
# Requisits Generals de Seguretat per a la contractació de Serveis i Productes TI i OT (dins del marc de l'ENS)

*Barcelona, març de 2024*
*Versió v1.0*

## Contingut

# 1 Introducció i objectius

Aquest document té com a objectiu informar dels requisits de seguretat que haurà de complir qualsevol servei i/o producte amb característiques IT o OT que es vulgui implantar a l'organització Hospital Clínic de Barcelona en compliment dels requisits exigits per l'Esquema Nacional de Seguretat (ENS en endavant).

# 2 Abast

Establir els criteris de seguretat necessaris per a garantir que tots els serveis i productes que necessitin ser desplegats o integrats a la corporació Hospital Clínic ho faci amb un nivell òptim de seguretat i garantint en la mesura de lo possible l'acompliment normatiu vigent.

El document pretén incloure la casuística de compliment com de no compliment de la legalitat vigent, en aquest cas respecte de l'ENS, de les diferents casuístiques.

Aquest document aplica a qualsevol procés de contractació o compra de productes i serveis IT/OT. En el cas de productes, es consideraran dins de l'abast tant els sistemes de TI com l'equipament OT (IoMT, IoT).

Entenem com a productes i serveis IT/OT (IoMT) tots aquells que:

- Es connecten a la xarxa de l'hospital Clínic (LAN/WAN/WIFI)
- Requereixen de la connexió telemàtica d'un professional/servei/sistema de l'hospital per a la realitzar activitat professional de l'hospital (producte/servei extern)

En el cas de la incorporació de productes, s'han de presentar les evidències d'acord amb l'opció d'acreditació escollida i aportar la documentació necessària que ho certifiqui.

# 3 Aspectes Generals de Seguretat per a Serveis

Davant del procés de contractació i incorporació d'un servei a l'àmbit d'IT o OT cal seguir en tot moment el principi de professionalitat, segons l'article 16 de l'ENS:

- La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.
- Les organitzacions que prestin serveis a l'Hospital Clínic de Barcelona han de comptar amb professionals qualificats i amb uns nivells idonis de gestió i maduresa en els serveis prestats.
- Es determinaran els requisits de formació i experiència necessària del personal per al desenvolupament del lloc de treball.

## *3.1 Requisits per a la contractació de Serveis d'Implantació d'Infraestructura i programari tant IT com OT*

En el cas de serveis, cal presentar Certificat de Conformitat amb l'ENS relatiu al servei que es pretén prestar amb la categoria d'acord amb la sol·licitud. Per defecte es sol·licitarà per a la provisió de serveis que sustentin les activitats principals del Clínic un certificat de nivell MITJÀ com a mínim.

Aquest requisit aplica a qualsevol implantació d'infraestructura d'IT i OT, com per exemple xarxes, emmagatzemament, servidors, dispositius de còpies de seguretat i altres elements d'infraestructura, aparells d'electromedicina o de manteniment. etc. Aplica tanmateix al desplegament d'elements de programari específics de suport a la infraestructura tecnològica o de suport a negoci.

**Detall de requisits de components subministrats a la contractació de Serveis On Premise**

Qualsevol component o producte subministrat dins el servei caldrà que compleixi els criteris indicats a l'apartat 4. Aspectes Generals de Seguretat per a Productes.

Addicionalment, El Clínic podrà requerir del proveïdor, a més a més del Certificat de Conformitat amb l'ENS del servei contractar, el detall de la Declaració d'Aplicabilitat i mesures utilitzades, per garantir que els components proveïts garanteixin els requisits de l'ENS.

### *3.2 Subcontractació*

L'entitat proveïdora del servei haurà de disposar d'una documentació que detalli clarament els elements que formen part de la cadena de subcontractació, així com implicacions derivades de qualsevol canvi o modificació que pugui patir algun esglaó d' aquesta cadena.
El proveïdor haurà d'assegurar que els sistemes d'informació de les empreses subcontractades són conformes amb l' ENS pel que fa als serveis que afectin al Clínic, per la qual cosa el contingut del present document resultarà així mateix d'aplicació a la cadena de subministrament del proveïdor.
En aquest sentit, el Clínic podrà requerir del prestador, a més de la corresponent Certificació de Conformitat amb l' ENS, el detall de la Declaració d' Aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries de vigilància utilitzades.

### *3.3 Requisits de serveis de Desenvolupament de Programari*

Es presenten els requisits específics per a aquest tipus de Servei, segons ENS, nivell MITJÀ com a mínim:

- Desenvolupament Mitjançant Metodologia de Desenvolupament de Programari Segur:

| mp.sw | Protecció de les aplicacions informàtiques | Dimensió | BAIX | MITJÀ | ALT |
|---|---|---|---|---|---|
| mp.sw.1 | Desenvolupament de programari | Categoria | n.a. | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 |

| | | | | | |
|---|---|---|---|---|---|
| mp.sw.2 | Acceptació i posada en servei | Categoria | aplica | + R1 | + R1 |

Requisits.

- [mp.sw.1.1] El desenvolupament d'aplicacions es realitzarà sobre un sistema diferent i separat del de producció, no havent d'existir eines o dades de desenvolupament en l' entorn de producció, ni dades de producció en el de desenvolupament.

Reforç R1-Mínim privilegi.

- [mp.sw.1.r1.1] Les aplicacions es desenvoluparan respectant el principi de mínim privilegi, accedint únicament als recursos imprescindibles per a la seva funció, i amb els privilegis que siguin indispensables.

Reforç R2-Metodologia de desenvolupament segur.

- [mp.sw.1.r2.1] S'aplicarà una metodologia de desenvolupament segur reconeguda que:

a) Tindrà en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
b) Inclourà normes de programació segura, especialment: control d'assignació i alliberament de memòria, desbordament de memòria (*overflow*).
c) Tractarà específicament les dades usades en proves.
d) Permetrà la inspecció del codi font.

S'haurà de tenir en compte la guia de Desenvolupament Segur del CCN quan es tractin de desenvolupaments Web "CCN-STIC-812 Guia de Seguretat en Entorns i Aplicacions Web" així com la guia relativa a desenvolupament segur "CCN-CERT Recomanacions sobre desenvolupament segur"

Reforç R3-Seguretat des del disseny.

- [mp.sw.1.r3.1] Els següents elements seran part integral del disseny del sistema:

a) Els mecanismes d' identificació i autenticació.
b) Els mecanismes de protecció de la informació tractada.
c) La generació i tractament de pistes d' auditoria.

Reforç R4-Dades de proves.

- [mp.sw.1.r4.1] Preferiblement, les proves prèvies a la implantació o modificació dels sistemes d' informació no es realitzaran amb dades reals. En cas que fos necessari recórrer a dades reals es garantirà el nivell de seguretat corresponent.

Reforç R5-Llista de components programari.

- [mp.sw.1.r5.1] El desenvolupador elaborarà i mantindrà actualitzada una relació formal dels components programari de tercers emprats en l' aplicació o producte. Es mantindrà un històric dels components utilitzats en les diferents versions del programari. El contingut mínim de la llista de components, que contindrà, almenys, la identificació del component, el fabricant i la versió emprada.

- Protecció de les Comunicacions en el Desenvolupament:

Caldrà que el desenvolupament tingui en compte el compliment del requisits relatius a les comunicacions:

| mp.com | Protecció de les comunicacions | Dimensió | BAIX | MITJÀ | ALT |
|---|---|---|---|---|---|
| mp.com.2 | Protecció de la confidencialitat | C | aplica | + R1 | + R1 + R2 + R3 |
| mp.com.3 | Protecció de la integritat i de l'autenticitat | I A | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 |
| mp.com.4 | Separació en fluxos d'informació a la xarxa | Categoría | n.a. | + [R1 o R2 o R3] | + [R2 o R3] + R4 |

Documentació general del sistema segons:
El desenvolupament ha d'incloure una descripció de la seva arquitectura de sistemes, si escau i la manera en que compleix els requisits d'arquitectura de seguretat.

| op.pl.2 | Arquitectura de Seguretat | Categoria | aplica | + R1 | + R1 + R2 + R3 |
|---|---|---|---|---|---|

- Protecció dels Serveis desenvolupats:
Caldrà que el desenvolupament tingui en compte el compliment del requisits relatius a la protecció de serveis i aplicatius web.

| mp.s.2 | Protecció de serveis i aplicacions web | Categoria | + [R1 o R2] | + [R1 o R2] | + R2 + R3 |
|---|---|---|---|---|---|

### *3.4 Serveis al Núvol*

Addicionalment si el servei ofert es tracta de serveis al núvol l'adjudicatari haurà de:

- Complir les guies del CCN-STIC (Centre Criptològic Nacional) ja siguin en modalitat IaaS, PaaS o SaaS vigents aplicables en funció de la modalitat relatives a la gestió, manteniment, configuració, administració, disseny i explotació
- Realitzar auditories de proves de penetració.
- Ser transparent en quant a facilitar informació relativa al servei i infraestructures prestada
- Utilitzar xifratge de dades i gestionar les claus d'acord amb les guies del CCN-STIC
- Facilitar una avaluació d'impacte associada al servei que es presta

### *3.5 Excepcions*

Com a excepció, **si l'entitat licitadora no disposés dels requisits anteriors**, s'acceptarà el disposar de la certificació sobre l'abast del servei mitjançant ISO 27001 o un certificat de Nivell MITJÀ com a mínim de l'ENS.
No obstant això, en cas que una d'aquestes sigui l'opció escollida, l'empresa proveïdora **haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell MITJÀ com a mínim**.

Addicionalment, si es fa servir aquesta excepció, es requerirà s'aporti informació necessària sobre el sistema que suporta els serveis, respecte a la arquitectura de seguretat. Així mateix, aportarà els diagrames de xarxa, esquemes d'elements físics, esquemes de interconnexió i esquemes lògics de sistemes que mostrin al Clínic, la infraestructura física i lògica de la qual forma part el servei objecte de contractació. Tanmateix es requerirà una Declaració d'Aplicabilitat segons els requisits de l'Annex II de l'ENS per conèixer com compleix la solució aportada cadascun dels requisits, si li aplica o no i en cas d'haver-hi responsabilitats creuades entre el Clínic i el proveïdor, com està pensat s'organitzi i es doni suport a cadascuna de les mesures.

## 4 Aspectes Generals de Seguretat per a Productes

Per a productes de TI i OT, els dispositius del sistema han de tenir una configuració de seguretat adequada per garantir el control del flux definit d'entrada i sortida de la informació. Els dispositius presents a la xarxa que disposin d'algun tipus d'emmagatzematge temporal o d'informació permanent proporcionaran la funcionalitat necessària per eliminar informació de suports d'informació.

Per garantir que el producte o productes implantats a l'entitat Hospital Clínic de Barcelona compleix les directrius de seguretat mínimes, qualsevol producte haurà de complir algun dels següents requisits per ordre de rellevància:

### *4.1 Primera Opció – "Certificació del Producte al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació"*

Si el producte ja està a la llista del Catàleg CPSTIC de productes Qualificats segons la "Guia de Seguretat de les TIC CCN-STIC 105" caldrà remetre el certificat corresponent emès per entitat acreditada.

En cas de no complir amb el requisit anterior s'ha de complir amb alguna de les opcions presentades a continuació, exposats per ordre de preferència.

### *4.2 Segona Opció – Certificació Internacional del Producte*

El producte o la solució amb qualsevol característica IT haurà d'estar certificada en alguna homologació nacional o internacional de seguretat.

Llistat de Certificacions admissibles:

- Common Criteria CC/CEM v3.1 (CC= Common Criteria for Information Technology Security Evaluation): EAL3
- SOGIS MRA v3 (Senior Officers Group for Information Systems, Mutual Recognition Agreement), per:
    - Smartcards and Similar Devices - Aquest domini tècnic està relacionat amb les targetes intel·ligents i dispositius similars.
    - Hardware Devices with Security Boxes - Aquest domini tècnic està relacionat amb productes compostos per una o més plaques de circuit imprès on gran part de la funcionalitat de seguretat requerida depèn del seu embolcall físic (l'anomenada Caixa de Seguretat)

### *4.3 Tercera Opció - Certificació de Conformitat amb l'Esquema Nacional de Seguridad (ENS) per part de la empresa subministradora del producte*

Aquesta opció es vàlida si l'empresa que fabrica el component físic o de programari disposa de Certificació de Conformitat amb l'ENS per fabricar el dispositiu o programari corresponent, amb el nivell MITJÀ com a mínim.

En aquest sentit, l'Hospital Clínic de Barcelona podrà requerir del prestador, a més de la corresponent Certificació de Conformitat amb l'ENS de l'empresa, el detall de la Declaració d'Aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries que implementa el component aportat.

### *4.4 Quarta Opció – Auditoria de Seguretat*

Disposar d'un informe d'Auditoria de Seguretat de la informació aportat per una entitat certificada en el camp de la seguretat de la informació amb certificació ISO 27001 o ENS nivell MITJÀ, amb els resultats recents com a màxim de sis mesos, en què no es detectin riscos ni vulnerabilitats de nivell crític ni alts.

Aquesta auditoria ha de ser del tipus caixa blanca, presentant contra quins marcs de seguretat s'han realitzat, presentant un resum executiu del resultat i haurà d'indicar segons els criteris de l'article 19 de l'ENS i els criteris de la Guia "CCN-STIC 140 Taxonomia de referència per a productes de seguretat TIC", si es considera:

- Favorable
- Favorable amb NO confirmades (en tal cas incloure Pla d'Accions Correctives)

Addicionalment, l'Hospital Clínic de Barcelona podrà requerir del prestador, el detall de la Declaració d'Aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries que implementa el component aportat

En cas que aquesta sigui l'opció escollida per garantir el nivell de seguretat del producte, **l'empresa proveïdora haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell Mitjà com a mínim.**

### *4.5 Cinquena Opció – Declaració de Responsabilitat Legal i Qüestionari de Seguretat*

S'haurà d'emplenar el següent formulari associat a les característiques del producte o productes oferts, per conèixer el grau de compliment de seguretat que ofereix, i el pla d'acció que prendrà l'oferent per solucionar-lo en cas de no complir els requisits.

Aquest formulari haurà d'anar acompanyada d'una declaració de responsabilitat signada per l'apoderat de l'entitat proveïdora avalant la veracitat de les dades proporcionades per part del proveïdor relatius al nivell de compliment dels requisits de seguretat del producte.

S'hauran d'aportar per a cada apartat els detalls i evidències suficients per corroborar el compliment del requisit. Els aspectes per valorar són els següents:

- ***El producte incorpora canals de comunicació fiables i assegurances:*** *Cal establir canals de comunicació segurs entre les parts utilitzant algoritmes i protocols segons la guia CCNSTIC-807 (ex.: HTTPS/TLS 1.2 o superior, IPSEC, etc.).*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte s'executa sobre una plataforma fiable:*** *incloent-hi el sistema operatiu o qualsevol entorn d'execució i dependència sobre el qual s'utilitzi. Les versions de les plataformes i productes relacionats han de ser les recomanades per les guies de seguretat CCN-STIC.*
    - *Seran admissibles, encara que no recomanables, versions que estiguin properes al seu cicle de vida i que encara tinguin suport amb actualitzacions de seguretat, amb el compromís d'evolucionar a versions superiors i suportades.*
    - *En cap cas no s'acceptaran versions o dependències sense suport del fabricant o fora del seu cicle de vida.*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte té la capacitat anti-explotació:*** *Depenent de l'àmbit del producte s'autoprotegirà quan estigui en execució, per exemple: protecció contra atacs de força bruta, protecció contra manipulacions, protecció contra manipulació de fitxers, etc. El producte ha d'estar configurat amb els permisos més restrictius, sense permisos d'accés a fitxers de manera anònima i protegir els accessos no autoritzats.*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte tindrà actualitzacions periòdiques per evitar vulnerabilitats i obsolescència:*** *El desenvolupament del producte serà actualitzat pel proveïdor durant el cicle de vida d'aquest mantenint-lo certificat en versions suportades dels elements que composen la solució global, i comunicarà les actualitzacions evolutives o que corregeixin vulnerabilitats conegudes a fitxers i protegir els accessos no autoritzats.*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte aporta restriccions d'accés a àrees restringides:*** *El producte ha de controlar l'accés a la interfície de gestió i control d'usuaris amb accés restringit mitjançant sessions no manipulables.*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte no permet la possibilitat d'injecció de codi:*** *El producte ha de controlar que els paràmetres rebuts per part de l'usuari siguin correctes i no permetin la injecció de codi o manipulació de dades.*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte us permet assegurar una política de contrasenyes robustes:*** *El producte ha de contenir un sistema de control i gestió d'autenticació mitjançant contrasenyes segures i/o certificats digitals.*

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

Data prevista del compliment: __/__/__

- ***El producte incorpora un mètode de xifratge:*** *El producte ha de contenir un sistema de xifratge que garanteixi la protecció de dades sensibles.*

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

Data prevista del compliment: __/__/__

- ***El producte permet utilitzar usuaris d'administració nominals:*** *El producte ha de treballar amb usuaris nominals i no es permetran comptes genèrics o compartits.*

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

- ***El producte incorpora capacitat d'auditoria:*** *El producte ha de permetre el control de sessions, la traçabilitat de les accions dels usuaris i administradors.*

| |
|---|
| |

***Compleix requisits:*** ***SI*** ☐ ***NO*** ☐
*En cas de no complir indicar el pla d'acció:*

| |
|---|
| |

Data prevista del compliment: __/__/__

Un cop rebudes les evidències i les respostes a cadascun dels punts, en cas d'incompliment de tres o més requisits que apliquin a la solució proposada es considerarà el producte com a NO APTE. Quan l'incompliment sigui d'un o dos punts, l'adjudicatari haurà de donar solució en temps d'implantació i en coordinació amb l'equip tècnic de l'Hospital Clínic de Barcelona. En cas que algun d'aquests requisits no apliqui s'hauran d'exposar els motius.

**En cas que aquesta sigui l'opció escollida per garantir el nivell de seguretat del producte, l'empresa proveïdora haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell Mitjà com a mínim.**

### *4.6 Recordatori Documentació Tècnica exigible*

Es recorda que qualsevol producte amb connexions de TI o OT ha d'incorporar com a documentació:

- Guies d'Instal·lació Segura
- Llistat de Components programari i maquinari que el constitueixen
- Proposta de Pla d'actualitzacions per cobrir elements obsolets de programari

## 5 Avaluació d'Impacte

Per complir els requisits que es desprenen de la legislació de protecció de dades personals vigent, en cas que, per tipologia de dades personals, finalitat, emplaçament de l'adjudicatari,

quantitat de dades, tecnologia nova o qualsevol circumstància que aconselli realitzar una avaluació d'impacte sobre la privadesa, es traslladarà a l'adjudicatari l'obligació de realitzar aquesta avaluació, seguint les indicacions del delegat de protecció de dades de l'HCB per detectar els riscos derivats del tractament de dades personals.