmetres de configuració de la seguretat del mètode d'accés, assegurant que compleixin els següents requeriments de seguretat definits pel Marc Normatiu:

- Definir un límit de 5 intents d'accés fallit al sistema abans de bloquejar l'usuari.
- Establir una caducitat de contrasenya de com a màxim 90 dies.
- Establir un històric de contrasenyes de com a mínim 10.
- Establir un criteri de complexitat de contrasenya tal que obligui a contenir obligatòriament almenys un caràcter de cada un dels següents grups: numèric, alfabètic (majúscules i minúscules) i, si el sistema ho permet, caràcters especials (*, +, $, &, #, @, -, !, %, ^, *, ;, (,), {, }, [,], <, >, ?, /,_).

Pel que fa el prestador de serveis de CPD Mediacloud-NTT, pel sistema EACAT:

- S'han de retirar els usuaris estàndard i els usuaris genèrics amb contrasenyes per defecte, en cas que hi hagi usuaris no nominals hi ha d'haver una relació unívoca entre l'usuari i un propietari de la compte.
- Els comptes d'usuaris administradors han de ser inhabilitats en el cas que aquests deixin l'organització.
- Els comptes d'usuaris administradors s'han de retenir durant el període necessari per atendre les necessitats de traçabilitat dels registres d'activitat que hi estan associats (període de retenció).
- S'ha de disposar d'un llistat d'usuaris administradors, aprovat i actualitzat, i s'han de fer revisions periòdicament dels usuaris donats de baixa, així com dels permisos que se'ls hi assigna.

R.08: Registre d'activitats i traces

Subdomini	Control d'accés
Mesures	op.acc.1; op.acc.6.1
Sistemes afectats	EACAT

Observacions

El prestador de serveis d'aplicació Opentrends, pel sistema auditat, tot i que es disposa d'un registre dels accessos dels usuaris de l'aplicació i els usuaris gestors, no disposa d'un registre de les seves accions realitzades.

En canvi, pel que fa el prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, tot i que disposen d'un registre de les accions realitzades, no es poden identificar els usuaris administradors perquè són genèrics.

Recomanacions

Els prestadors de serveis d'aplicació Opentrends, han de registrar i revisar les activitats dels usuaris gestors, de l'aplicació i administradors de manera que:

- El registre ha d'indicar qui fa l'activitat, quan la fa i sobre quina informació.
- S'han de registrar les activitats efectuades amb èxit i els intents fallits.
- S'han de revisar els registres d'activitat per buscar patrons anòmals.

En quant al prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, ha de registrar les traces d'activitat dels usuaris administradors de tal forma que es pugui visualitzar les accions realitzades dels usuaris administradors, així com registrar els intents d'accés erronis.

R.09: Accés local i remot

Subdomini	Control d'accés
Mesures	op.acc.6.1
Sistema afectat	EACAT
Observacions	
En quant al prestador de serveis d'aplicació Opentrends, s'ha identificat que no disposa d'un procediment d'accés local que contempli totes les accions de seguretat a tenir en compte. Per altra banda, pel que fa al sistema auditat EACAT, s'ha identificat que no s'informa als usuaris gestors, als usuaris de l'aplicació i als usuaris administradors de les seves obligacions immediatament després d'accedir al sistema.	
Recomanacions	
Pel que fa al prestador de serveis d'aplicació Opentrends, s'ha de documentar i implantar una política d'accés local que contempli el següent: • S'han de prevenir atacs que puguin revelar informació dels sistemes sense arribar a accedir-hi. La informació revelada a qui intenta accedir-hi ha de ser la mínima imprescindible (els diàlegs d'accés només han de proporcionar la informació indispensable). • El nombre d'intents permesos ha de ser limitat, i s'ha de bloquejar l'oportunitat d'accés una vegada efectuats un cert nombre d'errors consecutius. • S'han de registrar els accessos amb èxit i els fallits. • El sistemes han d'informar a l'usuari de les seves obligacions immediatament després d'obtenir l'accés. Per altra banda, pel que fa al sistema auditat, s'ha d'informar als usuaris gestors, usuaris de l'aplicació i als usuaris administradors de les seves obligacions immediatament després d'obtenir accés als sistemes.	

R.10: Inventari d'actius

Subdomini	Explotació
Mesures	op.exp.1
Sistemes afectats	EACAT
Observacions	
Pel que fa al prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, tot i disposar d'un inventari d'actius que conforma el sistema, amb la informació proporcionada no es pot assegurar que aquest es revisi i es mantingui actualitzat.	
Recomanacions	
Pel que fa al prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, ha de revisar i mantenir actualitzat l'inventari d'actius dels sistemes.	

R.11: Arquitectura de Seguretat

Subdomini	Explotació
Mesures	op.exp.2
Sistema afectat	EACAT

Observacions

Pel que fa al sistema EACAT, en quant als prestadors de serveis de CPD Mediacloud-NTT i d'aplicació Opentrends, s'ha identificat que no disposen d'un procediment de configuració de seguretat que especifiqui les accions dels usuaris que poden posar en risc la informació o el sistema. A més, s'ha identificat que no hi ha advertències de seguretat en cas que hi hagi situacions que puguin posar en risc la seguretat del sistema auditat.

Així mateix, no es requereix del consentiment exprés dels usuaris gestors, de l'aplicació i administradors assumint el risc d'aquestes accions.

Per altra banda, pel que fa el prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, s'ha identificat que es disposa d'usuaris administradors genèrics. Així mateix, amb la informació proporcionada no es pot assegurar que es realitzin diverses validacions funcionals i de seguretat abans de l'entrada a producció dels sistemes.

Recomanacions

Pel que fa al sistema auditat, en quant als prestadors de serveis de CPD Mediacloud-NTT i d'aplicació Opentrends, per tal de garantir la traçabilitat sobre les possibles accions que puguin posar en risc el sistema, s'ha de realitzar un registre de les accions de risc realitzades pels usuaris. A més, en cas que hi hagi situacions que puguin posar en risc la seguretat del sistema, hi ha d'haver advertències de seguretat que requereixin del consentiment exprés per part dels usuaris, assumint el risc. Així mateix, ha d'existir un registre d'aquests consentiments de les advertències de seguretat.

A més, per tal de garantir la traçabilitat sobre les possibles accions que puguin posar en risc els sistemes, s'ha de realitzar un registre de les accions de risc realitzades pels usuaris, tant pels usuaris propis de les aplicacions com els administradors.

En quant al prestador de serveis de CPD Mediacloud-NTT, pel sistema auditat, s'han de retirar els usuaris estàndard i els usuaris genèrics amb contrasenyes per defecte. Per altra banda, per tal de garantir una configuració segura, s'han de portar a terme validacions funcionals i de seguretat abans de l'entrada a producció dels sistemes.

R.12: Criptografia

Subdomini	Explotació; Protecció de la informació
Mesures	op.exp.11.1; mp.info.4.1
Sistemes afectats	EACAT

Observacions

Pel que fa al CAOC, pel sistema EACAT, s'ha identificat que no es disposa d'un procediment ni normativa de signatura electrònica. Addicionalment, tot i que es realitza de manera operativa, no es disposa d'un procediment per a la protecció de les claus criptogràfiques ni es disposa d'un procediment de generació de certificats digitals.

Recomanacions

El CAOC, ha de disposar d'un procediment de signatura electrònica i segellat de temps que identifiqui la informació que hagi de prevenir la possibilitat de repudi posterior i que sigui susceptible de ser utilitzada com a evidència electrònica en el futur. Addicionalment el procediment ha d'indicar els algorismes criptogràfics emprats i indicar, si s'escau, les mesures compensatòries suficients en cas d'utilitzar altres mesures alternatives.

Per altra banda, ha de disposar d'un procediment de protecció de claus criptogràfiques que indiqui que s'han de protegir durant tot el seu cicle de vida (generació, transport al punt d'explotació, custòdia durant l'explotació, arxivament posterior a la seva retirada d'explotació activa i destrucció final), assegurant el següent:

- Els mitjans de generació han d'estar aïllats dels mitjans d'explotació.
- Les claus retirades d'operació que hagin de ser arxivades, ho han de ser en mitjans aïllats dels d'explotació.

R.13: Monitorització del sistema

Subdomini	Monitorització del sistema
Mesures	op.mon.2.1
Sistemes afectats	EACAT
Observacions	
Pel que fa al CAOC, tot i que es disposi d'una anàlisi de riscos del sistema EACAT, incloent indicadors de risc, amb la informació proporcionada no s'ha pogut assegurar que s'hagi documentat un procediment per a la gestió d'aquests indicadors, així com la freqüència d'addició o eliminació dels mateixos.	
Recomanacions	
Pel que fa al CAOC, s'ha de disposar d'un procediment per a la gestió d'indicadors que contempli el següent: • L'assignació de la responsabilitat en la definició d'indicadors i la freqüència en l'addició o eliminació d'aquests. • L'objectiu que es pretén mesurar. • L'origen de la informació, el procediment de recollida i tractament de les dades, la freqüència de recollida de dades. • La presentació de resultats o els criteris de valoració de l'indicador a efectes de reaccionar i prendre decisions.	

R.14: Deures i obligacions del personal

Subdomini	Gestió del personal; Protecció dels equips
Mesures	mp.per.2; mp.eq.1.1
Sistemes afectats	EACAT

Observacions

Pel que fa al CAOC, s'ha identificat que no es disposa d'un procediment que indiqui que els llocs de treball han de romandre endreçats. A més, s'ha identificat que no es disposa d'un procediment en el qual s'especifiqui:

- Com informar cada titular d'un lloc de treball dels deures i responsabilitats en matèria de seguretat.
- Els deures i responsabilitats en matèria de seguretat del lloc de treball.
- La necessitat d'acceptació de deures i responsabilitats signades pel personal.

Pel que fa al prestador de serveis d'aplicació Opentrends, amb la informació proporcionada no es pot assegurar que es disposi:

- D'una normativa on s'especifiquin els deures i obligacions del personal contractat a través d'un tercer i que aquesta es trobi reflectida en el contracte amb el tercer.
- D'un procediment que defineixi la resolució d'incidents relacionats amb l'incompliment de les obligacions per part del personal del tercer.

Recomanacions

Pel que fa al CAOC, ha de disposar d'una política o normativa documentada que indica que els llocs de treball han de romandre endreçats, sense més material sobre de la taula què el requerit per a l'activitat que s'està realitzant en cada moment. A més, aquesta política 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.
Tanmateix, s'indica que els documents de nivell mitjà de seguretat es guardaran en un lloc tancat quan no s'estiguin utilitzant.

A més, el CAOC i el prestador de serveis d'aplicació Opentrends, han d'informar a cada persona que treballi en el sistema dels deures i responsabilitats del seu lloc de treball en matèria de seguretat. Així doncs:

- S'han d'especificar les mesures disciplinàries que siguin procedents.
- S'ha de cobrir tant el període durant el qual s'exerceix el lloc com les obligacions en cas de finalització de l'assignació, o trasllat a un altre lloc de treball.
- S'ha de preveure el deure de confidencialitat respecte de les dades a què tingui accés, tant durant el període que estigui adscrit al lloc de treball com posteriorment a la finalització.

En cas de personal contractat a través d'un tercer:

- S'han d'establir els deures i obligacions del personal.
- S'han d'establir els deures i obligacions de cada part.
- S'ha d'establir el procediment de resolució d'incidents relacionats amb l'incompliment de les obligacions.

R.15: Formació i conscienciació

Subdomini	Gestió del personal
Mesures	mp.per.3; mp.per.4
Sistemes afectats	EACAT

Observacions

Pel que fa al CAOC, s'ha identificat que no es disposa d'un pla de formació.

Pel que fa el prestador de serveis d'aplicació Opentrends, amb la informació proporcionada no es pot assegurar que es realitzin accions de conscienciació.

Recomanacions

El CAOC, ha de realitzar formacions periòdiques, d'acord amb el pla de formació establert. El pla de formació ha de contenir, com a mínim, els següents punts:

- Continguts formatius relatius a la configuració de sistemes.
- Continguts formatius relatius a la detecció i reacció a incidents.
- Continguts formatius relatius a la gestió de la informació en qualsevol suport en que es trobi, almenys en el que es refereix a emmagatzematge, transferència, còpia, distribució i destrucció.

Pel que fa el prestador de serveis d'aplicació Opentrends, han de dur a terme les accions necessàries per conscienciar regularment el personal sobre el seu paper i responsabilitat perquè la seguretat del sistema assoleixi els nivells exigits.
En particular, s'ha de recordar regularment:

- La normativa de seguretat relativa al bon ús dels sistemes.
- La identificació d'incidents, activitats o comportaments sospitosos que s'hagin de reportar per al seu tractament per personal especialitzat.
- El procediment de report d'incidents de seguretat, ja siguin reals o falses alarmes.

R.16: Manteniment i protecció d'equips

Subdomini	Protecció dels equips
Mesures	mp.eq.3.1
Sistemes afectats	EACAT
Observacions	
En quant al lloc de treball: • No es disposa d'un procediment documentat que especifiqui la necessitat de revisar periòdicament l'inventari de les estacions de treball. • No es realitza una revisió periòdica de l'inventari validant la possessió de l'equip corresponent per part del responsable indicat a l'inventari.	
Recomanacions	
Pel que fa al lloc de treball: • Ha de disposar d'un procediment documentat que requereixi, que a més de disposar d'un inventari d'equips portàtils, és necessari la seva revisió periòdica. • Ha de realitzar de forma periòdica un control físic de l'inventari dels equips portàtils.	

R.17: Desenvolupament segur i gestió del canvi

Subdomini	Protecció de les aplicacions informàtiques
Mesures	mp.sw.2.1
Sistemes afectats	EACAT
Observacions	
Pel que fa al prestador de serveis d'aplicació Opentrends, tot i que es disposa d'un procediment per l'elaboració i execució del pla de proves del sistema no s'especifica que les proves s'hagin de realitzar en un entorn aïllat a producció, ni que es poden utilitzar dades reals.	
Recomanacions	
El prestador de serveis d'aplicació Opentrends, ha d'assegurar que no es deteriora la seguretat d'altres components del servei. Així doncs, ha de disposar d'un pla de proves del sistema que inclogui el següent: • Les proves s'han de fer en un entorn aïllat (preproducció). • Les proves d'acceptació no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.	

07 ANNEXOS

7.1 ANNEX I: QUADRE DE RECOMANACIONS PER DOMINIS DE L'ENS

Els resultats obtinguts durant la revisió i que es detallen a continuació poden reflectir els següents nivells de compliment:

- La situació actual de l'entorn cobreix els requeriments necessaris per complir les mesures de seguretat de l'ENS.
- La situació actual de l'entorn cobreix parcialment els requeriments necessaris per a les mesures de seguretat de l'ENS.
- La situació actual de l'entorn no cobreix els requeriments necessaris per complir les mesures de seguretat de l'ENS.
- Aquesta mesura de seguretat de l'ENS no és d'aplicació per l'Organisme.

A més, s'indiquen les referències a les recomanacions (R) detallades en l'apartat *6.2 Debilitats o recomanacions detectades en l'auditoria ENS de la Fase III* del present informe.

		Nivells de les dimensions de seguretat		EACAT				
				D	A	I	C	T
				Baix	Baix	Baix	Baix	Baix
	Marc Organitzatiu							
Marc Organitzatiu	Baix	org.1	Política de seguretat	●				
	Baix	org.2	Normativa de seguretat	●				**R.01**
	Baix	org.3	Procediments de seguretat	●				**R.01; R.02; R.03**
	Baix	org.4	Procés d'autorització	●				**R.01; R.04; R.05**
	Planificació							
Marc Operacional	Baix	op.pl.1.1	Anàlisis de riscos	●				
	Mig	op.pl.1.2	Anàlisis de riscos	●				
	Alt	op.pl.1.3	Anàlisis de riscos	●				
	Baix	op.pl.2.1	Arquitectura de seguretat	●				
	Mig	op.pl.2.2	Arquitectura de seguretat	●				
	Alt	op.pl.2.3	Arquitectura de seguretat	●				
	Baix	op.pl.3	Adquisició de nous components	●				**R.06**
	Mig	op.pl.4	Dimensionament/Gestió de capacitats	●				
	Alt	op.pl.5	Components certificats	●				
	Control d'accés							
	Baix	op.acc.1	Identificació	●				**R.07; R.08**
	Baix	op.acc.2	Requisits d'accés	●				**R.07**
	Mig	op.acc.3	Segregació de funcions i tasques	●				
	Baix	op.acc.4	Procés de gestió de drets d'accés	●				**R.07**
	Baix	op.acc.5.1	Mecanisme d'autenticació	●				**R.07**
	Mig	op.acc.5.2	Mecanisme d'autenticació	●				
	Alt	op.acc.5.3	Mecanisme d'autenticació	●				
	Baix	op.acc.6.1	Accés local (local logon)	●				**R.07; R.08; R.09**
	Mig	op.acc.6.2	Accés local (local logon)	●				
	Alt	op.acc.6.3	Accés local (local logon)	●				
	Baix	op.acc.7.1	Accés remot (remote login)	●				
	Mig	op.acc.7.2	Accés remot (remote login)	●				

				EACAT				
			Nivells de les dimensions de seguretat	D	A	I	C	T
				Baix	Baix	Baix	Baix	Baix
Marc Operacional		**Explotació**						
	Baix	op.exp.1	Inventari d'actius					**R.10**
	Baix	op.exp.2	Configuració de seguretat					**R.11**
	Mig	op.exp.3	Gestió de la configuració					
	Baix	op.exp.4	Manteniment					
	Mig	op.exp.5	Gestió de canvis					
	Baix	op.exp.6	Protecció contra codi perjudicial					
	Mig	op.exp.7	Gestió d'incidents					
	Baix	op.exp.8.1	Registre de l'activitat dels usuaris					
	Mig	op.exp.8.2	Registre de l'activitat dels usuaris					
	Alt	op.exp.8.3	Registre de l'activitat dels usuaris					
	Mig	op.exp.9	Registre de la gestió d'incidents					
	Alt	op.exp.10	Protecció dels registres d'activitat					
	Baix	op.exp.11.1	Protecció de claus criptogràfiques					**R.12**
	Mig	op.exp.11.2	Protecció de claus criptogràfiques					
		Serveis Externs						
	Mig	op.ext.1	Contractació i acords de nivell de servei					
	Mig	op.ext.2	Gestió diària					
	Alt	op.ext.9	Mitjans alternatius					
		Continuïtat del Servei						
	Mig	op.cont.1	Anàlisis d'impacte					
	Alt	op.cont.2	Pla de continuïtat					
	Alt	op.cont.3	Proves periòdiques					
		Monitorització del sistema						
	Mig	op.mon.1	Detecció d'intrusió					
	Baix	op.mon.2.1	Sistema de mètriques					**R.13**
	Mig	op.mon.2.2	Sistema de mètriques					
	Alt	op.mon.2.3	Sistema de mètriques					

		Nivells de les dimensions de seguretat	EACAT D Baix	A Baix	I Baix	C Baix	T Baix
Mesures de protecció		**Protecció de les instal·lacions i infraestructures**					
	Baix	mp.if.1 Àrees separades i amb control d'accés	●				
	Baix	mp.if.2 Identificació de les persones	●				
	Baix	mp.if.3 Acondicionament dels locals	●				
	Baix	mp.if.4.1 Energia elèctrica	●				
	Mig	mp.if.4.2 Energia elèctrica	●				
	Baix	mp.if.5 Protecció contra incendis	●				
	Mig	mp.if.6 Protecció contra inundacions	●				
	Baix	mp.if.7 Registre d'entrada i sortida d'equipament	●				
	Alt	mp.if.9 Instal·lacions alternatives	●				
		Gestió del personal					
	Mig	mp.per.1 Caracterització del lloc de treball	●				
	Baix	mp.per.2 Deures i obligacions	●				**R.14**
	Baix	mp.per.3 Conscienciació	●				**R.15**
	Baix	mp.per.4 Formació	●				**R.15**
	Alt	mp.per.9 Personal alternatiu	●				
		Protecció dels equips					
	Baix	mp.eq.1.1 Lloc de treball endreçat	●				**R.14**
	Mig	mp.eq.1.2 Lloc de treball endreçat	●				
	Mig	mp.eq.2.1 Bloqueig de lloc de treball	●				
	Alt	mp.eq.2.2 Bloqueig de lloc de treball	●				
	Baix	mp.eq.3.1 Protecció d'equips portàtils	●				**R.16**
	Alt	mp.eq.3.2 Protecció d'equips portàtils	●				
	Mig	mp.eq.9 Mitjans alternatius	●				
		Protecció de les comunicacions					
	Baix	mp.com.1.1 Perímetre segur	●				
	Alt	mp.com.1.2 Perímetre segur	●				
	Mig	mp.com.2.1 Protecció de la confidencialitat	●				
	Alt	mp.com.2.2 Protecció de la confidencialitat	●				
	Baix	mp.com.3.1 Protecció de l'autenticitat i de la integritat	●				**R.03**
	Mig	mp.com.3.2 Protecció de l'autenticitat i de la integritat	●				
	Alt	mp.com.3.3 Protecció de l'autenticitat i de la integritat	●				
	Alt	mp.com.4 Segregació de xarxes	●				
	Alt	mp.com.9 Mitjans alternatius	●				

		Nivells de les dimensions de seguretat	EACAT D Baix	A Baix	I Baix	C Baix	T Baix
Mesures de protecció		Protecció dels suports d'informació					
	Baix	mp.si.1 Etiquetatge	●				
	Mig	mp.si.2.1 Criptografia	●				
	Alt	mp.si.2.2 Criptografia	●				
	Baix	mp.si.3 Custodia	●				
	Baix	mp.si.4 Transport	●			R.05	
	Baix	mp.si.5.1 Esborrament i destrucció	●				
	Mig	mp.si.5.2 Esborrament i destrucció	●				
		Protecció de les aplicacions informàtiques					
	Baix	mp.sw.1 Desenvolupament d'aplicacions	●				
	Baix	mp.sw.2.1 Acceptació i posada en servei	●			R.17	
	Mig	mp.sw.2.2 Acceptació i posada en servei	●				
	Alt	mp.sw.2.3 Acceptació i posada en servei	●				
		Protecció de la informació					
	Baix	mp.info.1 Dades de caràcter personal	●				
	Baix	mp.info.2.1 Qualificació de la informació	●				
	Mig	mp.info.2.2 Qualificació de la informació	●				
	Alt	mp.info.3 Xifrat	●				
	Baix	mp.info.4.1 Firma electrònica	●			R.12	
	Mig	mp.info.4.2 Firma electrònica	●				
	Alt	mp.info.4.3 Firma electrònica	●				
	Alt	mp.info.5 Segells de temps	●				
	Baix	mp.info.6 Neteja de documents	●				
	Baix	mp.info.9 Còpies de seguretat (backup)	●				
		Protecció dels serveis					
	Baix	mp.s.1 Protecció del correu electrònic	●			R.03	
	Baix	mp.s.2.1 Protecció de serveis i aplicacions web	●			R.03	
	Alt	mp.s.2.2 Protecció de serveis i aplicacions web	●				
	Mig	mp.s.8.1 Protecció contra la denegació de servei	●				
	Alt	mp.s.8.2 Protecció contra la denegació de servei	●				
	Alt	mp.s.9 Mitjans alternatius	●				

Aquesta pàgina s'ha deixat en blanc intencionadament.

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA