Document confidencial

Aquest full no ha de separar-se del document que l'acompanya

Informació important del document

- El personal del CESICAT no podrà enviar missatges des de bústies de correu NO CESICAT o GENCAT.
- L'enviament d'aquesta informació per correu electrònic cal fer-la, sempre que sigui possible, de forma xifrada, protegint la informació amb una paraula de pas.
- No està autoritzat enviar missatges a bústies de correu d'ús Personal (yahoo, gmail, etc.)
- Els destinataris de correus electrònics amb informació CONFIDENCIAL, sempre s'adreçaran a bústies nominals.
- Aquesta informació no pot ser enviada per correu electrònic a destinataris genèrics (no nominals).
- En cas que l'origen de l'enviament sigui una bústia NO NOMINAL, cal indicar sempre el nom de l'emissor.
- Mai es podrà enviar aquesta informació a un equip de fax "no atès" per la persona autoritzada. Es contactarà amb el receptor per confirmar la recepció.
- 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 pel CESICAT.
- S'ha de garantir que la informació en format paper estigui fora de l'abast de tercers no autoritzats.
- Per tractar la informació confidencial amb paper fora les oficines del CESICAT es requereix autorització del Director de l'Àrea.
- Cal utilitzar protocols segurs en cas d'enviament per xarxes de dades no segures.
- Els documents impresos s'han de recollir al moment, i no s'han de deixar ni oblidar a la safata de la impressora.
- En la divulgació d'aquesta informació se n'ha de garantir la integritat per evitar la modificació per part d'un tercer NO autoritzat.
- 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).
- 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, es recomana utilitzar destructora que impedeixi la seva recuperació o lectura.

Generalitat de Catalunya
Centre de Seguretat de la Informació de Catalunya

Informe de Diagnòstic de Compliment de l'Esquema Nacional de Seguretat (ENS) sobre el sistema eNotum del Consorci AOC

Juliol 2019

Generalitat de Catalunya
Centre de Seguretat de la Informació de Catalunya

Fitxa del document

Títol	Informe de Diagnòstic de Compliment de l'ENS sobre el sistema eNotum del Consorci AOC
Fitxer físic	CESICAT - Informe Diagnòstic de Compliment de l'ENS sobre eNotum-Consorci AOC_v1.doc

Versió	Redactat per	Revisat per	Aprovat per	Data aprovació
1.0	Servei Auditoria (CESICAT)	Àrea de Compliment Normatiu (CESICAT)	CESICAT	01/07/2019

Registre de canvis			
Versió	**Pàgines**	**Data de modificació**	**Motiu del canvi**
1.0	48	12/04/2019	Esborrany d'Informe de Diagnòstic
1.0	48	01/07/2019	Informe de Diagnòstic

Entitat Auditada: **Consorci Administració Oberta de Catalunya (AOC)**
Entitat Auditora: **CESICAT**

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, el Centre de Seguretat de la Informació de Catalunya (en endavant, CESICAT), tal i com indica l'Acord de Govern GOV/103/2012, com a entitat encarregada de planificar, gestionar i controlar la seguretat de les TIC de l'Administració de la Generalitat i el seu sector públic, portarà a terme un diagnòstic sobre el compliment de l'ENS.

En el present document es detallen els resultats del diagnòstic del servei eNotum del Consorci Administració Oberta de Catalunya (en endavant, Consorci AOC).

02 OBJECTIU I ABAST

L'objectiu d'aquest informe és expressar una opinió a partir del diagnòstic realitzat sobre el grau de compliment i nivell de maduresa per part del Consorci AOC 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. Degut a la naturalesa de sistema notificador de l'eNotum, també s'han tingut en compte els articles del Capítol IV sobre Comunicacions electròniques i Notificacions electròniques de l'ENS.

L'opinió reflectida en aquest document es refereix exclusivament a la situació de compliment a data 12 de febrer de 2019.

La conformitat dels sistemes d'informació amb tots els requisits establerts en l'Annex II del RD 3/2010 s'ha obtingut mitjançant les respostes proporcionades per tots els actors implicats en el present diagnòstic i que es detallen més endavant en l'apartat *4.2.1 Identificació dels controls i actors implicats*. 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.

L'eNotum és un sistema de notificacions electròniques que permet a la ciutadania, les empreses i les entitats rebre les notificacions oficials de la Generalitat de Catalunya per mitjans electrònics.

Els ciutadans accedeixen a l'eNotum mitjançant el Portal web Ciutadà. El personal de les diferents administracions que gestionen les notificacions i la pròpia aplicació ho fan mitjançant el Portal de gestió de l'eNotum (o Portlet de l'empleat). Per tal de poder signar les notificacions és necessari accedir a l'eNotum mitjançant certificat digital.

L'aplicació eNotum utilitza un servei propi de correu electrònic, gestionat pel prestador de serveis NTT, per realitzar les comunicacions de les notificacions. Així doncs, les mesures referides al correu electrònic s'han analitzat únicament per aquestes comunicacions.

En tractar-se d'una aplicació transversal només s'han tingut en compte les mesures relacionades amb la protecció dels equips dels usuaris del Consorci AOC gestors de l'aplicació eNotum.

Pel mateix motiu les mesures relacionades amb la protecció dels suports d'informació s'han analitzat únicament pels usuaris del Consorci AOC gestors de l'aplicació eNotum i pels usuaris administradors del CPD.

En el present diagnòstic s'han avaluat els aspectes de seguretat del Portal web Ciutadà i del Portal web de gestió de l'eNotum, de l'aplicació, la Base de Dades i els controls de seguretat associats a la infraestructura dels servidors i comunicacions que donen suport al sistema.

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

	Actors implicats						Categorització					
Sistema d'informació	**Org**	**CPD**	**APP**	**LLT**	**COM**	**SAU**	**D**	**A**	**I**	**C**	**T**	**Global sistema**
eNotum	Consorci AOC	NTT Mediacloud	Consorci AOC	Consorci AOC	NTT	Everis	Mig	Alt	Alt	Alt	Alt	Alt

Org: Organisme responsable **COM:** Comunicacions
APP: Aplicació **LLT:** Lloc de Treball
SAU: Servei d'Atenció a l'Usuari
CPD: Centre de Processament de Dades

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

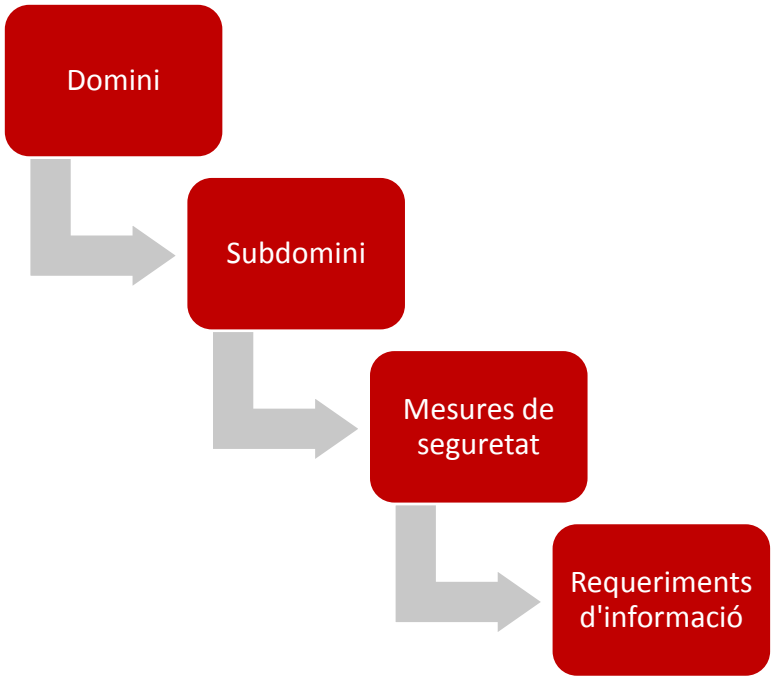
Les mesures de seguretat que es troben definides en l'Annex II de l'ENS es troben agrupades en els següents **tres dominis** i per cadascun d'ells en diversos subdominis de seguretat:

- **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 es centren en protegir actius concrets, segons la seva naturalesa i la qualitat exigida pel nivell de seguretat.

S'ha afegit un domini addicional als que recull l'Annex II de l'ENS, considerant els articles de l'ENS específics per a sistemes notificadors:

- **Comunicacions i Notificacions electròniques** que està format per requisits funcionals de seguretat que haurà de garantir un sistema de notificació electrònica.

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



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'ha de dur a terme determinades activitats, les responsabilitats i autoritzacions en l'us de les TIC.

   Aquests aspectes són requerits tant pel Consorci AOC, com pels prestadors dels serveis que intervenen en la seva operativa.

- ***Marc operacional:***

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

   Aquests aspectes són requerits al Consorci AOC, al responsable de l'Aplicació i al prestador de serveis de CPD.

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 finals, com dels que gestionen l'aplicació, així com dels usuaris administradors dels sistemes (prestador de serveis de CPD) amb accés a les Bases de Dades i a la configuració dels entorns de producció.

4. **Explotació:** Es tracten com a mesures destacables les següents: mesures de seguretat relacionades amb la gestió de la configuració del sistema, 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 al Consorci AOC, com als prestadors dels serveis que intervenen en la seva operativa.

5. **Serveis externs:** Fa referència als acords de nivell de servei definits amb els prestadors de serveis i els mecanismes establerts per vetllar pel compliment de les seves obligacions de servei.

   Aquests aspectes són requerits als prestadors dels serveis que intervenen en l'operativa del sistema.

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.

   Aquests aspectes són requerits al Consorci AOC.

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 al Consorci AOC 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 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 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 al Consorci AOC, al responsable de l'Aplicació i als prestadors de serveis de CPD i del SAU.

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

    Aquests aspectes són requerits al Consorci AOC.

11. **Protecció de les comunicacions:** S'enfoca a les mesures de seguretat 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 prestadors 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.

    Aquests aspectes són requerits al Consorci AOC i al 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 Consorci AOC.

14. **Protecció de la informació:** Hi ha establertes un conjunt de mesures de seguretat, 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 al Consorci AOC, com als prestadors de serveis de CPD i de Comunicacions.

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

    Aquests aspectes són requerits al Consorci AOC i als prestadors de serveis de CPD i Correu.

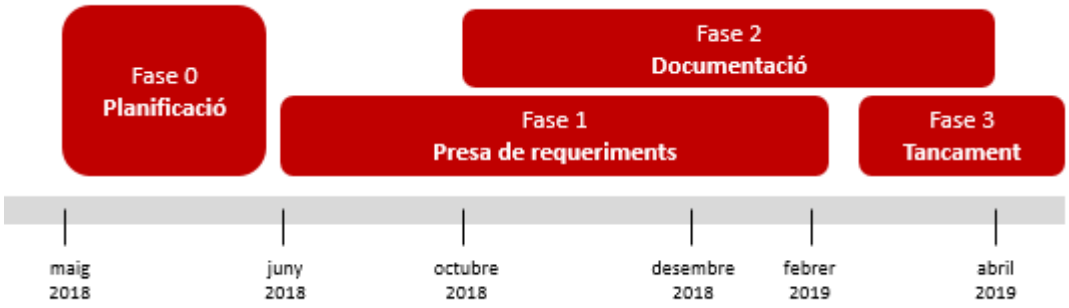
❖ ***Comunicacions i Notificacions electròniques:***

16. **Notificacions electròniques:** Es tracten els requisits funcionals de seguretat que haurà de garantir un sistema de notificació electrònica.

    Aquests aspectes són requerits al Consorci AOC.

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 maig de 2018 ha consistit en planificar el present dignostic i en definir el seu objectiu i abast.

4.2 Fase 1 – Presa de requeriments

La següent fase s'ha desenvolupat des del mes de juny al mes de febrer de 2019.

4.2.1 Identificació dels controls i actors implicats

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

- S'han identificat i analitzat els controls de l'ENS que apliquen a l'eNotum, 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.
- S'han identificat els controls de l'ENS específics per a sistemes de notificacions electròniques que estableix les obligacions de seguretat de la informació d'accés electrònic dels ciutadans als serveis públics en relació amb els sistemes de comunicacions electròniques emprats per les Administracions públiques.

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 del present disgnòstic es detallen a continuació:

- A partir de la identificació dels controls de l'ENS que apliquen a l'eNotum, s'han elaborat els qüestionaris de requeriments d'informació.
- S'han realitzat diverses reunions amb els responsables d'eNotum del Consorci AOC. En aquestes reunions, els interlocutors han donat resposta a les preguntes realitzades pels auditors en base als qüestionaris de requeriments. Tota la informació provinent de la resta de prestadors de serveis d'eNotum fora del Consorci AOC, ha estat requerida i facilitada a través dels interlocutors del Consorci AOC.

4.3 Fase 2 – Documentació

Aquesta fase s'ha desenvolupat durant el mes d'octubre de 2018 fins l'abril de 2019.

4.3.1 **Anàlisi de la informació**

Les tasques dutes a terme per poder realitzar l'anàlisi dels requeriments d'informació han estat les següents:

- S'ha desenvolupat i implementat un programa de treball per tal de poder realitzar adequadament el seguiment i l'anàlisi de les respostes obtingudes durant el diagnòstic.
- S'ha analitzat la informació tècnica rebuda per tal de validar-ne cadascuna de les mesures de seguretat establertes en l'apartat *4.2.1 Identificació dels controls i actors implicats*.
- Durant l'anàlisi de les respostes obtingudes en el present diagnòstic 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).
- S'ha determinat el grau de compliment de les mesures de seguretat de l'Annex II de l'ENS i els controls propis per sistemes de notificacions electròniques definits a l'ENS, a partir de les següents perspectives: la definició de procediments documentats i l'execució de procediments de forma operativa.

4.3.2 **Resultats**

El diagnòstic mostra el grau de compliment, grau de fiabilitat i nivell de maduresa agrupats per subdomini. Addicionalment, es mostra una visió del compliment de les mesures analitzades segons la seva naturalesa técnica i organitzativa.

4.3.2.1 **Grau de compliment**

El grau de compliment de les mesures de seguretat incloses en l'Annex II de l'ENS respecte el sistema d'informació definit en l'abast d'aquest diagnòstic, 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, els requeriments d'informació dels quals no s'ha obtingut resposta 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 de respostes obtingudes respecte a les sol·licitades, amb l'objectiu de tenir present en quina mesura les respostes 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) - Equema Nacional de Seguridad - Guía de Implantación'**

4.3.2.4 **Interpretació dels resultats**

Els resultats obtinguts en el present diagnòstic es mostren segons les següents perspectives:

- **Compliment del sistema**: Inclou els resultats agregats i per subdomini del compliment i la fiabilitat de les respostes rebudes.
- **Maduresa del sistema**: Recull el nivell de maduresa agregat i per subdomini.
- **Visió per mesures Tècniques/Organitzatives**: Anàlisi de compliment segons es tracti de mesures Tècniques o mesures Organitzatives 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 del present diagnòstic.

A l'apartat 6.2 i l'Annex II es mostra una anàlisi del compliment de les mesures de l'ENS segons la seva naturalesa Tècnica o Organitzativa.

Al punt 6.3 d'aquest document 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 detallada de les debilitats i recomanacions del sistema eNotum del Consorci AOC.

4.4 Fase 3 – Tancament

Aquesta fase, que s'ha desenvolupat des del mes de febrer al mes de abril de 2019, ha consistit en la el·laboració del present informe a partir dels resultats obtinguts en aquest diagnòstic.

05 **RESUM EXECUTIU**

En funció del treball realitzat i dels resultats obtinguts en el mateix, d'acord amb l'abast del present diagnòstic descrit en el capítol 2, es determina que, el **grau de compliment** de les mesures de seguretat previstes pels Reglaments de desplegament de l'ENS per part del Consorci AOC és del **70,4%,** el que suposa un **nivell de maduresa** del sistema eNotum de **2 sobre 5.**

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:

- En relació al *Marc Organitzatiu*, s'ha obtingut un grau de compliment del 100,0%. En aquest subdomini, els diferents actors implicats han donat resposta als requeriments d'informació plantejats a través del Marc Normatiu, els estàndards propis dels prestadors de serveis i els procediments de seguretat del Consorci AOC.
- Respecte als *Serveis Externs*, el grau de compliment assolit ha estat del 100,0%. En aquest cas, és important destacar que l'evolució i manteniment del sistema eNotum es gestiona internament, on els servidors del sistema són propietat del Consorci AOC, ubicats físicament a les instal·lacions de Mediacloud i el manteniment del maquinari i programari està subcontractat a NTT, complint aquests amb les mesures de seguretat requerides als prestadors de serveis externs pel que respecte a Contractació i Acords de Nivell de Servei, la gestió diària i els mitjans alternatius.
- Respecte a la *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 Mediacloud relatiu al CPD, 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 pel compliment de les normatives industrials relatives a la protecció contra incendis i el registre detallat de qualsevol entrada i sortida d'equipament.
- En relació als requeriments específics per *Notificacions Electròniques*, s'ha obtingut un grau de compliment del 100,0%. En aquest subdomini, el Consorci AOC ha donat resposta a les condicions tècniques de seguretat de les notificacions al ciutadà, habilitant els mecanismes necessaris per permetre que la persona interessada conegui d'una manera efectiva la recepció de les notificacions, se n'acrediti el consentiment de la seva recepció per mitjà electrònic, s'enregistrin les dates de posada a disposició i d'accés al contingut de les notificacions i se n'acrediti la recepció.
- Pel que fa a la *Protecció de les Comunicacions*, s'ha obtingut un grau de compliment del 93,3%. Respecte a aquest subdomini, s'ha observat que es disposa de les mesures necessàries en la gestió de les xarxes privades virtuals i d'una correcta segmentació de xarxes. Respecte a la gestió del perímetre segur, tot i disposar de tallafocs en cascada a nivell lògic, no es disposa de tallafocs de diferents fabricants disposats físicament en cascada. En referència a la prevenció d'atacs actius, tot i disposar dels mecanismes necessaris, no es disposa d'una normativa que especifiqui l'aplicació d'aquests mecanismes, la seva detecció i la conseqüent activació dels procediments previstos.

- Referent a la *Protecció dels Equips* dels Usuaris del Consorci AOC gestors de l'eNotum, el grau de compliment assolit ha estat del 91,0%. Aquest subdomini s'assoleix disposant de mitjans alternatius de protecció dels equips i de la validació de la seva entrada en funcionament, dels llocs de treball endreçats, sense material damunt la taula més enllà del requerit per a l'activitat que es realitza en cada moment, i del bloqueig de pantalla seguint les recomanacions del Marc Normatiu.

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

- Respecte a la *Continuïtat del Servei*, el grau de compliment obtingut ha estat del 0%. S'ha de tenir en compte que als sistemes classificats amb un grau mitjà de disponibilitat, com és el cas de l'eNotum, en aquest subdomini, l'ENS només requereix que es disposi d'una anàlisi d'impacte. En el present diagnòstic, s'ha identificat que no es disposa d'aquesta anàlisi, motiu pel qual el grau de compliment és d'un 0%.
- En relació al subdomini de *Planificació*, s'ha obtingut un grau de compliment del 33,9%. Malgrat que es disposa d'una correcta documentació de l'arquitectura de l'aplicació, de les instal·lacions i dels sistemes, s'ha identificat que no es disposa d'una anàlisi de riscos ni d'un procediment d'adquisició de nous components, així com no es realitza un estudi de dimensionament i anàlisi de la capacitat previ a la posada en producció de nous evolutius del sistema.
- En relació a la *Monitorització del Sistema* s'ha obtingut un grau de compliment del 42,7%. Respecte a aquest subdomini, s'ha detectat que no es disposa d'un procediment documentat per la gestió del monitoratge.
- Al subdomini de *Gestió del personal* el grau de compliment obtingut ha estat del 46,3%. S'ha identificat que el Consorci AOC no disposa d'un pla de formació, així com d'un pla de conscienciació. D'altra banda, el prestador de serveis NTT del CPD no disposa d'un pla de formació.
- Respecte al subdomini d'*Explotació* s'ha obtingut un grau de compliment del 57,7%. En referència al CPD, s'ha identificat que no es disposa d'antivirus instal·lat als servidors. També s'ha observat que no es realitza una correcta gestió de les traces d'activitat dels usuaris. D'altra banda, s'ha identificat que no es disposa d'un control que sol·liciti i enregistri l'acceptació de l'usuari en accedir a accions que poden posar en risc el sistema. Així mateix, no es disposa d'un procediment que identifiqui aquestes situacions de risc. Tampoc s'estan realitzant validacions funcionals i de seguretat abans de l'entrada a producció.
- Respecte al subdomini de *Protecció de la Informació*, s'ha obtingut un grau de compliment del 63,3%. Les principals no conformitats identificades estan relacionades amb el xifrat de la informació i, tot i que es fa servir la signatura electrònica i el segell de temps, no es disposa d'un procediment que identifiqui la informació a signar i segellar electrònicament.

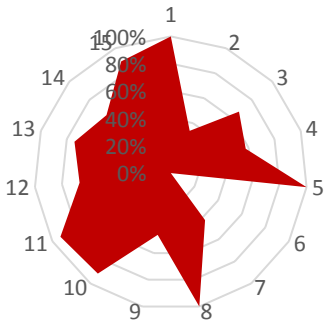
En l'apartat 6 d'aquest document es detallen els incompliments totals o parcials identificats en el present diagnòstic, així com les recomanacions pertinents.

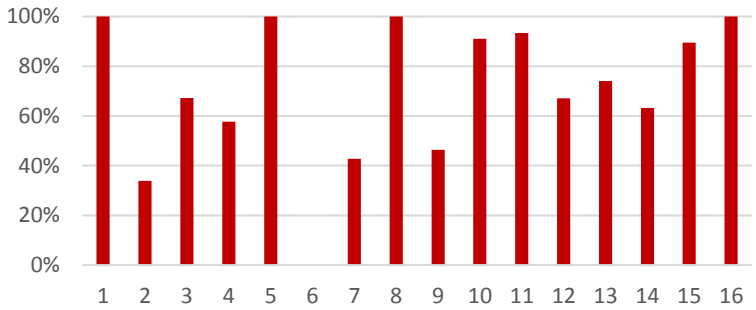
06 RESULTATS DEL DIAGNÒSTIC DE L'ENS DEL SISTEMA eNOTUM

6.1 Anàlisi del Compliment i Maduresa del sistema eNotum

eNotum		70,4%	100,0%
Marc organitzatiu		**Compliment**	**Fiabilitat**
1	Marc organitzatiu	100,0%	100,0%
Marc operacional		**Compliment**	**Fiabilitat**
2	Planificació	33,9%	100,0%
3	Control d'accés	67,2%	100,0%
4	Explotació	57,7%	100,0%
5	Serveis externs	100,0%	100,0%
6	Continuïtat del servei	0,0%	100,0%
7	Monitorització del sistema	42,7%	100,0%
Mesures de protecció		**Compliment**	**Fiabilitat**
8	Protecció de les instal·lacions i infraestructures	100,0%	100,0%
9	Gestió del personal	46,3%	100,0%
10	Protecció dels equips	91,0%	100,0%
11	Protecció de les comunicacions	93,3%	100,0%
12	Protecció dels suports d'informació	67,0%	100,0%
13	Protecció de les aplicacions informàtiques	74,1%	100,0%
14	Protecció de la informació	63,3%	100,0%
15	Protecció dels serveis	89,4%	100,0%
Comunicacions electróniques		**Compliment**	**Fiabilitat**
16	Notificacions electróniques	100,0%	100,0%

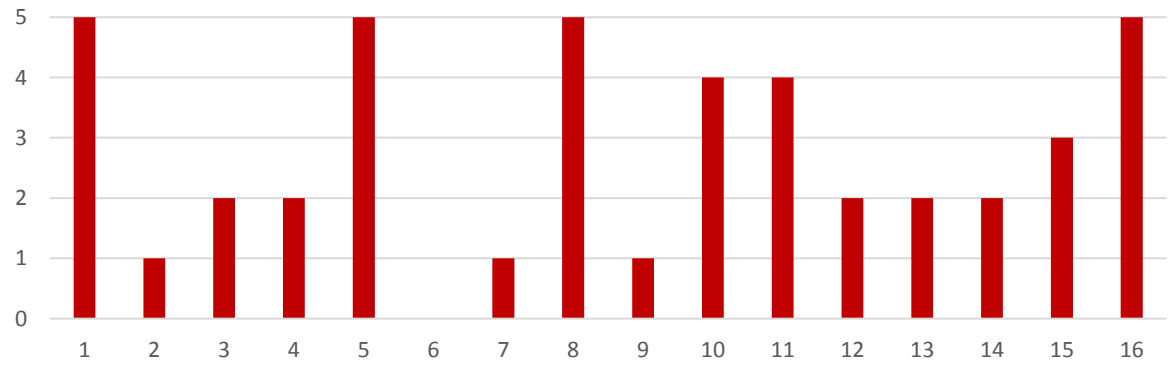
A continuació, es mostra de forma gràfica el grau de compliment del diagnòstic del sistema eNotum per subdomini.





eNotum		2
Marc organitzatiu		**Maduresa**
1	Marc organitzatiu	5
Marc operacional		**Maduresa**
2	Planificació	1
3	Control d'accés	2
4	Explotació	2
5	Serveis externs	5
6	Continuïtat del servei	0
7	Monitorització del sistema	1
Mesures de protecció		**Maduresa**
8	Protecció de les instal·lacions i infraestructures	5
9	Gestió del personal	1
10	Protecció dels equips	4
11	Protecció de les comunicacions	4
12	Protecció dels suports d'informació	2
13	Protecció de les aplicacions informàtiques	2
14	Protecció de la informació	2
15	Protecció dels serveis	3
Comunicacions electróniques		**Maduresa**
16	Notificacions electróniques	5

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



6.2 Visió per mesures Tècniques/Organitzatives

En aquest apartat es pot observar l'estudi del compliment de les mesures de l'ENS segons la seva naturalesa (Tècnica / Organitzativa).

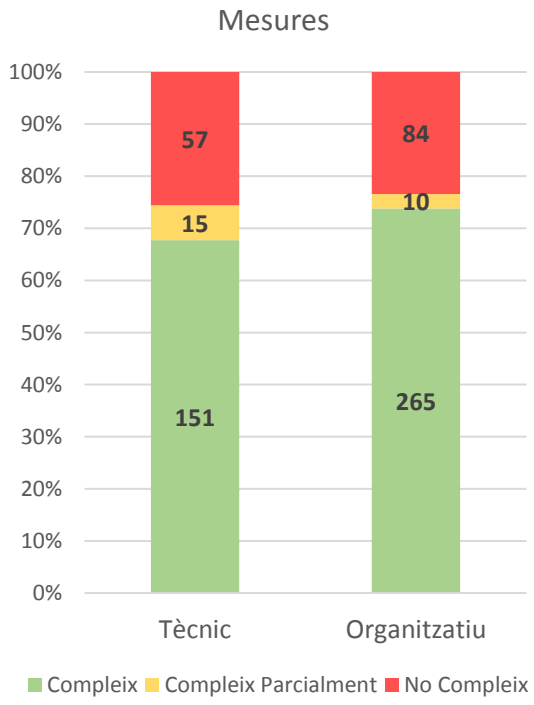
A la següent taula es mostra la distribució dels compliments segons:

- Mesures Tècniques: Mesures relacionades amb la configuració i parametrització d'actius tecnològics per garantir la seguretat de la informació.
- Mesures Organitzatives: Mesures relacionades amb l'organització global de la seguretat, incloent-hi polítiques, procediments, definició de processos i totes aquelles mesures que afectin a l'estructura i a la presa de decisions per garantir la seguretat de la informació.

	Compleix		Compleix Parcialment		No Compleix	
Global	416	71,48%	25	4,30%	141	24,23%
Tècnic	151	67,71%	15	6,73%	57	25,56%
Organitzatiu	265	73,82%	10	2,79%	84	23,40%

Addicionalment, en l'Annex II es troba detallat el resultat d'aquesta anàlisi, així com les recomanacions associades a cada un dels incompliments identificats i que es corresponen amb les relacionades a l'apartat *6.3 Debilitats i Recomanacions detectades en el diagnòstic del sistema eNotum.*

A continuació, es mostra un gràfic amb el nivell de compliments per tipologia de mesura:



6.3 Debilitats i Recomanacions detectades en el diagnòstic del sistema eNotum

R.01: Anàlisis de riscos

Subdomini	Planificació
Sistemes afectats	eNotum

Observacions

El Consorci AOC no ha realitzat una anàlisi de riscos del sistema.

Recomanacions

Cal disposar d'una anàlisi de riscos formal i aprovat per la Direcció, que tingui en compte els següents aspectes:

- Ha d'identificar i valorar qualitativament els actius més valuosos del sistema.
- Ha d'identificar i quantificar les amenaces possibles.
- Ha d'identificar les vulnerabilitats que habiliten aquestes amenaces.
- Ha d'identificar i valorar les salvaguardes que mitiguen aquestes amenaces i el seu nivell d'eficàcia.
- Ha d'identificar i valorar els riscos residuals.

Adicionalment, aquesta anàlisi ha de ser revisada anualment i aprovada per la Direcció.

R.02: Documentació dels controls tècnics interns

Subdomini	Planificació
Sistemes afectats	eNotum

Observacions

Pel que fa al sistema eNotum s'ha identificat que el Consorci AOC no disposa de documentació on es detallin els controls tècnics necessaris per a la validació de les dades d'entrada, sortida i dades intermèdies en l'intercanvi d'informacio amb altres sistemes, malgrat que sí que s'està aplicant un filtratge de caràcters no autoritzats en l'integració amb la base de dades.

Recomanacions

És necessari disposar d'un document que detalli com es controlen les dades en l'intercanvi d'informació amb altres sistemes (p.e. implantació de controls d'integritat de les dades) i una vegada dins dels sistemes (p.e. validant caràcters no autoritzats).

R.03: Adquisició de nous components

Subdomini	Planificació
Sistemes afectats	eNotum

Observacions

El Consorci AOC no disposa d'un procediment d'adquisició de nous components.

Recomanacions

S'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.04: Anàlisi, desenvolupament, acceptació i posada en servei

Subdomini	Planificació; Protecció de les aplicacions informàtiques
Sistemes afectats	eNotum

Observacions

S'identifica que a nivell d'aplicació el Consorci AOC, amb caràcter previ a la posada en explotació, no s'analitzen les necessitats de dimensionament. En concret, s'ha observat que:

- No es realitza un informe de dimensionament de l'aplicació.
- No es disposa d'un informe de proves de rendiment, qualitat i/o estrès de l'aplicació.
- No existeix un pla de proves de rendiment formalitzat.

Addicionalment, s'observa que pel que fa al desenvolupament de l'aplicació:

- Tot i que no es permet l'ús de dades reals en entorns no productius i que es disposa d'entorns separats per desenvolupament, no es disposa ni es fa ùs d'una metodologia de desenvolupament reconeguda.
- No existeix una política o normativa documentada respecte al disseny del sistema que contempli els mecanismes d'identificació i autenticació, així com els mecanismes de protecció de la informació tractada.
- Pel que fa a nous evolutius no es disposa d'un pla de proves prèvi a la seva pujada a producció.

Recomanacions

Amb caràcter previ a la posada en explotació, s'ha de realitzar un estudi previ documentat i pla de proves que cobreixi els aspectes següents:

- Necessitats de processament.
- Necessitats d'emmagatzematge d'informació: durant el processament i durant el període que s'hagi de retenir.
- Necessitats de comunicació.
- Necessitats de personal: quantitat i qualificació professional de forma adequada.
- Necessitats d'instal·lacions i mitjans auxiliars.

S'ha disposar d'una política o normativa de desenvolupament que indiqui que:

- El desenvolupament d'aplicacions s'ha de fer sobre un sistema diferent i separat del de producció, i no hi ha d'haver eines o dades de desenvolupament en l'entorn de producció.
- S'ha disposar i aplicar una metodologia de desenvolupament reconeguda que:
  - Prengui en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
  - Tracti específicament les dades utilitzades en proves.
  - Permeti la inspecció del codi font.
  - Inclogui normes de programació segura.
- Els elements següents han de ser part integral del disseny del sistema:
  - Els mecanismes d'identificació i autenticació.
  - Els mecanismes de protecció de la informació tractada.
  - La generació i el tractament de pistes d'auditoria.
- Les proves anteriors a la implantació o modificació dels sistemes d'informació no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.

D'altra banda, abans de passar a producció s'ha de comprovar el funcionament correcte de l'aplicació.

- S'ha de comprovar que:
  - Es compleixen els criteris d'acceptació en matèria de seguretat.
  - No es deteriora la seguretat d'altres components del servei.
- 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.

R.05: Procediments de control d'accés i gestió d'usuaris

Subdomini	Control d'accés; Proteció de la informació
Sistemes afectats	eNotum

Observacions

Pels usuaris del Consorci AOC gestors de l'eNotum, s'ha observat que no existeix un esquema de funcions i tasques en què es contemplin aquelles que són crítiques i incompatibles en una mateixa persona.

Pel que fa al prestador de serveis NTT del CPD, s'ha identificat que:

- L'accés al sistema es realitza amb usuaris genèrics, addicionalment la contrasenya no caduca.
- No es disposa, d'un acord de confidencialitat on es faci constar el lliurament dels identificadors al usuari.

D'altra banda, tant per als usuaris del Consorci AOC gestors de l'eNotum com per als usuaris administradors del prestador de serveis NTT del CPD, s'ha identificat que:

- No es disposa d'un procediment de gestió d'usuaris on s'indiqui quin és el procés d'alta, baixa o modificació, qui és el responsable de cada recurs i el responsable d'assignar les autoritzacions.
- S'ha identificat que no es no es realitza una revisió periòdica dels usuaris del sistema, on es comprovi que els usuaris donats de baixa de l'organització han estat bloquejats o eliminats.
- No es disposa d'un procediment d'accés local que especifiqui que el sistema no ha de revelar informació després d'un intent fallit, que el sistema ha d'informar sempre als usuaris de la data de l'últim accés i de les seves obligacions després d'accedir al sistema, que el sistema ha de tenir regulats els horaris d'accés i que ha d'haver-hi punts de renovació de l'autenticació durant la sessió dels usuaris.
- No es disposa de doble factor d'autenticació ni d'un procediment que ho específiqui.
- Les credencials han de ser obtingudes després d'un registre previ presencial o telemàtic usant un certificat electrònic.
- No es disposa d'un procediment on s'especifiqui els privilegis i permisos que han de tenir els usuaris en funció del seu rol i que aquests han de disposar dels mínims privilegis necessaris.

Recomanacions

Pels usuaris del Consorci AOC gestors de l'eNotum, el control d'accés s'haurà d'organitzar de forma que s'exigeixi la concurrència de dos o més persones per a realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per a poder realitzar alguna acció il·lícita. S'ha de disposar d'un document que especifiqui quines tasques es consideren crítiques i per tant, incompatibles en un mateix usuari.

Pel que fa als usuaris administradors del prestador de serveis NTT del CPD:

- En el cas que un usuari tingui diferents rols, s'ha de disposar d'identificadors únics per cada un dels rols de manera que sempre es pugui saber qui i quins drets d'accés es reben o es pugui saber qui o que ha fet l'usuari.
- S'ha de disposar d'un acord de confidencialitat on l'usuari reconegui que ha rebut les credencials d'accés, conegui i accepti les obligacions que implica en relació a la confidencialitat i de les gestions a realitzar en cas de pèrdua.

D'altra banda, tant per als usuaris del Consorci AOC gestors de l'eNotum com per als usuaris administradors del prestador de serveis NTT del CPD:

- S'ha de disposar d'un procediment de gestió d'usuaris on s'indiqui quin és el procés d'alta, baixa o modificació i indiqui que només el personal amb la competència adequada podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, acord amb els criteris establerts pel responsable d'aquests.
- S'han de realitzar revisions periòdiques dels usuaris del sistema, on es comprovi que els usuaris donats de baixa de l'organització han estat bloquejats o eliminats. S'ha de disposar d'evidència sobre aquestes revisions.
- S'ha de disposar d'un procediment que indiqui:
  - Que el sistema no ha de revelar cap tipus d'informació després d'un intent fallit per part de l'usuari.
  - Que un cop l'usuari accedeix amb èxit al sistema, aquest l'ha d'informar de les seves obligacions i de la data de l'últim accés.
  - Que l'accés estigui limitat per horari, data i lloc des d'on s'accedeix.
  - S'ha de definir en quin punt el sistema requerirà una renovació de l'autenticació per part de l'usuari, mitjançant una identificació addicional a l'inicial, no sent suficient la secció establerta.
- S'ha de disposar i implantar un procediment d'autenticació que exigeixi l'ús d'almenys dos factors d'autenticació.
- Les credencials utilitzades hauran de ser obtingudes després d'un registre previ presencial o telemàtic mitjançant certificat electrònic.
- S'ha de disposar d'un procediment que indiqui que els privilegis dels usuaris s'hauran de reduir al mínim necessari per poder complir amb les seves obligacions.

R.06: Configuració de la seguretat

Subdomini	Explotació
Sistemes afectats	eNotum

Observacions

Pel que fa al sistema eNotum s'ha identificat que el Consorci AOC:

- No disposa d'un control que sol·liciti i enregistri l'acceptació de l'usuari en accedir a accions que poden posar en risc el sistema. Així mateix, no es disposa d'un procediment que identifiqui aquestes situacions de risc.
- No està portant a terme validacions funcionals i de seguretat abans de l'entrada a producció de nous evolutius del sistema.

Recomanacions

S'ha de disposar i implantar un procediment de seguretat on s'indiqui que s'han de configurar els equips prèviament a la seva entrada en operació, de forma que s'ha d'aplicar la regla de 'seguretat per defecte':

- Les mesures de seguretat han de ser respectuoses amb l'usuari i protegir-lo, llevat que s'exposi conscientment a un risc.
- Si és necessari executar accions que poden suposar un risc per la seguretat, l'usuari ha d'acceptar de forma expressa una advertència del sistema i aquesta ha de quedar enregistrada.
- L'ús natural, en els casos que l'usuari no ha consultat el manual, és un ús segur.

D'altra banda, per l'entrada en operació de nous evolutius del sistema, s'han de configurar els equips i fer les validacions oportunes per part dels usuaris gestors del sistema, validant que:

- Es retirin comptes genèrics o estàndard.
- S'ha d'aplicar la regla de "mínima funcionalitat":
  - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització assoleixi els seus objectius i cap altra funcionalitat.
  - No ha de proporcionar funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, de manera que es redueixi el seu perímetre al mínim imprescindible.
  - S'han d'eliminar o desactivar mitjançant el control de la configuració les funcions que no siguin d'interès, no siguin necessàries, i fins i tot les que siguin inadequades al fi que es persegueix.

R.07: Canvis al sistema

Subdomini	Explotació
Sistemes afectats	eNotum

Observacions

Al Consorci AOC, no s'està executant un procediment de gestió de canvis que evaluï si els potencials canvis al sistema poden provocar una situació de risc.

Recomanacions

S'ha de mantenir un control continu de canvis realitzats en el sistema, de forma que:

- Tots els canvis anunciats pel fabricant o proveïdor s'han d'analitzar per determinar-ne la conveniència per ser incorporats o no.
- Abans de posar en producció una nova versió o una versió apedaçada, s'ha de comprovar en un equip que no estigui en producció que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per a la feina diària. L'equip de proves ha de ser equivalent al de producció en els aspectes que es comproven.
- Els canvis s'han de planificar per reduir l'impacte sobre la prestació dels serveis afectats.
- Mitjançant anàlisis de riscos s'ha de determinar si els canvis són rellevants per a la seguretat del sistema. Els canvis que impliquin una situació de risc de nivell alt s'han d'aprovar explícitament de forma prèvia a la implantació.

R.08: Protecció contra codi maliciós

Subdomini	Explotació; Monitorització del sistema
Sistemes afectats	eNotum

Observacions

Pel que fa al prestador de serveis NTT del CPD, malgrat que es disposa de Firewall operatiu, a nivell d'eines de detecció o prevenció d'intrusió, s'indica que no s'ha instal·lat programari d'antivirus.

Recomanacions

S'ha de disposar de mecanismes de prevenció enfront de codi maliciós (virus, cucs, troians...) a tots els equips i s'ha de disposar d'un procediment que defineixi la monitorització i la reacció enfront a la detecció de codi maliciós. S'ha d'assegurar que al mecanisme de prevenció instal·lat se li aplica la configuració i actualització amb la frequencia recomanada pel fabricant.

R.09: Gestió de traces d'activitat d'usuaris

Subdomini	Explotació
Sistemes afectats	eNotum

Observacions

Pel que fa al prestador de serveis NTT del CPD i a l'aplicació, s'identifica que no es disposa d'un registre de traces d'activitat dels usuaris.

Recomanacions

Tant per l'activitat dels usuaris de l'aplicació com per l'activitat dels usuaris administradors del CPD, s'han de registrar les activitats d'aquests usuaris, de manera que:

- El registre ha d'indicar qui fa l'activitat, quan la fa i sobre quina informació.
- S'ha d'incloure l'activitat dels usuaris i, especialment, la dels operadors i administradors quan puguin accedir a la configuració i actuar en el manteniment del sistema.
- S'han de registrar les activitats efectuades amb èxit i els intents fracassats.
- La determinació de quines activitats s'han de registrar i amb quins nivells de detall s'ha d'adoptar en vista de l'anàlisi de riscos feta sobre el sistema.
- S'han d'activar els registres d'activitat en els servidors.
- S'ha de disposar d'un sistema automàtic de recol·lecció de registres i correlació d'esdeveniments; és a dir, una consola de seguretat centralitzada.

S'han de protegir els registres d'activitat, de forma que:

- S'ha de determinar el període de retenció dels registres.
- S'ha d'assegurar la data i hora.
- Els registres no poden ser modificats ni eliminats per personal no autoritzat.
- Les còpies de seguretat, si n'hi ha, s'han d'ajustar als mateixos requisits.

R.10: Continuïtat del servei

Subdomini	Continuïtat del servei
Sistemes afectats	eNotum

Observacions

No es disposa d'una anàlisi d'impacte que identifiqui requisits de disponibilitat i elements crítics per a la prestació del servei.

Recomanacions

S'ha de dur a terme una anàlisi d'impacte que permeti determinar:

- Els requisits de disponibilitat del servei mesurats com l'impacte d'una interrupció durant un cert període de temps. Entre aquests requisits es trobarà la identificació del temps màxim de dades que es considera tolerable perdre, el qual serà contemplat en la freqüència de les còpies de seguretat.
- Els elements que són crítics per a la prestació del servei siguin propis o proporcionats per tercers.

És recomanable disposar d'un procediment per la gestió d'aquesta anàlisi d'impacte on es contempli el responsable, la freqüència de revisió i l'actualització després de canvis als sistemes.

R.11: Indicadors del sistema de gestió de la seguretat de la informació

Subdomini	Monitorització del sistema
Sistemes afectats	eNotum

Observacions

A nivell del Consorci AOC, malgrat es disposa d'alguns d'indicadors, no s'han definit els indicadors per mesurar la seguretat del sistema ni s'ha documentat un procediment per a la gestió d'aquest indicadors.

Recomanacions

Al Consorci AOC, s'han de recopilar les dades necessàries atenent la categoria del sistema per establir un conjunt d'indicadors que mesuri el sistema en matèria de seguretat, en els aspectes següents:

- Grau d'implantació de les mesures de seguretat.
- Eficàcia i eficiència de les mesures de seguretat.
- Impacte dels incidents de seguretat.

Per gestionar aquest conjunt d'indicadors, s'ha de disposar d'un procediment que contempli:

- 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.12: Formació, conscienciació i gestió del personal

Subdomini	Gestió del personal; Protecció dels suports d'informació; Protecció de la informació
Sistemes afectats	eNotum

Observacions

Pel que fa al Consorci AOC no es disposa de pla de conscienciació.
Tant per al Consorci AOC com pel prestador de serveis de CPD NTT no es disposa de pla de formació.

Recomanacions

S'han de dur a terme les accions necessàries per conscienciar regularment al 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 pel personal especialitzat.
- El procediment per reportar els esdeveniments de seguretat.

Tant per al Consorci AOC, com per al prestador de serveis NTT del CPD, s'ha de formar regularment al personal en les matèries que siguin necessàries per a l'exercici de les seves funcions en materia de seguretat, en particular pel que fa a:

- Configuració de sistemes.
- Detecció i reacció a incidents.
- Gestió de la informació en qualsevol suport en que es trobi. S'han de cobrir almenys les activitats d'emmagatzematge, transferència, còpies, distribució i destrucció.
- S'ha d'incloure dins del pla formatiu, la formació necessària per tal que el personal pugui entendre el significat de les etiquetes, bé mitjançant una simple inspecció o bé recorrent a un repositori que ho expliqui.

R.13: Accés remot

Subdomini	Protecció dels equips
Sistemes afectats	eNotum

Observacions

S'ha observat que els equips dels usuaris del Consorci AOC gestors de l'eNotum:

- No es disposa d'un procediment documentat que especifiqui les mesures de seguretat que han de complir els equips que abandonin les instal·lacions de l'organització.
- No es disposa de mecanismes per detectar de manipulació dels equips portàtils.

Recomanacions

En relació al usuaris del Consorci AOC gestors de l'eNotum:

- S'ha de disposar d'un procediment en el que es descrigui com protegir adequadament els equips que siguin susceptibles de sortir de les instal·lacions de l'organització i no es puguin beneficiar de la protecció física corresponent, amb un risc manifest de pèrdua o robatori. S'han d'adoptar i documentar al procediment les següents messures:
  - S'ha de portar un inventari d'equips portàtils juntament amb una identificació de la persona que n'és responsable i un control regular del fet que està positivament sota el seu control.
  - S'ha d'establir un canal de comunicació per informar, el servei de gestió d'incidents, de pèrdues o sostraccions.
  - Quan un equip portàtil es connecti remotament a través de xarxes que no estan sota el control estricte de l'organització, l'àmbit d'operació del servidor ha de limitar la informació i els serveis accessibles als mínims imprescindibles, i s'ha de requerir una autorització prèvia dels responsables de la informació i els serveis afectats. Aquest punt és aplicable a connexions a través d'Internet i altres xarxes que no siguin de confiança.
  - S'ha d'evitar, en la mesura en què sigui possible, que l'equip contingui claus d'accés remot a l'organització. Es consideren claus d'accés remot les que siguin capaces d'habilitar un accés a altres equips de l'organització, o altres de naturalesa anàloga.
- S'ha de dotar el dispositiu de mecanismes que permetin saber si l'equip ha estat manipulat i activin els procediments previstos de gestió de l'incident.

R.14: Xifrat de la informació i signatura electrònica

Subdomini	Protecció de les comunicacions; Protecció de la informació
Sistemes afectats	eNotum

Observacions

Pel que fa al sistema eNotum s'han identificat les següents deficiències:

- No es xifra ni es disposa d'un procediment que indiqui quina informació emmagatzemada cal xifrar.
- Tot i que sí que s'empra la signatura electrònica i segells de temps, no s'adjunten les dades de verificació i validació de la signatura electrònica.
- Addicionalment no es disposa d'un document formalitzat en el que s'indiqui la informació que cal signar i segellar elèctrònicament.

En relació a les Comunicacions s'han observat les següents mancances:

- Els tallafocs es disposen en cascada a nivell lògic, però no a nivell físic i són tots del mateix fabricant.
- No es disposa d'una política o normativa documentada que especifiqui l'aplicació de mecanismes de prevenció d'atacs actius, la seva detecció i la consegüent activació dels procediments previstos.

Recomanacions

Pel que fa al sistema eNotum:

- S'ha de xifrar la informació i disposar d'una política o normativa documentada que indiqui que la informació amb un nivell alt de confidencialitat es xifra tant durant el seu emmagatzematge com durant la seva transmissió. Aquesta política o normativa ha d'indicar que la informació amb un nivell alt de confidencialitat només pot estar en clar mentre s'està fent ús. Addicionalment, s'ha de disposar d'un procediment documentat que determini la informació a xifrar en funció de la seva classificació i el medi en el qual s'emmagatzema.

- En referència a la signatura electrònica:
  - S'ha de garantir la verificació i validació de la signatura electrònica durant el temps requerit per l'activitat administrativa que aquesta suporti, sens perjudici que es pugui ampliar aquest període d'acord amb el que estableixi la política de signatura electrònica i de certificats que sigui aplicable.
  - S'ha d'adjuntar a la signatura o s'ha de referenciar tota la informació pertinent a la seva verificació i validació: Certificats i Dades de verificació i validació.
  - L'organisme que sol·liciti documents signats per l'administrat ha de verificar i validar la signatura rebuda en el moment de la recepció, i ha d'annexar o referenciar sense ambigüitat els Certificats i Dades de verificació i validació esmentats al punt anterior.
  - La signatura electrònica de documents per part de l'Administració ha d'annexar o referenciar sense ambigüitat els Certificats i Dades de verificació.

- Cal 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.

En concret per les Comunicacions:

- El sistema de tallafocs ha de disposar de sistemes redundats i cada sistema ha de constar de dos o més equips de diferent fabricant disposats en cascada.
- S'ha de disposar d'una política o normativa documentada de Protecció de l'Autenticitat i Integritat de les Comunicacions que especifiqui l'ús de mecanismes de prevenció d'atacs actius, garantint la seva detecció i la consegüent activació dels procediments previstos de tractament de l'incident. Considerant atacs actius, l'alteració de la informació en trànsit, la injecció d'informació espúria o el segrest de la sessió per una tercera part.

R.15: Protecció dels suports d'informació

Subdomini	Protecció dels suports d'informació; Protecció de la informació
Sistemes afectats	eNotum

Observacions

Pel que fa al Consorci AOC:

- No es disposa de procediment ni es fan servir mecanismes criptogràfics de protecció dels suports d'informació per garantir la confidencialitat i la integritat de la informació continguda.
- No es realitza ni es disposa d'un procediment per controlar l'entrada/sortida de suports d'informació.
- No es contempla dins del pla formatiu, la formació referent a com etiquetar i com interpretar les etiquetes dels suports d'informació.

Pel que fa al prestador de serveis NTT del CPD:

- No es disposa d'algoritmes certificats en el xifratge de la informació.
- Tot i que es disposa d'un registre de sortides de suports, no es disposa ni del control ni del procediment d'entradas/sortides on es registri el responsable d'aquestes i on es realitzi una comparació d'aquests moviments d'entrada i sortida per detectar possibles incidents.
- No es disposa d'un procediment formalitzat d'etiquetatge dels suports d'informació.

Tant el Consorci AOC com el prestador de serveis NTT del CPD, no es disposa de les suficients mesures físiques i/o lògiques en la custòdia dels suports d'informació.

Recomanacions

Pel que fa al Consorci AOC:

- S'ha de disposar i implantar un procediment formalitzat que indiqui l'ús de mecanismes criptogràfics acreditats que garanteixin la confidencialitat i integritat de la informació continguda a tots els dispositius removibles i que aquests mecanismes han d'utilitzar productes degudament certificats.
- És necessari disposar i implantar un procediment formalitzat de les entrades i sortides dels suports d'informació, on consti que:
  - S'ha de disposar d'un registre de sortida que identifiqui el transportista que rep el suport per traslladar-lo.
  - S'ha de disposar d'un registre d'entrada que identifiqui el transportista que el lliura.
  - S'ha de disposar d'un procediment rutinari que compari les sortides amb les arribades i dispari les alarmes pertinents quan es detecti algun incident.
  - S'han d'utilitzar els mitjans de protecció criptogràfica corresponents al nivell de qualificació de la informació continguda amb un nivell més alt.
- Tal com s'ha indicat a la recomanació R.12, s'ha d'incloure dins del pla formatiu, la formació necessària per tal que el personal pugui interpretar el significat de les etiquetes dels suports d'informació, bé mitjançant una simple inspecció o bé recorrent a un repositori que ho expliqui.

Pel que fa al prestador de serveis NTT del CPD:

- Ha de garantir l'ús de mecanismes criptogràfics degudament certificats que garanteixen la confidencialitat i integritat de la informació continguda a tots els suports d'informació.
- Cal fer un control exhaustiu de les entrades i sortides dels suports d'informació, tot i disposar d'un procediment de transport, s'ha de disposar d'un control que identifiqui els transportistes encarregats de les sortides i/o entrades de suports, així com disposar d'un procediment rutinari que compari les sortides amb les entrades i dispari les alarmes pertinents quan es detecti algun incident.
- Cal disposar d'un procediment formalitzat per a l'etiquetatge dels suports d'informació, tant els que romanen en les ubicacions de l'organització com els que surtin a altres destinacions especificant:
  - El responsable de l'etiquetatge.
  - Que l'etiquetatge no ha de revelar el contingut.
  - Que l'etiquetatge ha d'indicar el nivell de seguretat de la informació continguda de més qualificació, però de manera que no sigui comprensible per a algú aliè al sistema.
  - La forma de difondre aquesta informació al personal de forma que els usuaris puguin entendre el significat de les etiquetes.

Pel que fa tant al CPD com al Consorci AOC, s'han d'aplicar les mesures de seguretat sobre els suports d'informació que estan sota la seva responsabilitat de forma que es garanteixi el control d'accés amb mesures físiques i/o lògiques, com per exemple control d'accés físic amb controls d'entrades i sortides a les zones de custòdia dels suports o zones separades respecte a les zones de custòdia i les zones d'operació.

R.16: Protecció dels serveis i correu electrònic

Subdomini	Protecció dels serveis
Sistemes afectats	eNotum

Observacions

Pel que fa al servei de correu electrònic de l'aplicatiu eNotum, no disposa de les següents mesures per protegir-se enfront d'amenaces:

- No es disposa de protecció davant de l'encaminament de missatges i establiment de connexions.
- No es disposa d'un sistema de monitoratge de les amenaces detectades per les eines d'antivirus o antispam.

Pel que fa al prestador de serveis NTT del CPD, no es disposa de mecanisme per impedir atacs de manipulació de "proxys" o "caché", ni de les mesures suficients per evitar l'accés a informació obviant l'autenticació necessària.

Recomanacions

Pel que fa al servei de correu electrònic de l'aplicatiu eNotum s'ha de protegir contra les amenaces que li són pròpies de la manera següent:

- 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 (p. ex, protegint el servidor de DNS i la seva configuració, impedint que l'usuari final modifiqui la configuració del compte de correu) i establiment de connexions (p. ex. impedint que l'usuari final pugui connectar-se a un servidor de correu que no sigui el corporatiu, -com pogués ser amb regles de tallafocs).

Pel que fa al prestador de serveis NTT del CPD:

- Quan la informació tingui algun tipus de control d'accés, s'ha de garantir la impossibilitat d'accedir a la informació obviant l'autenticació, en particular prenent mesures en els aspectes següents:
  - S'ha d'evitar que el servidor ofereixi accés als documents per vies alternatives al protocol determinat.
  - S'han de prevenir atacs de manipulació d'URL.
  - S'han de prevenir 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".
  - S'han de prevenir atacs d'injecció de codi.
- S'han de prevenir intents d'escalat de privilegis.
- S'han de prevenir atacs de "cross site scripting".
- S'han de prevenir atacs de manipulació de programes o dispositius que fan una acció en representació d'altres, coneguts en terminologia anglesa com a "proxies", i sistemes especials d'emmagatzematge d'alta velocitat, coneguts en terminologia anglesa com a "caches".

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

A més, s'indiquen les referències a les recomanacions tècniques detallades en l'apartat 6.3 del present informe.

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

				eNotum				
		Nivells de les dimensions de seguretat		D	A	I	C	T
				Mitja	Alt	Alt	Alt	Alt
Marc Operacional		Explotació						
	Baix	op.exp.1	Inventari d'actius	●				
	Baix	op.exp.2	Configuració de seguretat	●				**R.06**
	Mig	op.exp.3	Gestió de la configuració	●				
	Baix	op.exp.4	Manteniment	●				
	Mig	op.exp.5	Gestió de canvis	●				**R.07**
	Baix	op.exp.6	Protecció contra codi perjudicial	●				**R.08**
	Mig	op.exp.7	Gestió d'incidents	●				
	Baix	op.exp.8.1	Registre de l'activitat dels usuaris	●				**R.09**
	Mig	op.exp.8.2	Registre de l'activitat dels usuaris	●				**R.09**
	Alt	op.exp.8.3	Registre de l'activitat dels usuaris	●				**R.09**
	Mig	op.exp.9	Registre de la gestió d'incidents	●				
	Alt	op.exp.10	Protecció dels registres d'activitat	●				**R.09**
	Baix	op.exp.11.1	Protecció de claus criptogràfiques	●				
	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	●				**R.10**
	Alt	op.cont.2	Pla de continuïtat	●				
	Alt	op.cont.3	Proves periòdiques	●				
		Monitorització del sistema						
	Mig	op.mon.1	Detecció d'intrusió	●				**R.08**
	Baix	op.mon.2.1	Sistema de mètriques	●				**R.11**
	Mig	op.mon.2.2	Sistema de mètriques	●				
	Alt	op.mon.2.3	Sistema de mètriques	●				**R.11**

				eNotum				
	Nivells de les dimensions de seguretat			D	A	I	C	T
				Mitja	Alt	Alt	Alt	Alt
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	●				
	Baix	mp.per.3	Conscienciació	●				**R.12**
	Baix	mp.per.4	Formació	●				**R.12**
	Alt	mp.per.9	Personal alternatiu	●				
		Protecció dels equips						
	Baix	mp.eq.1.1	Lloc de treball endreçat	●				
	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.13**
	Alt	mp.eq.3.2	Protecció d'equips portàtils	●				**R.13**
	Mig	mp.eq.9	Mitjans alternatius	●				
		Protecció de les comunicacions						
	Baix	mp.com.1.1	Perímetre segur	●				
	Alt	mp.com.1.2	Perímetre segur	●				**R.14**
	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.14**
	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		D	A	I	C	T
				Mitja	Alt	Alt	Alt	Alt
Mesures de protecció		Protecció dels suports d'informació						
	Baix	mp.si.1	Etiquetado	●		**R.12, R.15**		
	Mig	mp.si.2.1	Criptografia	●		**R.15**		
	Alt	mp.si.2.2	Criptografia	●		**R.15**		
	Baix	mp.si.3	Custodia	●		**R.15**		
	Baix	mp.si.4	Transport	●		**R.15**		
	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	●		**R.04**		
	Baix	mp.sw.2.1	Acceptació i posada en servei	●		**R.04**		
	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	●		**R.05, R.12, R.14, R.15**		
	Alt	mp.info.3	Xifrat	●		**R.14**		
	Baix	mp.info.4.1	Firma electrònica	●		**R.14**		
	Mig	mp.info.4.2	Firma electrònica	●		**R.14**		
	Alt	mp.info.4.3	Firma electrònica	●		**R.14**		
	Alt	mp.info.5	Segells de temps	●		**R.14**		
	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.16**		
	Baix	mp.s.2.1	Protecció de serveis i aplicacions web	●		**R.16**		
	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	●				
Notif.electrón		Notificacions electróniques						
	Baix	Art.31	Condicions tècniques de seguretat de les comunicacions electròniques	●				
	Baix	Art.32	Requeriments tècnics de notificacions i publicacions electròniques	●				

7.2 Annex II: Visió per mesures Tècniques/Organitzatives

Informe_Diagnostic
_Tec-Org_eNotum_v

Generalitat de Catalunya
Centre de Seguretat de la Informació de Catalunya