OBJECTE

En l'àmbit d'**FMB** i de la **protecció d'infraestructures crítiques i de la ciberesiliència en la seguretat OT,** en aquest document es determinen: requisits en qüestions de ciberseguretat aplicables als proveïdors de serveis per a sistemes operacionals d'FMB, d'acord amb l'aplicació de les recomanacions recopilades en les normatives UNE-EN IEC 62443, EN 50701 i l'Esquema Nacional de Seguretat (ENS – CCN).

CONSIDERACIONS PRÈVIES

Els requisits de sistema i de component estan previstos en la norma **UNE IEC 62443, part 3-3, requisits de seguretat del sistema i nivells de seguretat, i** en la norma **UNE IEC 62443, part 4-2, requisits tècnics de seguretat per a components iacs,** així com en la seva aplicació al sector ferroviari, UNE-CLCTS 507012021.

ACRÒNIMS

Acrònim	Concepte
BPCS	Sistema bàsic de control de processos
BR	Requisit bàsic
CR	Requisit de component
D. Req	Documentació requerida
EDR	Requisit per a dispositius integrats
ER	Millora dels requisits
EWS	Estacions de treball tècniques
HDR	Requisit per a dispositius host
ID req	Identificació dels requisits recollida en la UNE 62443-2-4
JTAG	Joint Test Action Group
NDR	Requisit per a dispositius de xarxa
PKI	Clau pública que permet xifrar i signar dades
SAR	Requisit per a aplicacions de programari
SIS	Sistema instrumentat de seguretat
SL	Nivell de seguretat
SP	Programa de seguretat
SR	Requisit de sistema
SuC	Sistema sota consideració

REQUISITS ESPECÍFICS RELACIONATS AMB LA CIBERSEGURETAT

Les empreses externes han de prendre una sèrie de mesures pel que fa a la seguretat tant física com cibernètica en els dispositius amb els quals treballen, ja que moltes vegades aquests dispositius o són a la infraestructura d'FMB o es relacionen amb aquestes infraestructures a l'hora d'efectuar-hi operacions.

Tenint en compte l'organització dels requisits recollits en la norma UNE 50701 i les descripcions d'aquests, recollides en l'UNE-EN IEC 62443, es classifiquen els diferents requisits segons l'obligatorietat, el tema que tracten i la necessitat o no d'aportar documentació per poder demostrar-ne el compliment.

1. Dotació de personal (SP.01)
2. Garantia (SP.02)
3. Arquitectura (SP.03)
4. Tecnologia sense fil (SP.04)
5. SIS (SP.05)
6. Gestió de la configuració (SP.06)
7. Accés remot (SP.07)
8. Gestió d'esdeveniments (SP.08)
9. Gestió de comptes (SP.09)
10. Protecció contra programari maliciós (SP.10)
11. Gestió de pedaços (SP.11)
12. Còpia de seguretat/restauració (SP.12)

ANNEX 0: Especificacions sobre l'inventari SuC i l'avaluació de risc inicial
ANNEX I: Requisits per a nivell SL1
ANNEX II: Requisits per a nivell SL2
ANNEX III: Requisits per a nivell SL3
ANNEX IV: Requisits per a nivell SL4

DOTACIÓ DE PERSONAL (SP.01)

Requisits relacionats amb l'assignació del personal de l'empresa externa que executa els treballs a FMB.

ID req	BR/RE	Aplicació	D.Req
SP.01.01 Formació - Requisits 62243	BR	Garantir que s'hi assigna només personal que hagi estat informat i que compleixi les responsabilitats, polítiques i procediments requerits per aquesta especificació.	No
	RE1	Garantir que s'assigna només personal del subcontractista o consultor a les activitats relacionades de les quals hagi estat informat i que compleixi les responsabilitats, polítiques i procediments requerits per aquesta especificació.	No
SP.01.02 Formació - Requisits propietari de l'actiu	BR	Garantir que s'assigna només personal del proveïdor de serveis, subcontractista o consultor a les activitats que hagi estat informat i que compleixi les responsabilitats, polítiques i procediments relacionats amb la seguretat requerits pel propietari dels actius.	No
	RE1	Garantir que s'assigna només personal del proveïdor de serveis, subcontractista o consultor a les activitats relacionades que hagi estat informat i que compleixi els processos de gestió de canvis i el permís de treball del propietari dels actius per als canvis que involucrin dispositius, estacions de treball i servidors, així com les connexions entre aquests.	No
SP.01.03 Formació - Dades confidencials	BR	Garantir que s'assigna només personal del proveïdor de serveis a les activitats relacionades que hagi estat informat i que compleixi les polítiques, procediments i obligacions contractuals requerits per protegir la confidencialitat de les dades del propietari dels actius.	No
	RE1	Garantir que s'assigna només subcontractistes, consultors i representants a les activitats relacionades que hagi estat informat i que compleixi les polítiques i procediments requerits per protegir la confidencialitat de les dades del propietari dels actius.	No
SP.01.04 Comprovació antecedents	BR	Garantir que s'assigna només personal del proveïdor de serveis a les activitats relacionades que hagi superat amb èxit les comprovacions d'antecedents relacionats amb la seguretat en la mesura en què ho permeti la legislació aplicable.	No
	RE1	Garantir que s'assigna només subcontractistes, consultors i representants a les activitats relacionades que hagi superat amb èxit les comprovacions d'antecedents (sempre que sigui possible) relacionats amb la seguretat en la mesura en què ho permeti la llei aplicable.	No
SP.01.05 Assignació laboral -	BR	Tenir la capacitat d'assignar-hi un contacte de seguretat en la seva organització, que serà responsable de les següents activitats: 1) Actuar com a enllaç amb el propietari dels actius. 2) Comunicar el punt de vista del proveïdor de serveis sobre la seguretat del IACS al personal del propietari dels actius. 3) Assegurar-se que les ofertes presentades al propietari dels actius estan d'acord	No

Contacte de seguretat		i compleixen amb els requisits de la part 2-4 especificats pel propietari dels actius i amb els requisits de seguretat interns del IACS del proveïdor de serveis. 4) Comunicar al propietari dels actius les desviacions d'assumptes que no s'ajustin als requisits.	
SP.01.06 Assignació laboral - Encarregat de seguretat	BR	Tenir documentades les qualificacions mínimes en seguretat cibernètica per als llocs de cap de seguretat i assignar caps de seguretat que tinguin aquestes qualificacions.	No
SP.01.07 Assignació laboral - Canvis	BR	Comptar amb la capacitat de notificar el propietari dels actius sobre els canvis en el personal del proveïdor de serveis, subcontractista o consultor que tingui accés a les activitats.	No

GARANTIA (SP.02)

Requisits relacionats amb la generació de confiança en l'aplicació de les polítiques de seguretat.

ID req	BR/RE	Explicació	D.Req
SP.02.01 Components de la solució - Verificació	BR	Proporcionar documentació que verifiqui que els components identificats pel propietari dels actius (per exemple, com a resultat d'una avaluació de seguretat, anàlisi d'amenaces i/o assajos de seguretat) tinguin la seguretat adequada per al seu nivell de risc.	Sí
SP.02.02 Eines i programari de seguretat	BR	Recomanar eines d'anàlisi de seguretat. 1) Proporcionar instruccions sobre com utilitzar-les. 2) Identificar qualsevol efecte advers conegut que puguin tenir en el funcionament. 3) Proporcionar recomanacions sobre com evitar-ne els efectes adversos.	Sí
	RE1	Garantir que obté l'aprovació del propietari dels actius abans d'utilitzar les eines d'anàlisi de seguretat (per exemple, l'anàlisi de xarxa) a l'emplaçament del propietari dels actius.	No
	RE2	Programar i utilitzar eines d'anàlisi de seguretat per descobrir sistemes indocumentats i/o no autoritzats o vulnerabilitats. Aquesta capacitat ha d'incloure la capacitat d'utilitzar aquestes eines d'acord amb els procediments operatius estàndard del propietari dels actius.	No
	RE3	Garantir que els components del sistema de control utilitzats tinguin la capacitat de mantenir l'operació de les funcions essencials del sistema de control en presència d'anàlisi del sistema i/o de la xarxa durant el funcionament normal.	No

SP.02.03 Directrius de protecció	BR	Proporcionar documentació al propietari dels actius que descrigui com protegir (hardening) els actius.	Sí
	RE1	Verificar que se segueixen les directrius (hardening) i procediments de protecció de la seguretat durant les activitats.	No

ARQUITECTURA (SP.03)

Requisits relacionats amb el disseny dels actius.

ID req	BR/RE	Explicació
SP.03.01 Avaluació de riscos	BR	Fer una avaluació de riscos de seguretat o participar en una avaluació de riscos de seguretat realitzada pel propietari dels actius o el seu agent. *Encara que no es requereixi documentació en aquest requisit, es podrà requerir l'avaluació de risc (vegeu l'annex 0).
	RE1	Informar el propietari dels actius dels resultats de les avaluacions de riscos de seguretat a les quals sotmeti els actius, inclosos els mecanismes i procediments de reducció de riscos.
	RE2	Verificar que un tercer hagi realitzat les revisions de l'arquitectura de seguretat i/o l'avaluació de la seguretat i/o les anàlisis d'amenaces del sistema de control utilitzat.
SP.03.02 Disseny de xarxes - Connectivitat	BR	Garantir que l'arquitectura física de segmentació de xarxa utilitzada en els actius, inclòs l'ús de dispositius de seguretat de xarxa o mecanismes equivalents, s'implementi d'acord amb el disseny aprovat pel propietari dels actius.
	RE1	Identificar i documentar els segments de xarxa dels actius i les seves interfícies amb altres segments, incloent-hi xarxes externes, i designar si cada interfície és fiable o no.
	RE2	Garantir que les interfícies que s'hagin identificat com a no fiables estiguin protegides per dispositius de seguretat de xarxa o mecanismes equivalents, amb normes de seguretat documentades i mantingudes.
SP.03.03 Vulnerabilitats	BR	Manejar les vulnerabilitats que afecten els components, incloent-hi les seves polítiques i procediments relacionats. Aquestes capacitats han d'abastar els següents punts: 1) el maneig de vulnerabilitats recentment descobertes o en les seves polítiques i procediments relacionats dels quals és responsable el proveïdor de serveis, i 2) el maneig de vulnerabilitats revelades públicament que afecten.
	RE1	Proporcionar documentació al propietari dels actius que descrigui com mitigar les febleses de seguretat inherents al disseny i/o implementació de protocols de comunicació utilitzats que es coneixien abans de les activitats d'integració o manteniment.
SP.03.04 Disseny de xarxes – Temps de xarxa	BR	Garantir que la distribució/sincronització de temps es du a terme des d'una font segura i precisa que utilitzi un protocol comunament acceptat tant per les comunitats dedicades a la seguretat com per aquelles dedicades a l'automatització industrial.

SP.03.05 Funcionalitat mínima	BR	Garantir que només les característiques de programari i maquinari requerides o aprovades pel propietari dels actius estiguin habilitades en els actius: 1) que es desactivin o eliminin les aplicacions i serveis de programari innecessari i els seus punts d'accés de comunicació associats, dispositius USB, comunicacions Bluetooth i sense fils, tret que ho requereixin els actius; 2) que estiguin autoritzades les adreces de xarxa en ús; 3) que l'accés físic i lògic als ports de diagnòstic i configuració estigui protegit contra l'accés i ús no autoritzats; 4) que els ports no utilitzats dels dispositius de xarxa es configuren per evitar l'accés no autoritzat a la infraestructura de xarxa; 5) que els processos de manteniment mantinguin l'estat de protecció (hardening) durant la seva vida útil.
	RE1	Les directrius i procediments de protecció (hardening) del proveïdor de serveis han de garantir que només s'instal·lin els certificats digitals necessaris, autoritzats i documentats per les entitats de certificació.
SP.03.06 Estacions de treball – Bloqueig de sessió	BR	Garantir que les estacions de treball sota la responsabilitat del proveïdor de serveis admeten l'ús de bloqueig de la sessió, de manera que 1) impedeixen que es mostri la informació en el dispositiu i 2) bloquegen l'entrada d'un altre usuari que no sigui el mateix o un administrador que desbloquegi.
SP.03.07 Estacions de treball – Control d'accés	BR	Garantir que les estacions de treball per cable i sense fils, inclosos els dispositius portàtils, utilitzades per al manteniment i l'enginyeria no eludeixen: 1) els controls d'accés i 2) proteccions de seguretat de la xarxa en el límit amb el nivell 3. Es prohibeix l'accés directe d'un dispositiu portàtil a un dispositiu sense fil de nivell 3 que se salti el dispositiu de seguretat de xarxa de nivell 2/3.
	RE1	Capacitat d'admetre l'ús d'autenticació multifactor segons ho requereixi el propietari de l'actiu.
SP.03.08 Dispositius - Xarxa	BR	Garantir que s'utilitzen els privilegis mínims per a l'administració dels dispositius.
	RE1	Garantir que els controls d'accés estan basats en rols d'usuari.
	RE2	Garantir que s'utilitza xifratge per protegir les dades, sigui en trànsit o en repòs.
	RE3	Garantir que els controls d'accés utilitzats per a l'administració dels dispositius de xarxa incloguin l'autenticació mútua.
SP.03.09 Protecció de dades - Comunicacions	BR	Assegurar que totes les accions de control i fluxos de dades, incloent-hi els canvis de configuració: 1) siguin vàlids; 2) els hagi iniciat o aprovat un usuari, i 3) s'hagin transferit a través d'una connexió aprovada en l'adreça aprovada.

SP.03.10 Protecció de dades – Dades confidencials	BR	Garantir que els punts d'emmagatzematge de dades i els fluxos de dades, segons el que ha definit o aprovat el propietari de l'actiu, estan documentats, incloent-hi els requisits de seguretat per a la seva protecció.
	RE1	Garantir que les dades estiguin protegides contra la divulgació o modificació no autoritzada, sigui en repòs o en trànsit.
	RE2	Proporcionar documentació al propietari de l'actiu que descrigui les capacitats de retenció proporcionades per a l'emmagatzematge/arxivament de dades confidencials.
	RE3	Garantir que els mecanismes criptogràfics utilitzats, inclosos els algorismes i la gestió/distribució/protecció de claus, siguin els comunament acceptats per les comunitats de seguretat i d'automatització industrial.
	RE4	Garantir que, quan es retiri un component, totes les dades del component que requereixin protecció es destruiran/eliminaran de forma permanent.

TECNOLOGIA SENSE FIL (SP.04)

Requisits relacionats amb l'ús de la tecnologia sense fil en els actius.

ID req	BR/RE	Explicació	D.Req
SP.04.01 Disseny de la xarxa – Descripció tècnica	BR	Garantir que la documentació de l'arquitectura dels actius que descriu els sistemes sense fils estigui actualitzada pel que fa a la descripció del següent: 1) intercanvi de dades entre una xarxa de nivell 1 i instrumentació sense fil; 2) intercanvi de dades entre una xarxa de nivell 2 i una xarxa de nivell 3 a través d'un enllaç sense fil segur; 3) mecanismes de seguretat que impedeixen que un intrús accedeixi als actius a través del sistema sense fil; 4) mecanismes de seguretat que restringeixen l'accés dins dels actius per part dels treballadors amb dispositius sense fils portàtils; 5) quan sigui necessari, mecanismes de seguretat que proporcionin protecció per a la gestió remota dels sistemes sense fils.	No
SP.04.02 Disseny de la xarxa	BR	Garantir que l'accés als dispositius sense fils estigui protegit per mecanismes d'autenticació i control d'accés comunament acceptats per les comunitats de seguretat i d'automatització industrial.	No
	RE1	Garantir que les comunicacions sense fils estiguin protegides per mecanismes criptogràfics comunament acceptats per les comunitats de seguretat i d'automatització industrial.	No
SP.04.03 Disseny de la xarxa	BR	Garantir que els protocols sense fils utilitzats en els actius compleixen les normes i les regulacions aplicables utilitzades dins de la comunitat de seguretat industrial.	No
	RE1	Garantir que s'utilitzen identificadors únics i específics dels actius per a les xarxes sense fils i que tots els identificadors sense fils són acrònims descriptius que no estan òbviament associats amb el lloc del propietari dels actius.	No
	RE2	Assegurar que els dispositius sense fils dels actius que tinguin adreces IP utilitzin un encaminament estàtic i tinguin desactivats els mecanismes d'assignació d'adreces dinàmiques (per exemple, DHCP).	No

SIS (SP.05)

Requisits relacionats amb un sistema d'integració d'un sistema instrumentat de seguretat (SIS) en els actius.

ID req	BR/RE	Explicació	D.Req
SP.05.01 Avaluació de riscos - Verificació	BR	Verificar que s'han realitzat i abordat les revisions de l'arquitectura de seguretat i/o les avaluacions dels riscos de seguretat de les comunicacions del SIS utilitzades en els actius.	No
SP.05.02 Disseny de la xarxa	BR	Garantir que les comunicacions crítiques de seguretat del SIS i les funcions de seguretat del SIS estiguin protegides de les comunicacions del BPCS (sistema bàsic de control de processos) o de qualsevol altre actiu.	No
SP.05.03 Disseny de la xarxa	BR	Garantir que les comunicacions externes als actius, incloent-hi les comunicacions d'accés remot, no puguin interferir amb el funcionament del SIS.	No
SP.05.04 Disseny de la xarxa	BR	Garantir que les aplicacions externes al SIS no puguin participar en les comunicacions del SIS que són crítiques per a les funcions de seguretat, o bé interrompre-les o interferir-hi d'alguna altra manera.	No
SP.05.05 Estacions de treball	BR	Garantir que les EWS del SIS que resideixen fora del SIS (externes a la interfície del SIS amb el sistema de control) no poden veure's compromeses per les comunicacions de nivell 3 (normes ISA95 i IEC62264-1) o superior.	No
	RE1	Garantir que les EWS dels actius que resideixen dins del SIS (internes a la interfície del SIS amb el sistema de control) no puguin veure's compromeses per l'accés remot (per exemple, RDP).	No
SP.05.06 Estacions de treball	BR	Garantir que tots els accessos al SIS siguin: 1) a través d'una passarel·la de nivell 2 dedicada al SIS i connectada físicament a aquest, i/o 2) des d'una EWS del SIS que està físicament connectada al SIS. Si l'EWS del SIS no està connectada físicament al SIS; la seva única opció és comunicar-se amb el SIS a través de passarel·la.	No
SP.05.07	BR	Garantir que l'EWS es limita a realitzar funcions del SIS.	No

Estacions de treball			
SP.05.08 Dispositius - Sense fils	BR	Verificar que no es permetin dispositius sense fils com a part integral de les funcions de seguretat del SIS.	No
SP.05.09 Interfície d'usuari	BR	Garantir que es proporciona una interfície d'usuari per activar i desactivar el mode de configuració del SIS. Mentre estigui bloquejada, aquesta interfície ha de prohibir la configuració del SIS.	No
	RE1	Garantir que es proporciona una implementació de maquinari de la interfície que sigui capaç de ser bloquejada físicament mentre el mode de configuració està deshabilitat.	No
	RE2	Capacitat de fer que una tercera part independent verifiqui que no és possible canviar la configuració del SIS quan la interfície de maquinari està bloquejada en el mode de configuració "deshabilitar".	No

GESTIÓ DE LA CONFIGURACIÓ (SP.06)

Requisits relacionats amb el control de configuració dels actius.

ID req	BR/RE	Explicació	D.Req
SP.06.01 Disseny de la xarxa	BR	Proporcionar gràfics/documentació precisos de la infraestructura lògica i física dels actius, incloent-hi els seus dispositius de xarxa, interfícies internes i interfícies externes. La documentació i els gràfics han de mantenir-se com una representació exacta.	No
	RE1	Mantenir actualitzats els documents de connexió i configuració dels equips instal·lats i en funcionament.	No
SP.06.02 Registre d'inventari	BR	Crear i mantenir un registre d'inventari SuC (vegeu annex 0), incloent-hi els números de versió i els números de sèrie, de tots els dispositius i els seus components de programari de què és responsable el proveïdor de serveis.	No
SP.06.03 Verificació	BR	Verificar que els dispositius amb fils i sense fils utilitzats per al control i la instrumentació s'han configurat correctament amb els valors aprovats.	No

ACCÉS REMOT (SP.07)

Requisits relacionats amb l'accés remot als actius.

ID req	BR/RE	Explicació	D.Req
SP.07.01 Eines i programari de seguretat	BR	Garantir que totes les aplicacions d'accés remot utilitzades en els actius siguin les comunament acceptades per les comunitats de seguretat i d'automatització industrial.	No
SP.07.02 Eines i programari de seguretat	BR	Proporcionar instruccions detallades per a la instal·lació, configuració, operació i terminació de les aplicacions d'accés remot utilitzades en els actius.	No
SP.07.03 Eines i programari de seguretat	BR	Proporcionar informació sobre totes les connexions d'accés remot proposades al propietari dels actius que inclogui, per a cada connexió: 1) el propòsit; 2) l'aplicació d'accés remot que cal utilitzar; 3) com s'establirà la connexió (per exemple, a través d'Internet mitjançant una VPN), i 4) la ubicació i identitat del client remot.	No
SP.07.04 Eines i programari de seguretat	BR	Assegurar-se d'obtenir l'aprovació del propietari dels actius abans d'utilitzar totes i cadascuna de les connexions d'accés remot.	No
	RE1	Garantir que totes les connexions d'accés remot als actius per part del proveïdor de serveis (per exemple, des d'una instal·lació del proveïdor de serveis) estan autenticades i xifrades.	No

GESTIÓ D'ESDEVENIMENTS (SP.08)

Requisits relacionats amb la gestió d'esdeveniments en els actius.

ID req	BR/RE	Explicació	D.Req
SP.08.01 Fallades de seguretat	BR	Gestionar incidents de ciberseguretat que afectin els actius que incloguin: 1) la detecció de fallades i incidents de ciberseguretat; 2) la notificació dels incidents de ciberseguretat al propietari dels actius; 3) la resposta als compromisos i incidents de ciberseguretat, incloent-hi el suport a un equip de resposta a incidents.	No
	RE1	Garantir que les fallades de seguretat que s'hagin detectat automàticament puguin notificar-se a través d'una interfície de comunicacions que sigui accessible per al propietari dels actius i que sigui comunament acceptada per les comunitats de seguretat i d'automatització industrial.	No
SP.08.02 Relacionats amb la seguretat	BR	Garantir que els actius estiguin configurats per registrar tots els esdeveniments relacionats amb la seguretat, incloses les activitats d'usuari i les activitats de gestió de comptes, en un registre d'auditoria que es manté durant el nombre de dies especificat pel propietari dels actius.	No
	RE1	Garantir que es pugui accedir a les dades i esdeveniments relacionats amb la seguretat a través d'una o més interfícies.	No
	RE2	Verificar que, mitjançant un esdeveniment simulat relacionat amb la seguretat aprovat pel propietari dels actius, els esdeveniments relacionats amb la seguretat poden recollir-se en un registre d'auditoria.	No
SP.08.03 Alarmes i esdeveniments	BR	Garantir que els actius estiguin configurats per registrar i notificar a l'operador els esdeveniments relacionats amb el procés segons ho requereixi el propietari dels actius.	No
	RE1	Garantir que es pugui informar de les alertes/esdeveniments de manera segura a través d'una interfície.	No
SP.08.04 Alarmes i esdeveniments	BR	Assegurar que els actius siguin capaços d'admetre l'ocurrència gairebé simultània d'un gran nombre d'esdeveniments (tempesta d'esdeveniments).	Sí

GESTIÓ DE COMPTES (SP.09)

Requisits relacionats amb l'administració de comptes d'usuari en els actius.

ID req	BR/RE	Explicació	D.Req
SP.09.01	BR	Garantir que els actius admetin: 1) la utilització d'una base de dades única i integrada, per definir i gestionar els comptes d'usuari i de servei; 2) la gestió restringida de comptes als usuaris autoritzats; 3) l'accés descentralitzat a aquesta base de	No

Comptes d'usuari i de servei		dades per a la gestió de comptes; 4) l'aplicació descentralitzada de la configuració dels comptes definits en aquesta base de dades.	
SP.09.02 Comptes d'usuari i de servei	BR	Assegurar que es poden crear i mantenir comptes únics per als usuaris.	No
	RE1	Proporcionar documentació al propietari dels actius que: 1) identifiqui tots els comptes d'usuari i de servei predeterminats; 2) descrigui les eines i procediments utilitzats per establir/restablir les contrasenyes de tots els comptes d'usuari i de servei predeterminats.	Sí
	RE2	Garantir que, si es genera automàticament un compte/contrasenya per a un usuari, tant el compte com la contrasenya generats seran únics.	No
	RE3	Assegurar que els comptes de servei, organitzats segons el que requereixi el propietari dels actius, s'han configurat de manera que mai caduquin ni es deshabilitin automàticament.	No
	RE4	Assegurar que el compte d'administrador incorporat es deshabiliti i, si això no és possible, que se li canviï el nom o que se'n dificulti l'explotació.	No
SP.09.03 Comptes predeterminats	BR	Garantir que els comptes predeterminats no utilitzats en el sistema hagin estat eliminats o desactivats.	No
SP.09.04 Usuari	BR	Garantir que tots els comptes d'usuari s'eliminin una vegada ja no es necessitin, i notificar el propietari dels actius sobre l'eliminació d'aquests.	No
	RE1	Generar un informe de registre d'auditoria després de la finalització de les activitats d'integració/manteniment que mostri que els comptes s'han eliminat si ja no són necessaris.	No
SP.09.05 Contrasenyes	BR	Garantir que les polítiques de contrasenyes puguin establir-se per aconseguir una complexitat mínima comunament acceptada per les comunitats de seguretat i d'automatització industrial.	No
SP.09.06 Contrasenyes	BR	Garantir que les contrasenyes dels comptes d'usuari locals i de tot el sistema es configuren perquè caduquin automàticament després d'haver estat en ús durant un període de temps especificat pel propietari dels actius.	No
	RE1	Garantir que les polítiques de contrasenyes s'estableixin per sol·licitar als usuaris que canviïn les contrasenyes N dies abans que caduquin, estant N especificat pel propietari dels actius. Aquest requisit no s'aplica a les contrasenyes que no estan configurades per caducar.	No
SP.09.07	BR	Assegurar que les contrasenyes predeterminades es canviïn segons ho requereixi el propietari dels actius.	No

Contrasenyes			
SP.09.08 Contrasenyes	BR	Assegurar que les polítiques de contrasenyes s'estableixen per evitar que els usuaris reutilitzin les seves últimes N contrasenyes, estant N especificada pel propietari dels actius.	No
	RE1	Assegurar que les polítiques de contrasenyes s'estableixen per evitar que els usuaris canviïn les seves contrasenyes més d'una vegada cada N dies, on N és especificat pel propietari dels actius.	No
SP.09.09 Contrasenyes	BR	Assegurar que els comptes les contrasenyes dels quals hagin estat aprovades pel propietari dels actius per ser compartits amb el proveïdor de serveis es troben documentats i es mantenen de manera segura.	No
	RE1	Informar el propietari dels actius sobre les contrasenyes que s'hagin compartit, divulgat o s'hagin vist compromeses.	No

PROTECCIÓ CONTRA PROGRAMARI MALICIÓS (SP.10)

Requisits relacionats amb l'ús de programari antimaliciós en els actius.

ID req	BR/RE	Explicació	D.Req
SP.10.01 Procés manual – Mecanismes protecció contra programari maliciós	BR	Proporcionar al propietari dels actius instruccions documentades per a la correcta instal·lació, configuració i actualització dels mecanismes de protecció contra el programari maliciós que es proven i verifiquen per als actius.	No
SP.10.02 Eines i programari de seguretat	BR	Garantir que: 1) els mecanismes de protecció contra el programari maliciós s'han instal·lat/actualitzat i configurat correctament; 2) els arxius de definició de programari maliciós s'instal·len dins del període de temps acordat amb el propietari dels actius; 3) les configuracions de programari maliciós es mantenen i s'actualitzen.	No
	RE	Crear i mantenir la documentació que descriu l'ús dels mecanismes de protecció contra el programari maliciós. Aquesta documentació ha d'incloure: 1) l'estat d'instal·lació; 2) els ajustos de configuració; 3) l'estat actual dels arxius de definició de programari maliciós; 4) l'ús d'altres característiques i funcions atenuants d'infeccions.	No
SP.10.03 Eines i programari	BR	Verificar que els mecanismes de protecció contra el programari maliciós instal·lats poden detectar i manejar adequadament el programari maliciós que no sigui de dia zero.	No

de seguretat			
SP.10.04 Procés manual – Arxius de definició de programari maliciós	BR	Proporcionar al propietari dels actius la documentació que descrigui: 1) com s'avaluen i aproven els arxius de definició de programari maliciós; 2) com informar de l'estat dels arxius de definició de programari maliciós al propietari dels actius. Aquest estat inclou l'aplicabilitat i l'estat d'aprovació.	Sí
SP.10.05 Dispositius	BR	Garantir que tots els dispositius, incloses les estacions de treball, subministrats als actius pel proveïdor de serveis estiguin lliures de programari maliciós conegut abans del seu ús.	No
	RE1	Garantir que els mitjans portàtils que utilitzi per a l'assaig, engegada i/o manteniment del sistema només s'utilitzen per a aquest propòsit.	No
	RE2	Garantir que tots els dispositius portàtils d'emmagatzematge i transferència de dades utilitzats o connectats als actius pel proveïdor de serveis estiguin lliures de programari maliciós conegut abans del seu ús.	No

GESTIÓ DE PEDAÇOS (SP.11)

Requisits relacionats amb els aspectes de seguretat de l'aprovació i instal·lació de pedaços de programari.

ID req	BR/RE	Explicació	D.Req
SP.11.01 Procés manual – Qualificació de pedaços	BR	Proporcionar documentació al propietari dels actius que descrigui com s'avaluen i aproven els pedaços de seguretat del programari dels actius de què és responsable.	Sí
	RE1	Revisar, com a resultat dels canvis en els riscos de seguretat, la forma en què avalua i aprova els pedaços de seguretat per al programari dels actius de què és responsable.	No
SP.11.02 Llista de pedaços	BR	Posar a la disposició del propietari dels actius la documentació que descriu els pedaços/actualitzacions de seguretat. Ha d'incloure: 1) pedaços de seguretat que són aplicables als components; 2) l'estat d'aprovació / estat del cicle de vida de cadascun; 3) un advertiment si l'aplicació d'un pedaç aprovat requereix o provoca un reinici del sistema; 4) la raó per les quals determinats pedaços no són aprovats o no són aplicables; 5) un pla de correcció per als que són aplicables, però no són aprovats.	Sí

	RE1	Posar a la disposició del propietari dels actius, a través d'una interfície comunament acceptada, una llista de pedaços que identifiqui: 1) pedaços de seguretat aprovats aplicables al programari dels actius; 2) quins d'aquests han estat aprovats per al seu ús en els actius; 3) els números de versió del programari al qual s'apliquen els pedaços aprovats.	No
	RE2	El proveïdor de serveis ha de tenir la capacitat de: 1) recomanar un pla de mitigació quan ho sol·liciti el propietari dels actius per als pedaços de seguretat que no van ser aprovats pel propietari dels actius, per exemple, perquè podrien afectar les operacions o el rendiment (vegeu el requisit bàsic SP 11.05 BR); 2) implementar el pla de mitigació després de l'aprovació del propietari dels actius.	No
SP.11.03 Pedaç de seguretat	BR	Gestionar: 1) pedaços que el propietari dels actius obtindrà directament del fabricant del pedaç, i/o 2) redistribució de pedaços per part del proveïdor de serveis sol si és aprovat pel propietari dels actius i permès pel fabricant del pedaç.	No
SP.11.04 Pedaç de seguretat	BR	Proporcionar documentació de les instruccions de com instal·lar el pedaç manualment o com utilitzar el servidor de gestió de pedaços.	Sí
SP.11.05 Pedaç de seguretat	BR	El proveïdor de serveis ha de tenir la capacitat d'assegurar-se d'obtenir l'aprovació del propietari dels actius per instal·lar tots i cadascun dels pedaços de seguretat.	No
SP.11.06 Pedaç de seguretat	BR	Garantir que el procés d'actualització asseguri l'autenticitat i integritat del programari o microprogramari (firmware) dels dispositius en els quals s'executi.	No
	RE1	Garantir que el nivell de protecció (hardening) de la seguretat dels actius es manté després de la instal·lació del pedaç, per exemple, mitjançant la reinstal·lació del programari o canviant els ajustos de configuració del sistema.	No
	RE2	Garantir que, en el cas dels dispositius que admeten la instal·lació de programari o microprogramari a la xarxa, el procés d'actualització asseguri l'autenticitat i integritat del programari o microprogramari dels dispositius.	No
	RE3	Determinar l'estat de la instal·lació de tots els pedaços de seguretat aplicables als actius de la qual és responsable el proveïdor de serveis.	No

CÒPIA DE SEGURETAT/RESTAURACIÓ (SP.12)

Requisits relacionats amb els aspectes de seguretat de les còpies de seguretat i la restauració.

ID req	BR/RE	Explicació	D.Req
SP.12.01 Procés manual – Descripció tècnica	BR	Proporcionar la documentació per als procediments de còpia de seguretat recomanats per als actius que incloguin: 1) Instruccions sobre com fer una còpia de seguretat completa i seguretat parcials, si escau, utilitzant almenys un dels següents mètodes en les arquitectures de les còpies de seguretat: a) patentada en mitjans extraïbles; b) d'un sol sistema en mitjans extraïbles; c) distribuïda; d) centralitzada. 2) Disposicions per fer una còpia de seguretat dels següents tipus de dades: arxius del sistema operatiu i dades criptogràfiques, aplicacions, dades de configuració, arxius de la base de dades, arxius de registre, llibre de registre electrònic, tipus d'arxius no convencionals, paràmetres de la instrumentació de camp, informació de directori, altres arxius identificats pel proveïdor de serveis que es requereixin per crear una còpia de seguretat completa dels actius. 3) Recomanacions per a l'emmagatzematge extern dels mitjans de còpia de seguretat. 4) Disposicions per garantir que els canvis en els actius que puguin afectar la integritat d'una còpia de seguretat no es realitzin mentre s'estigui fent una còpia de seguretat.	Sí
SP.12.02 Restauració	BR	Proporcionar instruccions documentades al propietari dels actius per restaurar els actius o els seus components al seu funcionament normal.	Sí
SP.12.03 Dispositius d'emmagatzematge portàtil	BR	Proporcionar documentació al propietari dels actius que descrigui com controlar i gestionar de manera segura els mitjans de còpia de seguretat extraïbles.	Sí
SP.12.04 Còpia de seguretat	BR	Proporcionar documentació al propietari dels actius que descrigui com verificar la còpia de seguretat del sistema amb èxit.	Sí
SP.12.05 Restauració	BR	Verificar que: 1) és possible fer una còpia de seguretat completa dels actius, i 2) és possible restablir els actius completament funcionals a partir d'aquesta còpia de seguretat.	No
SP.12.06 Còpia de seguretat	BR	Fer una còpia de seguretat dels actius d'acord amb els programes de còpia de seguretat del propietari dels actius i els objectius de restauració de dades i recuperació davant desastres.	No
SP.12.07	BR	Garantir que els actius puguin continuar funcionant normalment durant una còpia de seguretat.	No

Còpia de seguretat			
SP.12.08 Procés manual - Registre	BR	Proporcionar documentació al propietari dels actius que descrigui com generar i mantenir registres d'auditoria de totes les activitats de còpia de seguretat i restauració.	Sí
SP.12.09 Procés manual - Recuperació	BR	Documentar un pla recomanat de recuperació davant desastres que inclogui el següent, però no hi estigui limitat: 1) Descripció de diversos escenaris de desastre i el seu impacte en els actius. 2) Instruccions pas a pas per restaurar i reiniciar components amb fallades i integrar-los en els actius. 3) Requisit mínim d'arquitectura per restaurar els actius al complet.	Sí

ANNEX 0: ESPECIFICACIONS SOBRE L'INVENTARI SuC I L'AVALUACIÓ DE RISC INICIAL

Lliurables	**Especificacions**	
Identificar els actius del SuC	Establir un perímetre de seguretat i punts d'accés: - Inventari de sistema - Diagrama d'arquitectura de xarxa i flux de les dades	
Avaluació inicial dels riscos cibernètics *Identificar riscos no reduïts i l'impacte que poden tenir sobre diferents aspectes, com ara l'impacte per a la seguretat/salut, pèrdua de producció, interrupció del servei, entre d'altres.*	Divisió de les zones en zones i conductes	- Agrupar els actius segons diferents criteris, com l'avaluació de riscos, la criticitat dels actius, la ubicació física o lògica, l'accés requerit o l'organització responsable. Parar esment als sistemes sense fils, els dispositius amb punts de connexió d'Internet, els que interactuen amb el IACS gestionats per altres entitats i dispositius mòbils. - Separar en zones lògiques i/o físiques els actius del IACS dels de l'empresa. - Intentar separar els actius del IACS que estan relacionats amb la seguretat dels que no, quan sigui possible; si no ho és, identificar tot el conjunt com a actiu de seguretat, ja que necessita un nivell major de protecció. - Separar els actius connectats temporalment dels que no ho estan, si aquests actius s'usen amb altres dispositius; no s'aplica a dispositius que no s'utilitzen fora d'aquests sistemes. - Separar dispositius sense fils dels que funcionen amb fil, per exemple, a través d'un tallafoc. - Separar els dispositius que estan connectats al sistema a través de connexions externes.
	Comparació de riscos	- Si el risc inicial sobrepassa el risc tolerable, s'ha de fer una avaluació detallada. - Es poden agrupar zones que tinguin amenaces compartides i aplicar dissenys que s'hagin utilitzat amb anterioritat per a aquest nivell d'amenaça i que les hagi mitigat.
	Identificar les amenaces	- Identificar les vulnerabilitats i els punts d'accés - Determinar l'impacte i conseqüències ▪ Analitzar el cost i els beneficis dels controls de seguretat, mesurament qualitatiu o quantitatiu. - Determinar la probabilitat no mitigada

	Llistar de manera detallada i realista les amenaces (descriure la font, la capacitat de la font, vectors i actius afectats)	▪ Probabilitat que les amenaces es materialitzin tenint en compte l'historial, la motivació de la font, les vulnerabilitats conegudes, etc. - Determinar el risc no mitigat ▪ Determinar l'impacte combinant la probabilitat no mitigada. - Determinar el nivell de seguretat objectiu ▪ El mètode per determinar-lo és a elecció. - Comparar el risc no mitigat amb el risc no tolerable ▪ Determinar si el risc es transfereix, es mitiga o s'accepta. - Identificar i avaluar les contramesures existents ▪ Avaluar l'eficàcia d'aquestes en l'impacte. - Reavaluar la probabilitat i l'impacte - Determinar el risc residual ▪ Es determina combinant la probabilitat mitigada i l'impacte mitigat actual. - Comparar el risc actual amb el risc tolerable - Identificar contramesures addicionals de seguretat cibernètiques - Documentar i comunicar els resultats ▪ Diagrames d'arquitectura del sistema, les avaluacions de la vulnerabilitat i fonts d'informació de les amenaces.

	Documentar els requisits, les hipòtesis i les restriccions de seguretat cibernètica	- Especificació dels requisits de seguretat cibernètica ▪ Descripció del SUC ▪ Diagrames de zones i conductes ▪ Característiques de les zones i conductes a) Nom i/o identificador únic b) Organització/ons responsable/s c) Definició del límit lògic i físic, si correspon d) Designació de seguretat e) Llista de tots els punts d'accés lògics i físics f) Llista de flux de dades associades a cada punt d'accés g) Zones o conductes connectats h) Llista d'actius i la seva classificació, criticitat i valor de negoci i) Nivell de seguretat objectiu j) Requisits de seguretat aplicables k) Polítiques de seguretat aplicables l) Hipòtesi i dependències externes ▪ Hipòtesis de l'entorn de funcionament ▪ Entorn d'amenaces ▪ Polítiques de seguretat de l'organització ▪ Risc tolerable ▪ Requisits reglamentaris - Entorn d'amenaça ▪ Incloure amenaces tant actuals com futures, per exemple, clima geopolític, ajust físic i sensibilitat del sistema. - Polítiques de seguretat de l'organització ▪ Contramesures i elements de seguretat implementats - Risc tolerable - Requisits reglamentaris ▪ Important per al compliment de la normativa.

ANNEX I: REQUISITS PER A NIVELL SL1

Requisits de seguretat del sistema

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
SR 1.1	BR	Tots els usuaris que accedeixin al sistema han de ser identificats i autenticats tant a escala de sistemes com d'aplicació; pot ser a través de contrasenyes, dispositius d'accés o multifactor (combinació de les anteriors).
SR 1.3	BR	El sistema de control ha de tenir la capacitat de gestionar comptes d'usuaris (agregar-ne, eliminar-ne, modificar-ne o desactivar-ne) establint condicions per pertànyer a un grup i l'assignació d'autoritzacions. Només s'admetran comptes compartits quan, per condicions del sistema, s'estableixi en l'anàlisi de risc, encara que s'hauran d'establir contramesures i documentar-les.
SR 1.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la gestió dels identificadors (permet operar dins d'un domini o zona de control específic del sistema) per usuari, grup, rol o interfície del sistema de control.
SR 1.5	BR	El sistema de control ha de proporcionar la capacitat de: 1) iniciar el contingut de l'autenticador; 2) canviar tots els autenticadors predeterminats; 3) canviar/actualitzar els autenticadors; 4) protegir-los contra la divulgació i modificació no autoritzada. Exemples d'autenticadors són claus físiques, targetes d'accés, claus privades, entre d'altres.
SR 1.6	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris que participin en una comunicació sense fil. Exemples de tecnologies sense fils són Bluetooth, infrarojos, encaminadors mòbils, etc.
SR 1.7	BR	En els sistemes de control que utilitzin la contrasenya com a mitjà d'autenticació, s'ha d'aplicar una fortalesa configurable sobre la base de la longitud mínima i la varietat de caràcters. S'aplicarà vigència màxima per a les contrasenyes i es notificarà quan aquesta expiri. Aquesta protecció es pot millorar limitant la reutilització de les contrasenyes.
SR 1.10	BR	El sistema de control ha de proporcionar la capacitat d'ocultar la retroalimentació de la informació d'autenticació durant el procés. No ha de donar pistes sobre les fallades d'autenticació com, per exemple, "nom d'usuari desconegut".
SR 1.11	BR	El sistema de control ha de proporcionar la capacitat d'aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per qualsevol usuari dins d'un període configurable de temps.
SR 1.12	BR	El sistema de control ha de proporcionar la capacitat de mostrar un missatge d'avís del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge d'avís d'ús del sistema.
SR 1.13	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança. Ha de permetre l'accés només quan s'hi estigui autoritzat i restringir l'accés des de connexions telefòniques o no autoritzades. És possible que els procediments requereixin l'autenticació multifactor per permetre l'accés remot.

FR2. Control d'ús		
SR 2.1	BR	El sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris humans per controlar l'ús del sistema de control a fi d'admetre el repartiment de tasques i el privilegi mínim. Cal verificar que les accions de l'usuari estan permeses segons el rol assignat i permetre que només les persones qualificades i autoritzades facin canvis en els components del sistema.
SR 2.2	BR	El sistema de control ha de proporcionar la capacitat d'autoritzar, supervisar i aplicar les restriccions d'ús per a les connexions sense fils al sistema de control conformement a les pràctiques comunament acceptades en el sector de la seguretat.
SR 2.3	BR	El sistema de control ha de proporcionar la capacitat d'aplicar automàticament les restriccions d'ús configurables, que inclouen: a) prevenir l'ús de dispositius portàtils i mòbils; b) requerir autorització basada en un context específic, i c) restringir la transferència de codis i dades a/de dispositius portàtils i mòbils.
SR 2.4	BR	El sistema de control ha de proporcionar la capacitat d'aplicar restriccions d'ús per a les tecnologies de codi mòbil basades en la possibilitat que causin danys al sistema de control, incloent-hi: a) prevenir l'execució del codi mòbil; b) requerir processos d'autenticació i autorització adequats per a l'origen del codi; c) restringir la transferència del codi mòbil al/del sistema de control, i d) supervisar l'ús del codi mòbil.
SR 2.5	BR	El sistema de control ha de proporcionar la capacitat d'evitar un accés posterior iniciant un bloqueig de la sessió després d'un període de temps configurable d'inactivitat o mitjançant iniciació manual. La sessió ha de continuar bloquejada fins que l'usuari autoritzat restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats. En els casos en els quals el sistema de control no pugui admetre el bloqueig de la sessió, l'entitat responsable hauria d'emprar les contramesures compensatòries que es considerin adequades, com majors mesures de seguretat física i auditories.
SR 2.8	BR	El sistema de control ha de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: control d'accés, errors de sol·licitud, esdeveniments del sistema operatiu, esdeveniments del sistema de control, esdeveniments de còpies de seguretat i restauració, canvis en la configuració, activitat potencial de reconeixement i esdeveniments del registre d'auditoria. Els registres individuals d'auditoria han d'incloure la marca de temps, font (dispositiu, procés de programari o compte d'usuari humà d'origen), categoria, tipus, identificador de l'esdeveniment i resultat de l'esdeveniment.
SR 2.9	BR	El sistema de control ha d'assignar una capacitat suficient d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres i la configuració del sistema. El sistema de control ha de proporcionar mecanismes d'auditoria per reduir la possibilitat que s'excedeixi aquesta capacitat.
SR 2.10	BR	El sistema de control ha de proporcionar la capacitat d'alertar el personal i evitar la pèrdua de serveis i funcions essencials en cas que falli el processament d'auditories. El sistema de control ha de proporcionar la capacitat d'admetre les accions apropiades en resposta a una fallada en el processament d'auditories d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
FR3. Integritat del sistema		

SR 3.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el sistema per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física fent servir maquinari adequat per al context en el qual es troba.
SR 3.2	BR	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció per prevenir, detectar, mitigar i informar dels efectes d'un codi maliciós o de programari no autoritzat. El sistema de control ha de proporcionar la capacitat d'actualitzar els mecanismes de protecció.
SR 3.3	BR	El sistema de control ha de proporcionar la capacitat d'admetre la verificació del funcionament previst de les funcions de seguretat (mesures d'antivirus, identificació, detecció d'intrusos i auditories) i informar de les anomalies que es produeixin durant els assajos d'acceptació en fàbrica i en emplaçament i durant el manteniment programat. Les funcions de seguretat han d'incloure totes les funcions que siguin necessàries per complir els requisits de seguretat especificats en aquesta norma.
SR 3.5	BR	El sistema de control ha de validar la sintaxi i el contingut de qualsevol entrada que s'utilitzi com a entrada de control de processos industrials o entrada que tingui un impacte directe en l'acció del sistema de control. Les directrius que cal tenir en compte haurien d'incloure la Code Review Guide de l'Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control ha de proporcionar la capacitat d'establir el valor de sortida a un estat predeterminat si no es pot mantenir el funcionament normal com a resultat d'un atac.
FR4. Confidencialitat de les dades		
SR 4.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació (especialment en dispositius portàtils) per la qual s'admet l'autorització explícita de lectura, estigui en repòs o en trànsit. La tècnica triada ha de tenir en compte les possibles ramificacions en el rendiment del sistema de control i la capacitat de recuperar-se després d'una fallada del sistema o un atac.
SR 4.3	BR	Si es requereix l'ús de criptografia, el sistema de control ha d'usar algorismes criptogràfics, grandàries de clau i mecanismes per a l'establiment i gestió de claus conformement a les pràctiques i recomanacions de seguretat comunament acceptades en el sector que es troben en documents com la publicació especial NIST SP800-57
FR5. Flux de dades restringides		
SR 5.1	BR	El sistema de control ha de proporcionar la capacitat de segmentar de manera lògica les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control d'altres xarxes del sistema de control.
SR 5.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones i conductes de risc. Com a part d'una estratègia de protecció de defensa total, s'haurien de dividir els sistemes de control de major impacte en zones separades utilitzant conductes per restringir o prohibir l'accés a la xarxa conformement a les polítiques i procediments de seguretat i a una avaluació de riscos.

SR 5.3	BR	Un sistema de control ha de proporcionar la capacitat d'evitar la recepció de missatges de propòsit general (correu electrònic, xarxes socials o qualsevol altre sistema de missatgeria) entre persones procedents d'usuaris o sistemes externs al sistema de control.
SR 5.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la partició de dades (per mitjans físics o lògics), aplicacions i serveis sobre la base de la seva criticitat per facilitar la implementació d'un model de zonificació.
FR6. Resposta oportuna als incidents		
SR 6.1	BR	El sistema de control ha de proporcionar la capacitat que les persones i/o les eines autoritzades accedeixin als registres d'auditoria en mode de lectura.
FR7. Disponibilitat dels recursos		
SR 7.1	BR	El sistema de control ha de proporcionar la capacitat de funcionar en mode degradat durant un esdeveniment de denegació de servei. Un esdeveniment de denegació de servei en el sistema de control no hauria d'afectar negativament cap sistema relacionat amb la seguretat.
SR 7.2	BR	El sistema de control ha de proporcionar la capacitat de limitar l'ús de recursos per part de les funcions de seguretat per evitar l'esgotament dels recursos.
SR 7.3	BR	El sistema de control ha de facilitar la identitat i ubicació dels arxius crítics i la capacitat de dur a terme còpies de seguretat de la informació de l'usuari i del sistema (incloent-hi informació sobre l'estat del sistema) sense que això afecti les operacions habituals.
SR 7.4	BR	El sistema de control ha de proporcionar la capacitat de recuperar-se i reconstituir-se fins a un estat segur conegut després d'una interrupció o fallada. Un estat segur conegut significa que s'atribueixen a tots els paràmetres del sistema (siguin predeterminats o configurables) valors segurs, es reinstal·len els pedaços crítics per a la seguretat, es restableixen els ajustos de configuració relacionats amb la seguretat, es disposa de la documentació i els procediments operatius del sistema, es reinstal·la i configura l'aplicació i el programari del sistema amb ajustos segurs, es carrega la informació de les còpies de seguretat més recents i conegudes, i se sotmet a assaig i es comprova el funcionament del sistema íntegrament.
SR 7.5	BR	El sistema de control ha de proporcionar la capacitat de canviar d'una font d'alimentació d'emergència i a aquesta sense que això afecti l'estat de seguretat existent o un mode degradat documentat.
SR 7.6	BR	El sistema de control ha de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El sistema de control ha de proporcionar una interfície als ajustos de configuració de xarxa i seguretat desplegats actualment.
SR 7.7	BR	El sistema de control ha de proporcionar la capacitat de prohibir i/o restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.

Requisits de seguretat dels components generals

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
CR 1.1	BR	Els components han de proporcionar la capacitat d'identificar i autenticar tots els usuaris en totes les interfícies que permetin el repartiment de tasques i els privilegis mínims. Es pot proporcionar a escala component o a escala sistema.
CR 1.3	BR	Els components han de proporcionar la capacitat de permetre la gestió de tots els comptes de forma directa o integrant-se en un sistema que gestioni els comptes.
CR 1.4	BR	Els components han de proporcionar la capacitat d'integrar-se en un sistema que admeti la gestió d'identificadors i/o la capacitat de permetre la gestió d'identificadors.
CR 1.5	BR	Els components han de proporcionar la capacitat de: a) permetre l'ús del contingut inicial de l'autenticador; b) permetre el reconeixement dels canvis en els autenticadors predeterminats realitzats al moment de la instal·lació; c) funcionar correctament amb operacions periòdiques de modificació/actualització dels autenticadors, i d) protegir els autenticadors de la divulgació i modificació no autoritzada quan s'emmagatzemen, utilitzen i transmeten.
CR 1.7	BR	Els components que utilitzin autenticació basada en contrasenya, han de proporcionar o integrar-se en un sistema que proporcioni la capacitat d'aplicar la fortalesa de les contrasenyes configurables d'acord amb directrius de contrasenyes reconegudes i provades internacionalment.
CR 1.10	BR	Quan un component ofereixi la capacitat d'autenticació, el component ha d'oferir la capacitat d'ocultar la retroalimentació de la informació de l'autenticador durant el procés d'autenticació.
CR 1.11	BR	Quan un component ofereixi una capacitat d'autenticació, el component ha de proporcionar la capacitat de: a) aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per part de qualsevol usuari durant un període de temps configurable; b) denegar l'accés durant un període de temps específic o fins que un administrador el desbloquegi, quan s'hagi arribat a aquest límit. Un administrador pot desbloquejar un compte abans de la caducitat del període de temps d'espera.
CR 1.12	BR	Quan un component proporcioni un accés d'usuari humà local/IHM, ha de proporcionar la capacitat de mostrar un missatge de notificació d'ús del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge de notificació d'ús del sistema.
FR2. Control d'ús		
CR 2.1	BR	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris identificats i autenticats en funció de les responsabilitats que se'ls hagin assignat.
CR 2.2	BR	Si un component admet l'ús a través d'interfícies sense fils, ha de proporcionar la capacitat d'integrar-se en el sistema que admet l'autorització d'ús, la supervisió i les restriccions d'acord amb les pràctiques industrials comunament acceptades.

CR 2.5	BR	Si un component proporciona una interfície per a un usuari humà, tant si s'hi accedeix localment com a través d'una xarxa, el component ha de proporcionar la capacitat de: a) protegir-se contra l'accés posterior iniciant un bloqueig de sessió després d'un període de temps configurable d'inactivitat o mitjançant la iniciació manual per part de l'usuari i b) mantenir el bloqueig de la sessió fins que l'usuari propietari de la sessió, o un altre usuari humà autoritzat, restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats.
CR 2.8	BR	Els components han de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: a) control d'accés; b) errors de sol·licitud; c) esdeveniments del sistema de control; d) esdeveniment de còpia de seguretat i restauració; e) canvis de configuració, i f) esdeveniments de registre d'auditoria. Els registres d'auditoria individuals han d'incloure: a) marca de temps; b) font (dispositiu d'origen, procés de programari o compte d'usuari humà); c) categoria; d) tipus; e) ID de l'esdeveniment, i f) resultat de l'esdeveniment.
CR 2.9	BR	Els components han de: a) proporcionar la capacitat d'assignar una capacitat d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres, i b) proporcionar mecanismes per protegir contra una fallada del component quan arribi a la capacitat d'emmagatzematge de dades d'auditoria o la superi.
CR 2.10	BR	Els components han de: a) proporcionar la capacitat de protegir contra la pèrdua de serveis i funcions essencials en cas que falli el processament d'una auditoria, i b) proporcionar la capacitat per permetre les accions apropiades en resposta a una fallada en el processament d'una auditoria d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
CR 2.11	BR	Els components han de proporcionar la capacitat de crear marques de temps (incloent-hi data i hora) per al seu ús en els registres d'auditoria.
CR 2.12	BR	Si un component proporciona una interfície per a un usuari humà, el component ha de proporcionar la capacitat de determinar si un determinat usuari humà ha realitzat una determinada acció. Els elements de control que no puguin permetre aquesta capacitat s'han d'enumerar en els documents dels components.
FR3. Integritat del sistema		
CR 3.1	BR	Els components han de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el component per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
CR 3.3	BR	Els components han de proporcionar la capacitat de permetre la verificació de l'operació prevista de les funcions de seguretat d'acord amb el requisit del sistema.
CR 3.4	BR	Els components han de proporcionar la capacitat de fer o permetre verificacions d'integritat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'integritat.

CR 3.5	BR	Els components han de validar la sintaxi, la longitud i el contingut de qualsevol dada d'entrada que s'utilitzi com a entrada de control de processos industrials o entrada a través d'interfícies externes que tinguin un impacte directe en l'acció del component.
CR 3.6	BR	Els components que es connecten físicament o lògicament a un procés d'automatització han de proporcionar la capacitat d'establir sortides a un estat predeterminat si no es pot mantenir el funcionament normal definit pel proveïdor de components.
CR 3.7	BR	Els components han d'identificar i tractar les condicions d'error de manera que no proporcionin informació que pugui ser aprofitada per adversaris per atacar el sistema de control.
FR4. Confidencialitat de les dades		
CR 4.1	BR	Els components han de: a) proporcionar la capacitat de protegir la confidencialitat de la informació en repòs per a la qual s'admet l'autorització explícita de lectura, i b) permetre la protecció de la confidencialitat de la informació en trànsit, com defineix el requisit del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.3	BR	Si es requereix l'ús de criptografia, el component ha d'utilitzar mecanismes de seguretat criptogràfica d'acord amb pràctiques i recomanacions de seguretat internacionalment reconegudes i provades.
FR5. Flux de dades restringides		
CR 5.1	BR	Els components han de permetre una xarxa segmentada que admeti zones i conductes, segons sigui necessari, per permetre una arquitectura de xarxa més àmplia basada en la segmentació lògica i la criticitat.
FR6. Resposta oportuna als incidents		
CR 6.1	BR	Els components han de proporcionar la capacitat perquè les persones i/o les eines autoritzades puguin accedir als registres d'auditoria de només lectura.
FR7. Disponibilitat dels recursos		
CR 7.1	BR	Els components han de proporcionar la capacitat de mantenir les funcions essencials quan operin en mode degradat com a resultat d'un esdeveniment de denegació de servei.
CR 7.2	BR	Els components han de proporcionar la capacitat de limitar l'ús de recursos en les funcions de seguretat per protegir contra l'esgotament dels recursos.
CR 7.3	BR	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
CR 7.4	BR	Els components han de proporcionar la capacitat de poder-se recuperar i reconstituir fins a un estat segur conegut després d'una interrupció o fallada.

CR 7.6	BR	Els components han de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El component ha de proporcionar una interfície amb els ajustos de configuració de xarxa i seguretat actualment desplegats.
CR 7.7	BR	Els components han de proporcionar la capacitat de restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.

Requisits de seguretat del component pel que fa a programari

ID req	BR/RE	Explicació
SAR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
SAR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.

Requisits de seguretat per als dispositius integrats (PLC, IED)

ID req	BR/RE	Explicació
EDR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
EDR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.
EDR 3.10	BR	El dispositiu integrat ha d'admetre la capacitat de ser actualitzat i sotmetre's a una pujada de nivell.
EDR 3.14	BR	Els dispositius integrats han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per a l'arrencada del component i els processos en temps d'execució abans del seu ús.

Requisits de seguretat per als dispositius host

ID req	BR/RE	Explicació
HDR 2.4	BR	En cas que un dispositiu host utilitzi tecnologies de codi mòbil, aquest dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu host: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a carregar codi mòbil en el dispositiu host, i c) controlar l'execució del codi basant-se en comprovacions d'integritat en el codi mòbil i abans que el codi s'executi.
HDR 3.2	BR	Els dispositius host han de comptar amb mecanismes homologats pel proveïdor de productes del sistema de control que garanteixin la protecció contra codis maliciosos. El proveïdor del producte del sistema de control ha de documentar qualsevol requisit especial de configuració relacionat amb la protecció contra el codi maliciós.
HDR 3.10	BR	Els dispositius host han de comptar amb la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
HDR 3.14	BR	Els dispositius host han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.

Requisits de seguretat per als dispositius de xarxa

ID req	BR/RE	Explicació
NDR 1.6	BR	Un dispositiu de xarxa que permeti la gestió d'accés sense fil ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris (persones, processos de programari o dispositius) que participen en la comunicació sense fil.
NDR 1.13	BR	El dispositiu de xarxa que permeti l'accés de dispositius a una xarxa ha de poder supervisar i controlar tots els mètodes d'accés al dispositiu de xarxa a través de xarxes que no són de confiança.
NDR 2.4	BR	En cas que un dispositiu de xarxa utilitzi tecnologies de codi mòbil, ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu de xarxa: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil cap a / des del dispositiu de xarxa, i c) controlar l'execució del codi basant-se en verificacions d'integritat abans que el codi s'executi.
NDR 3.2	BR	El dispositiu de xarxa ha de proporcionar protecció contra codis maliciosos.
NDR 3.10	BR	Els dispositius de xarxa han d'admetre la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
NDR 3.14	BR	Els dispositius de xarxa han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.

NDR 5.2	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones de risc i conductes.
NDR 5.3	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de protegir contra la recepció de missatges de propòsit general entre persones rebuts d'usuaris o sistemes externs al sistema de control.

ANNEX II: REQUISITS PER A NIVELL SL2

Requisits de seguretat del sistema

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
SR 1.1	BR	Tots els usuaris que accedeixin al sistema han de ser identificats i autenticats tant a escala de sistemes com d'aplicació; pot ser a través de contrasenyes, dispositius d'accés o multifactor (combinació de les anteriors).
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris humans.
SR 1.2	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els processos de programari i dispositius. Aquesta capacitat ha de fer complir aquesta identificació i autenticació en totes les interfícies que proporcionin accés al sistema de control per permetre els privilegis mínims, de conformitat amb les polítiques i procediments de seguretat aplicables.
SR 1.3	BR	El sistema de control ha de tenir la capacitat de gestionar comptes d'usuaris (agregar-ne, eliminar-ne, modificar-ne o desactivar-ne) establint condicions per pertànyer a un grup i l'assignació d'autoritzacions. Només s'admetran comptes compartits quan, per condicions del sistema, s'estableixi en l'anàlisi de risc, encara que s'hauran d'establir contramesures i documentar-les.
SR 1.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la gestió dels identificadors (permet operar dins d'un domini o zona de control específic del sistema) per usuari, grup, rol o interfície del sistema de control.
SR 1.5	BR	El sistema de control ha de proporcionar la capacitat de: 1) iniciar el contingut de l'autenticador; 2) canviar tots els autenticadors predeterminats; 3) canviar/actualitzar els autenticadors; 4) protegir-los contra la divulgació i modificació no autoritzada. Exemples d'autenticadors són claus físiques, targetes d'accés, claus privades, entre d'altres.
SR 1.6	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris que participin en una comunicació sense fil. Exemples de tecnologies sense fils són Bluetooth, infrarojos, encaminadors mòbils, etc.
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris (persones, processos o dispositius) que participin en la comunicació sense fil.
SR 1.7	BR	En els sistemes de control que utilitzin la contrasenya com a mitjà d'autenticació, s'ha d'aplicar una fortalesa configurable sobre la base de la longitud mínima i la varietat de caràcters. S'aplicarà vigència màxima per a les contrasenyes i es notificarà quan aquesta expiri. Aquesta protecció es pot millorar limitant la reutilització de les contrasenyes.
SR 1.8	BR	En els casos en què s'utilitzi una PKI, el sistema de control ha de proporcionar la capacitat que una PKI funcioni conformement a les millors pràctiques comunament acceptades o obtenir certificats de clau pública d'una PKI existent. El registre d'aquesta ha d'incloure l'autorització d'un supervisor que verifiqui la identitat del titular del certificat i que garanteixi que s'emet a l'usuari previst.

SR 1.9	BR	En el cas dels sistemes de control que utilitzin autenticació de clau pública (PKI), el sistema de control ha de proporcionar la capacitat de: l) validar els certificats comprovant la validesa de la signatura d'un certificat determinat; m) validar els certificats a través d'una ruta de certificació a una CA acceptada o, en el cas dels certificats autosignats, desplegant certificats d'entitat final a tots els hosts que es comuniquen amb el subjecte al qual s'emet el certificat; n) validar els certificats comprovant l'estat de revocació d'un certificat determinat; o) establir el control de l'usuari sobre la clau privada corresponent, i p) assignar la identitat autenticada a un usuari.
SR 1.10	BR	El sistema de control ha de proporcionar la capacitat d'ocultar la retroalimentació de la informació d'autenticació durant el procés. No ha de donar pistes sobre les fallades d'autenticació com, per exemple, "nom d'usuari desconegut".
SR 1.11	BR	El sistema de control ha de proporcionar la capacitat d'aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per qualsevol usuari dins d'un període configurable de temps.
SR 1.12	BR	El sistema de control ha de proporcionar la capacitat de mostrar un missatge d'avís del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge d'avís d'ús del sistema.
SR 1.13	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança. Ha de permetre l'accés només quan s'hi estigui autoritzat i restringir l'accés des de connexions telefòniques o no autoritzades. És possible que els procediments requereixin l'autenticació multifactor per permetre l'accés remot.
	RE1	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança.
FR2. Control d'ús		
SR 2.1	BR	El sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris humans per controlar l'ús del sistema de control a fi d'admetre el repartiment de tasques i el privilegi mínim. Cal verificar que les accions de l'usuari estan permeses segons el rol assignat i permetre que només les persones qualificades i autoritzades facin canvis en els components del sistema.
	RE1	En totes les interfícies, el sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris (persones, processos de programari i dispositius) per controlar l'ús del sistema de control amb la finalitat d'admetre el repartiment de tasques i el privilegi mínim.
	RE2	El sistema de control ha de proporcionar la capacitat que un usuari o rol autoritzat defineixi i modifiqui l'assignació de permisos a rols per a tots els usuaris humans.
SR 2.2	BR	El sistema de control ha de proporcionar la capacitat d'autoritzar, supervisar i aplicar les restriccions d'ús per a les connexions sense fils al sistema de control conformement a les pràctiques comunament acceptades en el sector de la seguretat.
SR 2.3	BR	El sistema de control ha de proporcionar la capacitat d'aplicar automàticament les restriccions d'ús configurables, que inclouen: a) prevenir l'ús de dispositius portàtils i mòbils; b) requerir autorització basada en un context específic, i c) restringir la transferència de codis i dades a/de dispositius portàtils i mòbils.

SR 2.4	BR	El sistema de control ha de proporcionar la capacitat d'aplicar restriccions d'ús per a les tecnologies de codi mòbil basades en la possibilitat que causin danys al sistema de control, incloent-hi: a) prevenir l'execució del codi mòbil; b) requerir processos d'autenticació i autorització adequats per a l'origen del codi; c) restringir la transferència del codi mòbil al/del sistema de control, i d) supervisar l'ús del codi mòbil.
SR 2.5	BR	El sistema de control ha de proporcionar la capacitat d'evitar un accés posterior iniciant un bloqueig de la sessió després d'un període de temps configurable d'inactivitat o mitjançant iniciació manual. La sessió ha de continuar bloquejada fins que l'usuari autoritzat restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats. En els casos en els quals el sistema de control no pugui admetre el bloqueig de la sessió, l'entitat responsable hauria d'emprar les contramesures compensatòries que es considerin adequades, com majors mesures de seguretat física i auditories.
SR 2.6	BR	El sistema de control ha de proporcionar la capacitat de finalitzar una sessió remota, sigui automàticament després d'un període d'inactivitat configurable o manualment per part de l'usuari que va iniciar la sessió.
SR 2.8	BR	El sistema de control ha de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: d'accés, errors de sol·licitud, esdeveniments del sistema operatiu, esdeveniments del sistema de control, esdeveniments de còpies de seguretat i restauració, canvis en la configuració, activitat potencial de reconeixement i esdeveniments del registre d'auditoria. Els registres individuals d'auditoria han d'incloure la marca de temps, font (dispositiu, procés de programari o compte d'usuari humà d'origen), categoria, tipus, identificador de l'esdeveniment i resultat de l'esdeveniment.
SR 2.9	BR	El sistema de control ha d'assignar una capacitat suficient d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres i la configuració del sistema. El sistema de control ha de proporcionar mecanismes d'auditoria per reduir la possibilitat que s'excedeixi aquesta capacitat.
SR 2.10	BR	El sistema de control ha de proporcionar la capacitat d'alertar el personal i evitar la pèrdua de serveis i funcions essencials en cas que falli el processament d'auditories. El sistema de control ha de proporcionar la capacitat d'admetre les accions apropiades en resposta a una fallada en el processament d'auditories d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
SR 2.11	BR	El sistema de control ha de proporcionar marques de temps (data i hora) per a la generació de registres d'auditoria. Cal evitar que les fonts horàries sofreixin alteracions no autoritzades.

FR3. Integritat del sistema		
SR 3.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el sistema per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
SR 3.2	BR	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció per prevenir, detectar, mitigar i informar dels efectes d'un codi maliciós o de programari no autoritzat. El sistema de control ha de proporcionar la capacitat d'actualitzar els mecanismes de protecció.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció contra codis maliciosos en tots els punts d'entrada i sortida.
SR 3.3	BR	El sistema de control ha de proporcionar la capacitat d'admetre la verificació del funcionament previst de les funcions de seguretat (mesures d'antivirus, identificació, detecció d'intrusos i auditories) i informar de les anomalies que es produeixin durant els assajos d'acceptació en fàbrica i en emplaçament i durant el manteniment programat. Les funcions de seguretat han d'incloure totes les funcions que siguin necessàries per complir els requisits de seguretat especificats en aquesta norma.
SR 3.4	BR	El sistema de control ha de proporcionar la capacitat de detectar, registrar, informar i protegir contra canvis no autoritzats en el programari i en la informació en repòs.
SR 3.5	BR	El sistema de control ha de validar la sintaxi i el contingut de qualsevol entrada que s'utilitzi com a entrada de control de processos industrials o entrada que tingui un impacte directe en l'acció del sistema de control. Les directrius que cal tenir en compte haurien d'incloure la Code Review Guide de l'Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control ha de proporcionar la capacitat d'establir el valor de sortida a un estat predeterminat si no es pot mantenir el funcionament normal com a resultat d'un atac.
SR 3.7	BR	El sistema de control ha d'identificar i tractar les condicions d'error de manera que s'hi pugui aplicar un remei efectiu. Això s'ha de fer sense proporcionar informació que pugui ser aprofitada per adversaris per atacar el sistema de control, tret que sigui necessari per resoldre els problemes de manera oportuna.
SR 3.8	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de les sessions. El sistema de control ha de rebutjar qualsevol ús per part d'identificadors de sessió no vàlids.
SR 3.9	BR	El sistema de control ha de protegir la informació i les eines d'auditoria (si n'hi ha) contra l'accés, la modificació i l'eliminació no autoritzats.
FR4. Confidencialitat de les dades		
SR 4.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació (especialment en dispositius portàtils) per a la qual s'admet l'autorització explícita de lectura, estigui en repòs o en trànsit. La tècnica triada ha de tenir en compte

		les possibles ramificacions en el rendiment del sistema de control i la capacitat de recuperar-se després d'una fallada del sistema o un atac.
	RE1	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació en repòs i en sessions amb accés remot a través d'una xarxa que no és de confiança.
SR 4.2	BR	El sistema de control ha de proporcionar la capacitat d'eliminar tota la informació amb autorització explícita de lectura dels components que s'hagin d'alliberar del servei actiu i/o llocs fora de servei.
SR 4.3	BR	Si es requereix l'ús de criptografia, el sistema de control ha d'usar algorismes criptogràfics, grandàries de clau i mecanismes per a l'establiment i gestió de claus conformement a les pràctiques i recomanacions de seguretat comunament acceptades en el sector que es troben en documents com la publicació especial NIST SP800-57.
FR5. Flux de dades restringides		
SR 5.1	BR	El sistema de control ha de proporcionar la capacitat de segmentar de manera lògica les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control d'altres xarxes del sistema de control.
	RE1	El sistema de control ha de proporcionar la capacitat de segmentar físicament les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control de les xarxes no crítiques del sistema de control.
SR 5.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones i conductes de risc. Com a part d'una estratègia de protecció de defensa total, s'haurien de dividir els sistemes de control de major impacte en zones separades utilitzant conductes per restringir o prohibir l'accés a la xarxa conformement a les polítiques i procediments de seguretat i a una avaluació de riscos.
	RE1	El sistema de control ha de proporcionar serveis de xarxa a xarxes el sistema de control, siguin crítiques o no, sense que s'estableixi una connexió amb xarxes no pertanyents al sistema de control.
SR 5.3	BR	Un sistema de control ha de proporcionar la capacitat d'evitar la recepció de missatges de propòsit general (correu electrònic, xarxes socials o qualsevol altre sistema de missatgeria) entre persones procedents d'usuaris o sistemes externs al sistema de control.
SR 5.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la partició de dades (per mitjans físics o lògics), aplicacions i serveis sobre la base de la seva criticitat per facilitar la implementació d'un model de zonificació.
FR6. Resposta oportuna als incidents		
SR 6.1	BR	El sistema de control ha de proporcionar la capacitat que les persones i/o les eines autoritzades accedeixin als registres d'auditoria en mode de lectura.
SR 6.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar contínuament el rendiment del mecanisme de seguretat utilitzant pràctiques i recomanacions comunament acceptades en el sector de la seguretat per detectar, caracteritzar i reportar infraccions de seguretat de manera oportuna.

FR7. Disponibilitat dels recursos		
SR 7.1	BR	El sistema de control ha de proporcionar la capacitat de funcionar en mode degradat durant un esdeveniment de denegació de servei. Un esdeveniment de denegació de servei en el sistema de control no hauria d'afectar negativament cap sistema relacionat amb la seguretat.
	RE1	El sistema de control ha de proporcionar la capacitat de gestionar les càrregues de comunicació (per exemple, limitant la taxa) per mitigar els efectes dels tipus de desbordament d'informació dels esdeveniments de denegació de servei.
SR 7.2	BR	El sistema de control ha de proporcionar la capacitat de limitar l'ús de recursos per part de les funcions de seguretat per evitar l'esgotament dels recursos.
SR 7.3	BR	El sistema de control ha de facilitar la identitat i ubicació dels arxius crítics i la capacitat de dur a terme còpies de seguretat de la informació de l'usuari i del sistema (incloent-hi informació sobre l'estat del sistema) sense que això afecti les operacions habituals.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar la fiabilitat dels mecanismes de còpies de seguretat.
SR 7.4	BR	El sistema de control ha de proporcionar la capacitat de recuperar-se i reconstituir-se fins a un estat segur conegut després d'una interrupció o fallada. Un estat segur conegut significa que s'atribueixen a tots els paràmetres del sistema (siguin predeterminats o configurables) valors segurs, es reinstal·len els pedaços crítics per a la seguretat, es restableixen els ajustos de configuració relacionats amb la seguretat, es disposa de la documentació i els procediments operatius del sistema, es reinstal·la i configura l'aplicació i el programari del sistema amb ajustos segurs, es carrega la informació de les còpies de seguretat més recents i conegudes, i se sotmet a assaig i es comprova el funcionament del sistema íntegrament.
SR 7.5	BR	El sistema de control ha de proporcionar la capacitat de canviar d'una font d'alimentació d'emergència i a aquesta sense que això afecti l'estat de seguretat existent o un mode degradat documentat.
SR 7.6	BR	El sistema de control ha de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El sistema de control ha de proporcionar una interfície als ajustos de configuració de xarxa i seguretat desplegats actualment.
SR 7.7	BR	El sistema de control ha de proporcionar la capacitat de prohibir i/o restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.
SR 7.8	BR	El sistema de control ha de proporcionar la capacitat d'informar de la llista actual de components instal·lats i de les seves propietats associades.

Requisits de seguretat dels components generals

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
CR 1.1	BR	Els components han de proporcionar la capacitat d'identificar i autenticar tots els usuaris en totes les interfícies que permetin el repartiment de tasques i els privilegis mínims. Es pot proporcionar a escala component o a escala sistema.
	RE1	Els components han de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris humans.
CR 1.2	BR	Els components han de proporcionar la capacitat d'identificar-se a si mateixos i autenticar qualsevol altre component d'acord amb el requisit del sistema SR 1.2 de la Norma IEC62443-3-3. Si el component, com en el cas d'una aplicació, s'executa en el context d'un usuari humà, a més, la identificació i autenticació de l'usuari humà d'acord amb el requisit del sistema SR1.1 de la Norma IEC62443-3-3 pot formar part del procés d'identificació i autenticació del component cap als altres components.
CR 1.3	BR	Els components han de proporcionar la capacitat de permetre la gestió de tots els comptes de forma directa o integrant-se en un sistema que gestioni els comptes.
CR 1.4	BR	Els components han de proporcionar la capacitat d'integrar-se en un sistema que admeti la gestió d'identificadors i/o la capacitat de permetre la gestió d'identificadors.
CR 1.5	BR	Els components han de proporcionar la capacitat de: a) permetre l'ús del contingut inicial de l'autenticador; b) permetre el reconeixement dels canvis en els autenticadors predeterminats realitzats al moment de la instal·lació; c) funcionar correctament amb operacions periòdiques de modificació/actualització dels autenticadors, i d) protegir els autenticadors de la divulgació i modificació no autoritzada quan s'emmagatzemen, utilitzen i transmeten.
CR 1.7	BR	Els components que utilitzin autenticació basada en contrasenya, han de proporcionar o integrar-se en un sistema que proporcioni la capacitat d'aplicar la fortalesa de les contrasenyes configurables d'acord amb directrius de contrasenyes reconegudes i provades internacionalment.
CR 1.8	BR	Quan s'utilitzi una infraestructura de clau pública (PKI), el component ha de proporcionar un sistema que ofereixi la capacitat d'interactuar i funcionar de conformitat amb el requisit del sistema SR 1.8 de la Norma IEC62443-3-3 o integrar-se en aquest sistema.
CR 1.9	BR	Els components que utilitzin autenticació basada en clau pública han de subministrar-se directament o integrar-se en un sistema que ofereixi la capacitat en el mateix entorn del sistema de control per: a) validar els certificats comprovant la validesa de la signatura d'un certificat determinat; b) validar la cadena de certificats o, en el cas dels certificats autosignats, desplegar certificats d'entitat final a tots els hosts que es comuniquen amb el subjecte al qual s'emet el certificat; c) validar els certificats comprovant l'estat de revocació d'un certificat determinat; d) establir el control de l'usuari sobre la clau privada corresponent; e) assignar la identitat autenticada a un usuari, i f) garantir que els algorismes i claus utilitzats per a l'autenticació de clau pública compleixen els requisits establerts.

CR 1.10	BR	Quan un component ofereixi la capacitat d'autenticació, el component ha d'oferir la capacitat d'ocultar la retroalimentació de la informació de l'autenticador durant el procés d'autenticació.
CR 1.11	BR	Quan un component ofereixi una capacitat d'autenticació, el component ha de proporcionar la capacitat de: a) aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per part de qualsevol usuari durant un període de temps configurable; b) denegar l'accés durant un període de temps específic o fins que un administrador el desbloquegi, quan s'hagi arribat a aquest límit. Un administrador pot desbloquejar un compte abans de la caducitat del període de temps d'espera.
CR 1.12	BR	Quan un component proporcioni un accés d'usuari humà local/IHM, ha de proporcionar la capacitat de mostrar un missatge de notificació d'ús del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge de notificació d'ús del sistema.
CR 1.14	BR	Per als components que utilitzin claus simètriques, el component ha de proporcionar la capacitat de: a) establir la confiança mútua utilitzant la clau simètrica; b) emmagatzemar de forma segura el secret compartit; c) restringir l'accés al secret compartit, i d) garantir que els algorismes i les claus utilitzats per a l'autenticació de clau simètrica compleixen els requisits establerts.
FR2. Control d'ús		
CR 2.1	BR	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris identificats i autenticats en funció de les responsabilitats que se'ls hagin assignat.
	RE1	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris en funció de les responsabilitats que se'ls assignin i del privilegi mínim.
	RE2	Els components, directament o a través d'un mecanisme de compensació de seguretat, han de proporcionar un rol autoritzat per definir i modificar l'assignació de permisos a rols per a tots els usuaris humans. Els rols no haurien de limitar-se a jerarquies fixes niades en les quals un rol de nivell superior sigui un superconjunt d'un rol menys privilegiat. Per exemple, un administrador de sistema no hauria d'incloure necessàriament privilegis d'operador.
CR 2.2	BR	Si un component admet l'ús a través d'interfícies sense fils, ha de proporcionar la capacitat d'integrar-se en el sistema que admet l'autorització d'ús, la supervisió i les restriccions d'acord amb les pràctiques industrials comunament acceptades.
CR 2.5	BR	Si un component proporciona una interfície per a un usuari humà, tant si s'hi accedeix localment com a través d'una xarxa, el component ha de proporcionar la capacitat de: a) protegir-se contra l'accés posterior iniciant un bloqueig de sessió després d'un període de temps configurable d'inactivitat o mitjançant la iniciació manual per part de l'usuari i b) mantenir el bloqueig de la sessió fins que l'usuari propietari de la sessió, o un altre usuari humà autoritzat, restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats.
CR 2.6	BR	Si un component admet sessions remotes, ha de proporcionar la capacitat de finalitzar una sessió remota automàticament després d'un període d'inactivitat configurable manualment per part d'una autoritat local o manualment per part de l'usuari que va iniciar la sessió.

CR 2.8	BR	Els components han de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: a) control d'accés; b) errors de sol·licitud; c) esdeveniments del sistema de control; d) esdeveniment de còpia de seguretat i restauració; e) canvis de configuració, i f) esdeveniments de registre d'auditoria. Els registres d'auditoria individuals han d'incloure: a) marca de temps; b) font (dispositiu d'origen, procés de programari o compte d'usuari humà); c) categoria; d) tipus; e) ID de l'esdeveniment, i f) resultat de l'esdeveniment.
CR 2.9	BR	Els components han de: a) proporcionar la capacitat d'assignar una capacitat d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres, i b) proporcionar mecanismes per protegir contra una fallada del component quan arribi a la capacitat d'emmagatzematge de dades d'auditoria o la superi.
CR 2.10	BR	Els components han de: a) proporcionar la capacitat de protegir contra la pèrdua de serveis i funcions essencials en cas que falli el processament d'una auditoria, i b) proporcionar la capacitat per permetre les accions apropiades en resposta a una fallada en el processament d'una auditoria d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
CR 2.11	BR	Els components han de proporcionar la capacitat de crear marques de temps (incloent-hi data i hora) per al seu ús en els registres d'auditoria.
	RE1	Els components han de proporcionar la capacitat de crear marques de temps que estiguin sincronitzades amb una font de temps de tot el sistema.
CR 2.12	BR	Si un component proporciona una interfície per a un usuari humà, el component ha de proporcionar la capacitat de determinar si un determinat usuari humà ha realitzat una determinada acció. Els elements de control que no puguin permetre aquesta capacitat s'han d'enumerar en els documents dels components.
FR3. Integritat del sistema		
CR 3.1	BR	Els components han de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el component per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
	RE1	Els components han de proporcionar la capacitat de verificar l'autenticitat de la informació rebuda durant la comunicació.
CR 3.3	BR	Els components han de proporcionar la capacitat de permetre la verificació de l'operació prevista de les funcions de seguretat d'acord amb el requisit del sistema.
CR 3.4	BR	Els components han de proporcionar la capacitat de fer o permetre verificacions d'integritat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'integritat.

	RE1	Els components han de proporcionar la capacitat de fer o permetre verificacions d'autenticitat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'autenticitat.
CR 3.5	BR	Els components han de validar la sintaxi, la longitud i el contingut de qualsevol dada d'entrada que s'utilitzi com a entrada de control de processos industrials o entrada a través d'interfícies externes que tinguin un impacte directe en l'acció del component.
CR 3.6	BR	Els components que es connecten físicament o lògicament a un procés d'automatització han de proporcionar la capacitat d'establir sortides a un estat predeterminat si no es pot mantenir el funcionament normal definit pel proveïdor de components.
CR 3.7	BR	Els components han d'identificar i tractar les condicions d'error de manera que no proporcionin informació que pugui ser aprofitada per adversaris per atacar el sistema de control.
CR 3.8	BR	Els components han de proporcionar mecanismes per protegir la integritat de les sessions de comunicació, incloent-hi: a) la capacitat d'invalidar identificadors de sessió quan l'usuari tanqui la sessió o després de qualsevol altre tipus de tancament de sessió (incloses les sessions de navegació); b) la capacitat de generar un identificador de sessió únic per a cada sessió i reconèixer només els identificadors de sessió generats pel sistema, i c) la capacitat de generar identificadors de sessió únics amb fonts d'aleatorietat comunament acceptades.
CR 3.9	BR	Els components han de protegir la informació d'auditoria, els registres d'auditoria i les eines d'auditoria (si n'hi ha) contra l'accés, la modificació i l'eliminació no autoritzats.
FR4. Confidencialitat de les dades		
CR 4.1	BR	Els components han de: a) proporcionar la capacitat de protegir la confidencialitat de la informació en repòs per a la qual s'admet l'autorització explícita de lectura, i b) permetre la protecció de la confidencialitat de la informació en trànsit, com defineix el requisit del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Els components han de proporcionar la capacitat d'eliminar tota la informació amb autorització explícita de lectura dels components que s'hagin d'alliberar del servei actiu i/o posar fora de servei.
CR 4.3	BR	Si es requereix l'ús de criptografia, el component ha d'utilitzar mecanismes de seguretat criptogràfica d'acord amb pràctiques i recomanacions de seguretat internacionalment reconegudes i provades.

FR5. Flux de dades restringides		
CR 5.1	BR	Els components han de permetre una xarxa segmentada que admeti zones i conductes, segons sigui necessari, per permetre una arquitectura de xarxa més àmplia basada en la segmentació lògica i la criticitat.
FR6. Resposta oportuna als incidents		
CR 6.1	BR	Els components han de proporcionar la capacitat perquè les persones i/o les eines autoritzades puguin accedir als registres d'auditoria de només lectura.
CR 6.2	BR	Els components han de proporcionar la capacitat de ser contínuament supervisats utilitzant pràctiques i recomanacions comunament acceptades en el sector de la seguretat per detectar, caracteritzar i reportar infraccions de seguretat de manera oportuna.
FR7. Disponibilitat dels recursos		
CR 7.1	BR	Els components han de proporcionar la capacitat de mantenir les funcions essencials quan operin en mode degradat com a resultat d'un esdeveniment de denegació de servei.
	RE1	Els components han de proporcionar la capacitat de mitigar els efectes dels tipus d'esdeveniments de denegació de servei de desbordament d'informació i/o missatges.
CR 7.2	BR	Els components han de proporcionar la capacitat de limitar l'ús de recursos en les funcions de seguretat per protegir contra l'esgotament dels recursos.
CR 7.3	BR	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
	RE1	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
CR 7.4	BR	Els components han de proporcionar la capacitat de poder-se recuperar i reconstituir fins a un estat segur conegut després d'una interrupció o fallada.
CR 7.6	BR	Els components han de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El component ha de proporcionar una interfície amb els ajustos de configuració de xarxa i seguretat actualment desplegats.
CR 7.7	BR	Els components han de proporcionar la capacitat de restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.
CR 7.8	BR	Els components han de proporcionar la capacitat de permetre un inventari de components del sistema de control d'acord amb el requisit del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisits de seguretat del component pel que fa a programari

ID req	BR/RE	Explicació
SAR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
	RE1	L'aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat que permeti al dispositiu controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
SAR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.

Requisits de seguretat per als dispositius integrats (PLC, IED)

ID req	BR/RE	Explicació
EDR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
	RE1	El dispositiu integrat ha de proporcionar la capacitat d'aplicar una política de seguretat que li permeti controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
EDR 2.13	BR	Els dispositius integrats han de protegir contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, depuració JTAG).
EDR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.
EDR 3.10	BR	El dispositiu integrat ha d'admetre la capacitat de ser actualitzat i sotmetre's a una pujada de nivell.
	RE1	El dispositiu integrat ha de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell del programari abans de la instal·lació.

EDR 3.11	BR	El dispositiu integrat ha d'oferir mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
EDR 3.12	BR	Els dispositius integrats han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
EDR 3.13	BR	Els dispositius integrats han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
EDR 3.14	BR	Els dispositius integrats han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per a l'arrencada del component i els processos en temps d'execució abans del seu ús.
	RE1	Els dispositius integrats han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.

Requisits de seguretat per als dispositius host

ID req	BR/RE	Explicació
HDR 2.4	BR	En cas que un dispositiu host utilitzi tecnologies de codi mòbil, aquest dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu host: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a carregar codi mòbil en el dispositiu host, i c) controlar l'execució del codi basant-se en comprovacions d'integritat en el codi mòbil i abans que el codi s'executi.
	RE1	El dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat que li permeti controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
HDR 2.13	BR	Els dispositius host han de protegir-se contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, la depuració JTAG).
HDR 3.2	BR	Els dispositius host han de comptar amb mecanismes homologats pel proveïdor de productes del sistema de control que garanteixin la protecció contra codis maliciosos. El proveïdor del producte del sistema de control ha de documentar qualsevol requisit especial de configuració relacionat amb la protecció contra el codi maliciós.
	RE1	El dispositiu host ha d'informar automàticament de les versions del programari i dels arxius de protecció contra el codi maliciós en ús (com a part de la funció de registre general).
HDR 3.10	BR	Els dispositius host han de comptar amb la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.

	RE1	Els dispositius host han de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell de programari abans de la instal·lació.
HDR 3.11	BR	Els dispositius host han d'oferir la capacitat d'admetre mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
HDR 3.12	BR	Els dispositius host han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
HDR 3.13	BR	Els dispositius host han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
HDR 3.14	BR	Els dispositius host han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.
	RE1	Els dispositius host han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.

Requisits de seguretat per als dispositius de xarxa

ID req	BR/RE	Explicació
NDR 1.6	BR	Un dispositiu de xarxa que permeti la gestió d'accés sense fil ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris (persones, processos de programari o dispositius) que participen en la comunicació sense fil.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris (persones, processos o dispositius de programari) que participin en la comunicació sense fil.
NDR 1.13	BR	El dispositiu de xarxa que permeti l'accés de dispositius a una xarxa ha de poder supervisar i controlar tots els mètodes d'accés al dispositiu de xarxa a través de xarxes que no són de confiança.
NDR 2.4	BR	En cas que un dispositiu de xarxa utilitzi tecnologies de codi mòbil, ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu de xarxa: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil cap a / des del dispositiu de xarxa, i c) controlar l'execució del codi basant-se en verificacions d'integritat abans que el codi s'executi.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat d'aplicar una política de seguretat que permeti al dispositiu controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.

NDR 2.13	BR	Els dispositius de xarxa han de protegir-se contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, la depuració JTAG).
NDR 3.2	BR	El dispositiu de xarxa ha de proporcionar protecció contra codis maliciosos.
NDR 3.10	BR	Els dispositius de xarxa han d'admetre la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
	RE1	Els dispositius de xarxa han de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell de programari abans de la instal·lació.
NDR 3.11	BR	Els dispositius de xarxa han d'oferir mecanismes de detecció i resistència a la manipulació per protegir contra l'accés físic no autoritzat al dispositiu.
NDR 3.12	BR	Els dispositius de xarxa han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
NDR 3.13	BR	Els dispositius de xarxa han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
NDR 3.14	BR	Els dispositius de xarxa han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.
	RE1	Els dispositius de xarxa han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.
NDR 5.2	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones de risc i conductes.
	RE1	El component de xarxa ha de proporcionar la capacitat de denegar trànsit de xarxa per defecte i permetre trànsit de xarxa per excepció (també denominat "denegar-ho tot, permís per excepció").
NDR 5.3	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de protegir contra la recepció de missatges de propòsit general entre persones rebuts d'usuaris o sistemes externs al sistema de control.

ANNEX III: REQUISITS PER A NIVELL SL3

Requisits de seguretat del sistema

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
SR 1.1	BR	Tots els usuaris que accedeixin al sistema han de ser identificats i autenticats tant a escala de sistemes com d'aplicació; pot ser a través de contrasenyes, dispositius d'accés o multifactor (combinació de les anteriors).
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris humans.
	RE2	El sistema de control ha de proporcionar la capacitat d'emprar l'autenticació multifactor per permetre l'accés d'usuaris humans al sistema de control a través d'una xarxa que no és de confiança.
SR 1.2	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els processos de programari i dispositius. Aquesta capacitat ha de fer complir aquesta identificació i autenticació en totes les interfícies que proporcionin accés al sistema de control per permetre els privilegis mínims, de conformitat amb les polítiques i procediments de seguretat aplicables.
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els processos de programari i dispositius.
SR 1.3	BR	El sistema de control ha de tenir la capacitat de gestionar comptes d'usuaris (agregar-ne, eliminar-ne, modificar-ne o desactivar-ne) establint condicions per pertànyer a un grup i l'assignació d'autoritzacions. Només s'admetran comptes compartits quan, per condicions del sistema, s'estableixi en l'anàlisi de risc, encara que s'hauran d'establir contramesures i documentar-les.
	RE1	El sistema de control ha de proporcionar la capacitat d'admetre la gestió de comptes unificada.
SR 1.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la gestió dels identificadors (permet operar dins d'un domini o zona de control específic del sistema) per usuari, grup, rol o interfície del sistema de control.
SR 1.5	BR	El sistema de control ha de proporcionar la capacitat de: 1) iniciar el contingut de l'autenticador; 2) canviar tots els autenticadors predeterminats; 3) canviar/actualitzar els autenticadors; 4) protegir-los contra la divulgació i modificació no autoritzada. Exemples d'autenticadors són claus físiques, targetes d'accés, claus privades, entre d'altres.
	RE1	Per als usuaris de processos de programari i dispositius, el sistema de control ha de proporcionar la capacitat de protegir els autenticadors pertinents a través de mecanismes de maquinari.
SR 1.6	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris que participin en una comunicació sense fil. Exemples de tecnologies sense fils són Bluetooth, infrarojos, encaminadors mòbils, etc.

	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris (persones, processos de programari o dispositius) que participin en la comunicació sense fil.
SR 1.7	BR	En els sistemes de control que utilitzin la contrasenya com a mitjà d'autenticació, s'ha d'aplicar una fortalesa configurable sobre la base de la longitud mínima i la varietat de caràcters. S'aplicarà vigència màxima per a les contrasenyes i es notificarà quan aquesta expiri. Aquesta protecció es pot millorar limitant la reutilització de les contrasenyes.
	RE1	El sistema de control ha de proporcionar la capacitat d'evitar que un compte d'un usuari humà determinat reutilitzi una contrasenya per a un nombre configurable de generacions. A més, el sistema de control ha de proporcionar la capacitat d'aplicar restriccions de vigència mínimes i màximes de les contrasenyes als usuaris humans. Aquestes capacitats s'han d'ajustar a les pràctiques comunament acceptades en el sector de la seguretat.
SR 1.8	BR	En els casos en què s'utilitzi una PKI, el sistema de control ha de proporcionar la capacitat que una PKI funcioni conformement a les millors pràctiques comunament acceptades o obtenir certificats de clau pública d'una PKI existent. El registre d'aquesta ha d'incloure l'autorització d'un supervisor que verifiqui la identitat del titular del certificat i que garanteixi que s'emet a l'usuari previst.
SR 1.9	BR	En el cas dels sistemes de control que utilitzin autenticació de clau pública (PKI), el sistema de control ha de proporcionar la capacitat de: l) validar els certificats comprovant la validesa de la signatura d'un certificat determinat; m) validar els certificats a través d'una ruta de certificació a una CA acceptada o, en el cas dels certificats autosignats, desplegant certificats d'entitat final a tots els hosts que es comuniquen amb el subjecte al qual s'emet el certificat; n) validar els certificats comprovant l'estat de revocació d'un certificat determinat; o) establir el control de l'usuari sobre la clau privada corresponent, i p) assignar la identitat autenticada a un usuari.
	RE1	El sistema de control ha de proporcionar la capacitat de protegir les claus privades pertinents a través de mecanismes de maquinari conformement a les pràctiques i recomanacions comunament acceptades en el sector de la seguretat.
SR 1.10	BR	El sistema de control ha de proporcionar la capacitat d'ocultar la retroalimentació de la informació d'autenticació durant el procés. No ha de donar pistes sobre les fallades d'autenticació com, per exemple, "nom d'usuari desconegut".
SR 1.11	BR	El sistema de control ha de proporcionar la capacitat d'aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per qualsevol usuari dins d'un període configurable de temps.
SR 1.12	BR	El sistema de control ha de proporcionar la capacitat de mostrar un missatge d'avís del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge d'avís d'ús del sistema.
SR 1.13	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança. Ha de permetre l'accés només quan s'hi estigui autoritzat i restringir l'accés des de connexions telefòniques o no autoritzades. És possible que els procediments requereixin l'autenticació multifactor per permetre l'accés remot.
	RE1	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança.

FR2. Control d'ús		
SR 2.1	BR	El sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris humans per controlar l'ús del sistema de control a fi d'admetre el repartiment de tasques i el privilegi mínim. Cal verificar que les accions de l'usuari estan permeses segons el rol assignat i permetre que només les persones qualificades i autoritzades facin canvis en els components del sistema.
	RE1	En totes les interfícies, el sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris (persones, processos de programari i dispositius) per controlar l'ús del sistema de control amb la finalitat d'admetre el repartiment de tasques i el privilegi mínim.
	RE2	El sistema de control ha de proporcionar la capacitat que un usuari o rol autoritzat defineixi i modifiqui l'assignació de permisos a rols per a tots els usuaris humans.
	RE3	El sistema de control ha d'admetre el permís manual del supervisor de les autoritzacions actuals dels usuaris humans per a un temps o seqüència d'esdeveniments configurables.
SR 2.2	BR	El sistema de control ha de proporcionar la capacitat d'autoritzar, supervisar i aplicar les restriccions d'ús per a les connexions sense fils al sistema de control conformement a les pràctiques comunament acceptades en el sector de la seguretat.
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i informar de la presència de dispositius sense fils no autoritzats que transmetin dins de l'entorn físic del sistema de control.
SR 2.3	BR	El sistema de control ha de proporcionar la capacitat d'aplicar automàticament les restriccions d'ús configurables, que inclouen: a) prevenir l'ús de dispositius portàtils i mòbils; b) requerir autorització basada en un context específic, i c) restringir la transferència de codis i dades a/de dispositius portàtils i mòbils.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar que els dispositius portàtils i mòbils que intenten connectar-se a la zona en compleixin els requisits de seguretat.
SR 2.4	BR	El sistema de control ha de proporcionar la capacitat d'aplicar restriccions d'ús per a les tecnologies de codi mòbil basades en la possibilitat que causin danys al sistema de control, incloent-hi: a) prevenir l'execució del codi mòbil; b) requerir processos d'autenticació i autorització adequats per a l'origen del codi; c) restringir la transferència del codi mòbil al/del sistema de control, i d) supervisar l'ús del codi mòbil.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar la integritat del codi mòbil abans d'autoritzar que s'executi el codi.
SR 2.5	BR	El sistema de control ha de proporcionar la capacitat d'evitar un accés posterior iniciant un bloqueig de la sessió després d'un període de temps configurable d'inactivitat o mitjançant iniciació manual. La sessió ha de continuar bloquejada fins que l'usuari autoritzat restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats. En els casos en els quals el sistema

		de control no pugui admetre el bloqueig de la sessió, l'entitat responsable hauria d'emprar les contramesures compensatòries que es considerin adequades, com majors mesures de seguretat física i auditories.
SR 2.6	BR	El sistema de control ha de proporcionar la capacitat de finalitzar una sessió remota, sigui automàticament després d'un període d'inactivitat configurable o manualment per part de l'usuari que va iniciar la sessió.
SR 2.7	BR	El sistema de control ha de proporcionar la capacitat de limitar el nombre de sessions simultànies per interfície per a qualsevol usuari determinat a un nombre configurable de sessions.
SR 2.8	BR	El sistema de control ha de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: control d'accés, errors de sol·licitud, esdeveniments del sistema operatiu, esdeveniments del sistema de control, esdeveniments de còpies de seguretat i restauració, canvis en la configuració, activitat potencial de reconeixement i esdeveniments del registre d'auditoria. Els registres individuals d'auditoria han d'incloure la marca de temps, font (dispositiu, procés de programari o compte d'usuari humà d'origen), categoria, tipus, identificador de l'esdeveniment i resultat de l'esdeveniment.
	RE1	El sistema de control ha de proporcionar la capacitat de gestionar de manera centralitzada els esdeveniments d'auditoria i d'elaborar registres d'auditoria de múltiples components a través del sistema de control en una pista d'auditoria per a tot el sistema (lògica o física) amb correlació de temps. El sistema de control ha de proporcionar la capacitat d'exportar aquests registres d'auditories en formats habituals per a la indústria perquè s'analitzin amb les eines comercials habituals d'anàlisis de registres, com per exemple l'administració d'esdeveniments i informació de seguretat (SIEM).
SR 2.9	BR	El sistema de control ha d'assignar una capacitat suficient d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres i la configuració del sistema. El sistema de control ha de proporcionar mecanismes d'auditoria per reduir la possibilitat que s'excedeixi aquesta capacitat.
	RE1	El sistema de control ha de proporcionar la capacitat d'emetre un avís quan el volum d'emmagatzematge de registres d'auditoria assignat assoleixi un percentatge configurable de capacitat màxima d'emmagatzematge de registres d'auditoria.
SR 2.10	BR	El sistema de control ha de proporcionar la capacitat d'alertar el personal i evitar la pèrdua de serveis i funcions essencials en cas que falli el processament d'auditories. El sistema de control ha de proporcionar la capacitat d'admetre les accions apropiades en resposta a una fallada en el processament d'auditories d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
SR 2.11	BR	El sistema de control ha de proporcionar marques de temps (data i hora) per a la generació de registres d'auditoria. Cal evitar que les fonts horàries sofreixin alteracions no autoritzades.
	RE1	El sistema de control ha de proporcionar la capacitat de sincronitzar els rellotges interns del sistema a una freqüència configurable.
SR 2.12	BR	El sistema de control ha de proporcionar la capacitat de determinar si un usuari humà ha realitzat una acció concreta.

FR3. Integritat del sistema		
SR 3.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el sistema per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes criptogràfics per reconèixer canvis d'informació durant la comunicació.
SR 3.2	BR	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció per prevenir, detectar, mitigar i informar dels efectes d'un codi maliciós o de programari no autoritzat. El sistema de control ha de proporcionar la capacitat d'actualitzar els mecanismes de protecció.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció contra codis maliciosos en tots els punts d'entrada i sortida.
	RE2	El sistema de control ha de proporcionar la capacitat de gestionar els mecanismes de protecció contra codis maliciosos.
SR 3.3	BR	El sistema de control ha de proporcionar la capacitat d'admetre la verificació del funcionament previst de les funcions de seguretat (mesures d'antivirus, identificació, detecció d'intrusos i auditories) i informar de les anomalies que es produeixin durant els assajos d'acceptació en fàbrica i en emplaçament i durant el manteniment programat. Les funcions de seguretat han d'incloure totes les funcions que siguin necessàries per complir els requisits de seguretat especificats en aquesta norma.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes automàtics per facilitar la gestió de la verificació de la seguretat durant els assajos d'acceptació en fàbrica i en emplaçament i durant el manteniment programat.
SR 3.4	BR	El sistema de control ha de proporcionar la capacitat de detectar, registrar, informar i protegir contra canvis no autoritzats en el programari i en la informació en repòs.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar eines automatitzades que notifiquin un conjunt configurable de receptors quan es produeixin discrepàncies durant la verificació de la integritat.
SR 3.5	BR	El sistema de control ha de validar la sintaxi i el contingut de qualsevol entrada que s'utilitzi com a entrada de control de processos industrials o entrada que tingui un impacte directe en l'acció del sistema de control. Les directrius que cal tenir en compte haurien d'incloure la Code Review Guide de l'Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control ha de proporcionar la capacitat d'establir el valor de sortida a un estat predeterminat si no es pot mantenir el funcionament normal com a resultat d'un atac.
SR 3.7	BR	El sistema de control ha d'identificar i tractar les condicions d'error de manera que s'hi pugui aplicar un remei efectiu. Això s'ha de fer sense proporcionar informació que pugui ser aprofitada per adversaris per atacar el sistema de control, tret que sigui necessari per resoldre els problemes de manera oportuna.

SR 3.8	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de les sessions. El sistema de control ha de rebutjar qualsevol ús per part d'identificadors de sessió no vàlids.
	RE1	El sistema de control ha de proporcionar la capacitat d'anul·lar els identificadors de sessió quan l'usuari tanqui la sessió o després de qualsevol altre tipus de tancament de sessió (incloses les sessions de navegació).
	RE2	El sistema de control ha de proporcionar la capacitat de generar un identificador de sessió únic per a cada sessió i considerar no vàlids tots els identificadors de sessió imprevists.
SR 3.9	BR	El sistema de control ha de protegir la informació i les eines d'auditoria (si n'hi ha) contra l'accés, la modificació i l'eliminació no autoritzats.
FR4. Confidencialitat de les dades		
SR 4.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació (especialment en dispositius portàtils) per a la qual s'admet l'autorització explícita de lectura, estigui en repòs o en trànsit. La tècnica triada ha de tenir en compte les possibles ramificacions en el rendiment del sistema de control i la capacitat de recuperar-se després d'una fallada del sistema o un atac.
	RE1	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació en repòs i en sessions amb accés remot a través d'una xarxa que no és de confiança.
SR 4.2	BR	El sistema de control ha de proporcionar la capacitat d'eliminar tota la informació amb autorització explícita de lectura dels components que s'hagin d'alliberar del servei actiu i/o llocs fora de servei.
	RE1	El sistema de control ha de proporcionar la capacitat d'evitar la transferència d'informació no autoritzada i no intencionada a través de recursos de memòria compartida volàtils (no retenen la informació després de ser alliberats per a la gestió de la memòria).
SR 4.3	BR	Si es requereix l'ús de criptografia, el sistema de control ha d'usar algorismes criptogràfics, grandàries de clau i mecanismes per a l'establiment i gestió de claus conformement a les pràctiques i recomanacions de seguretat comunament acceptades en el sector que es troben en documents com la publicació especial NIST SP800-57.
FR5. Flux de dades restringides		
SR 5.1	BR	El sistema de control ha de proporcionar la capacitat de segmentar de manera lògica les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control d'altres xarxes del sistema de control.
	RE1	El sistema de control ha de proporcionar la capacitat de segmentar físicament les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control de les xarxes no crítiques del sistema de control.
	RE2	El sistema de control ha de proporcionar serveis de xarxa a xarxes el sistema de control, siguin crítiques o no, sense que s'estableixi una connexió amb xarxes no pertanyents al sistema de control.

SR 5.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones i conductes de risc. Com a part d'una estratègia de protecció de defensa total, s'haurien de dividir els sistemes de control de major impacte en zones separades utilitzant conductes per restringir o prohibir l'accés a la xarxa conformement a les polítiques i procediments de seguretat i a una avaluació de riscos.
	RE1	El sistema de control ha de proporcionar serveis de xarxa a xarxes el sistema de control, siguin crítiques o no, sense que s'estableixi una connexió amb xarxes no pertanyents al sistema de control.
	RE2	El sistema de control ha de proporcionar la capacitat d'evitar qualsevol comunicació a través del límit del sistema de control (també denominat mode illa).
	RE3	El sistema de control ha de proporcionar la capacitat d'evitar qualsevol comunicació a través del límit del sistema de control quan es produeixi una fallada operativa dels mecanismes de protecció de límits (també denominat tancament en cas de fallada). Aquesta funció de "tancament en cas de fallada" ha de dissenyar-se de tal forma que no interfereixi en el funcionament d'un sistema instrumentat de seguretat (SIS) o en altres funcions relacionades amb la seguretat.
SR 5.3	BR	Un sistema de control ha de proporcionar la capacitat d'evitar la recepció de missatges de propòsit general (correu electrònic, xarxes socials o qualsevol altre sistema de missatgeria) entre persones procedents d'usuaris o sistemes externs al sistema de control.
	RE1	El sistema de control ha de proporcionar la capacitat d'evitar tant la transmissió com la recepció de missatges entre persones de propòsit general.
SR 5.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la partició de dades (per mitjans físics o lògics), aplicacions i serveis sobre la base de la seva criticitat per facilitar la implementació d'un model de zonificació.
FR6. Resposta oportuna als incidents		
SR 6.1	BR	El sistema de control ha de proporcionar la capacitat que les persones i/o les eines autoritzades accedeixin als registres d'auditoria en mode de lectura.
	RE1	El sistema de control ha de permetre l'accés mitjançant programació als registres d'auditoria utilitzant una interfície de programació d'aplicacions (API).
SR 6.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar contínuament el rendiment del mecanisme de seguretat utilitzant pràctiques i recomanacions comunament acceptades en el sector de la seguretat per detectar, caracteritzar i reportar infraccions de seguretat de manera oportuna.
FR7. Disponibilitat dels recursos		
SR 7.1	BR	El sistema de control ha de proporcionar la capacitat de funcionar en mode degradat durant un esdeveniment de denegació de servei. Un esdeveniment de denegació de servei en el sistema de control no hauria d'afectar negativament cap sistema relacionat amb la seguretat.

	RE1	El sistema de control ha de proporcionar la capacitat de gestionar les càrregues de comunicació (per exemple, limitant la taxa) per mitigar els efectes dels tipus de desbordament d'informació dels esdeveniments de denegació de servei.
	RE2	El sistema de control ha de proporcionar la capacitat de restringir la possibilitat que qualsevol usuari provoqui esdeveniments de denegació de servei que puguin afectar altres sistemes de control o xarxes.
SR 7.2	BR	El sistema de control ha de proporcionar la capacitat de limitar l'ús de recursos per part de les funcions de seguretat per evitar l'esgotament dels recursos.
SR 7.3	BR	El sistema de control ha de facilitar la identitat i ubicació dels arxius crítics i la capacitat de dur a terme còpies de seguretat de la informació de l'usuari i del sistema (incloent-hi informació sobre l'estat del sistema) sense que això afecti les operacions habituals.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar la fiabilitat dels mecanismes de còpies de seguretat.
	RE2	El sistema de control ha de proporcionar la capacitat d'automatitzar la funció de còpia de seguretat sobre la base d'una freqüència configurable.
SR 7.4	BR	El sistema de control ha de proporcionar la capacitat de recuperar-se i reconstituir-se fins a un estat segur conegut després d'una interrupció o fallada. Un estat segur conegut significa que s'atribueixen a tots els paràmetres del sistema (siguin predeterminats o configurables) valors segurs, es reinstal·len els pedaços crítics per a la seguretat, es restableixen els ajustos de configuració relacionats amb la seguretat, es disposa de la documentació i els procediments operatius del sistema, es reinstal·la i configura l'aplicació i el programari del sistema amb ajustos segurs, es carrega la informació de les còpies de seguretat més recents i conegudes, i se sotmet a assaig i es comprova el funcionament del sistema íntegrament.
SR 7.5	BR	El sistema de control ha de proporcionar la capacitat de canviar d'una font d'alimentació d'emergència i a aquesta sense que això afecti l'estat de seguretat existent o un mode degradat documentat.
SR 7.6	BR	El sistema de control ha de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El sistema de control ha de proporcionar una interfície als ajustos de configuració de xarxa i seguretat desplegats actualment.
	RE1	El sistema de control ha de proporcionar la capacitat de generar un informe que enumeri els ajustos de seguretat desplegats actualment en un format llegible per una màquina.
SR 7.7	BR	El sistema de control ha de proporcionar la capacitat de prohibir i/o restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.
SR 7.8	BR	El sistema de control ha de proporcionar la capacitat d'informar de la llista actual de components instal·lats i de les seves propietats associades.

Requisits de seguretat dels components generals

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
CR 1.1	BR	Els components han de proporcionar la capacitat d'identificar i autenticar tots els usuaris en totes les interfícies que permetin el repartiment de tasques i els privilegis mínims. Es pot proporcionar a escala component o a escala sistema.
	RE1	Els components han de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris humans.
	RE2	Els components han de proporcionar la capacitat d'emprar l'autenticació multifactor per a tot l'accés d'usuaris humans al component.
CR 1.2	BR	Els components han de proporcionar la capacitat d'identificar-se a si mateixos i autenticar qualsevol altre component d'acord amb el requisit del sistema SR 1.2 de la Norma IEC62443-3-3. Si el component, com en el cas d'una aplicació, s'executa en el context d'un usuari humà, a més, la identificació i autenticació de l'usuari humà d'acord amb el requisit del sistema SR1.1 de la Norma IEC62443-3-3 pot formar part del procés d'identificació i autenticació del component cap als altres components.
	RE1	Els components han de proporcionar la capacitat d'identificar i autenticar de manera única qualsevol altre component.
CR 1.3	BR	Els components han de proporcionar la capacitat de permetre la gestió de tots els comptes de forma directa o integrant-se en un sistema que gestioni els comptes.
CR 1.4	BR	Els components han de proporcionar la capacitat d'integrar-se en un sistema que admeti la gestió d'identificadors i/o la capacitat de permetre la gestió d'identificadors.
CR 1.5	BR	Els components han de proporcionar la capacitat de: a) permetre l'ús del contingut inicial de l'autenticador; b) permetre el reconeixement dels canvis en els autenticadors predeterminats realitzats al moment de la instal·lació; c) funcionar correctament amb operacions periòdiques de modificació/actualització dels autenticadors, i d) protegir els autenticadors de la divulgació i modificació no autoritzada quan s'emmagatzemen, utilitzen i transmeten.
	RE1	Els autenticadors en els quals es recolza el component han d'estar protegits mitjançant mecanismes de maquinari (memòria protegida per contrasenya, memòria OTP, comprovacions d'integritat de maquinari de dades i mecanisme d'arrencada de seguretat de dispositius.).
CR 1.7	BR	Els components que utilitzin autenticació basada en contrasenya, han de proporcionar o integrar-se en un sistema que proporcioni la capacitat d'aplicar la fortalesa de les contrasenyes configurables d'acord amb directrius de contrasenyes reconegudes i provades internacionalment.
	RE1	Els components han de proporcionar la capacitat de protegir un compte d'usuari humà determinat contra la reutilització d'una contrasenya per a un nombre configurable de generacions, o integrar-se en un sistema que la proporcioni. A més, el component ha

		de proporcionar la capacitat d'aplicar les restriccions de vigència mínimes i màximes de la contrasenya per als usuaris humans. Aquestes capacitats s'han d'ajustar a les pràctiques comunament acceptades en el sector de la seguretat. El component hauria de proporcionar la capacitat de sol·licitar a l'usuari que canviï la seva contrasenya en un temps configurable abans de la caducitat.
CR 1.8	BR	Quan s'utilitzi una infraestructura de clau pública (PKI), el component ha de proporcionar un sistema que ofereixi la capacitat d'interactuar i funcionar de conformitat amb el requisit del sistema SR 1.8 de la Norma IEC62443-3-3 o integrar-se en aquest sistema.
CR 1.9	BR	Els components que utilitzin autenticació basada en clau pública han de subministrar-se directament o integrar-se en un sistema que ofereixi la capacitat en el mateix entorn del sistema de control per: a) validar els certificats comprovant la validesa de la signatura d'un certificat determinat; b) validar la cadena de certificats o, en el cas dels certificats autosignats, desplegar certificats d'entitat final a tots els hosts que es comuniquen amb el subjecte al qual s'emet el certificat; c) validar els certificats comprovant l'estat de revocació d'un certificat determinat; d) establir el control de l'usuari sobre la clau privada corresponent; e) assignar la identitat autenticada a un usuari, i f) garantir que els algorismes i claus utilitzats per a l'autenticació de clau pública compleixen els requisits establerts.
	RE1	Els components han de proporcionar la capacitat de protegir les claus privades crítiques de llarga durada mitjançant mecanismes de maquinari.
CR 1.10	BR	Quan un component ofereixi la capacitat d'autenticació, el component ha d'oferir la capacitat d'ocultar la retroalimentació de la informació de l'autenticador durant el procés d'autenticació.
CR 1.11	BR	Quan un component ofereixi una capacitat d'autenticació, el component ha de proporcionar la capacitat de: a) aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per part de qualsevol usuari durant un període de temps configurable; b) denegar l'accés durant un període de temps específic o fins que un administrador el desbloquegi, quan s'hagi arribat a aquest límit. Un administrador pot desbloquejar un compte abans de la caducitat del període de temps d'espera.
CR 1.12	BR	Quan un component proporcioni un accés d'usuari humà local/IHM, ha de proporcionar la capacitat de mostrar un missatge de notificació d'ús del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge de notificació d'ús del sistema.
CR 1.14	BR	Per als components que utilitzin claus simètriques, el component ha de proporcionar la capacitat de: a) establir la confiança mútua utilitzant la clau simètrica; b) emmagatzemar de forma segura el secret compartit; c) restringir l'accés al secret compartit, i d) garantir que els algorismes i les claus utilitzats per a l'autenticació de clau simètrica compleixen els requisits establerts.
	RE1	Els components han de proporcionar la capacitat de protegir claus simètriques crítiques i de llarga durada mitjançant mecanismes de maquinari.
FR2. Control d'ús		
CR 2.1	BR	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris identificats i autenticats en funció de les responsabilitats que se'ls hagin assignat.

	RE1	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris en funció de les responsabilitats que se'ls assignin i del privilegi mínim.
	RE2	Els components, directament o a través d'un mecanisme de compensació de seguretat, han de proporcionar un rol autoritzat per definir i modificar l'assignació de permisos a rols per a tots els usuaris humans. Els rols no haurien de limitar-se a jerarquies fixes niades en les quals un rol de nivell superior sigui un superconjunt d'un rol menys privilegiat. Per exemple, un administrador de sistema no hauria d'incloure necessàriament privilegis d'operador.
	RE3	Els components han de proporcionar el permís manual del supervisor durant un temps o seqüència d'esdeveniments configurables. La implementació d'un permís manual, controlat i auditat de mecanismes automatitzats en cas d'emergència o altres esdeveniments greus permet a un supervisor autoritzar un operador perquè reaccioni ràpidament davant condicions inusuals sense tancar la sessió actual i establir una nova sessió com un usuari humà amb majors privilegis.
CR 2.2	BR	Si un component admet l'ús a través d'interfícies sense fils, ha de proporcionar la capacitat d'integrar-se en el sistema que admet l'autorització d'ús, la supervisió i les restriccions d'acord amb les pràctiques industrials comunament acceptades.
CR 2.5	BR	Si un component proporciona una interfície per a un usuari humà, tant si s'hi accedeix localment com a través d'una xarxa, el component ha de proporcionar la capacitat de: a) protegir-se contra l'accés posterior iniciant un bloqueig de sessió després d'un període de temps configurable d'inactivitat o mitjançant la iniciació manual per part de l'usuari i b) mantenir el bloqueig de la sessió fins que l'usuari propietari de la sessió, o un altre usuari humà autoritzat, restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats.
CR 2.6	BR	Si un component admet sessions remotes, ha de proporcionar la capacitat de finalitzar una sessió remota automàticament després d'un període d'inactivitat configurable manualment per part d'una autoritat local o manualment per part de l'usuari que va iniciar la sessió.
CR 2.7	BR	Els components han de proporcionar la capacitat de limitar el nombre de sessions simultànies per interfície per a qualsevol usuari determinat (persona, procés de programari o dispositiu).
CR 2.8	BR	Els components han de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: a) control d'accés; b) errors de sol·licitud; c) esdeveniments del sistema de control; d) esdeveniment de còpia de seguretat i restauració; e) canvis de configuració, i f) esdeveniments de registre d'auditoria. Els registres d'auditoria individuals han d'incloure: a) marca de temps; b) font (dispositiu d'origen, procés de programari o compte d'usuari humà); c) categoria; d) tipus; e) ID de l'esdeveniment, i f) resultat de l'esdeveniment.
CR 2.9	BR	Els components han de: a) proporcionar la capacitat d'assignar una capacitat d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres, i b) proporcionar mecanismes per protegir contra una fallada del component quan arribi a la capacitat d'emmagatzematge de dades d'auditoria o la superi.
	RE1	Els components han de proporcionar la capacitat d'emetre un avís quan l'emmagatzematge de registres d'auditoria assignat arribi a un llindar de capacitat configurable.

CR 2.10	BR	Els components han de: a) proporcionar la capacitat de protegir contra la pèrdua de serveis i funcions essencials en cas que falli el processament d'una auditoria, i b) proporcionar la capacitat per permetre les accions apropiades en resposta a una fallada en el processament d'una auditoria d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
CR 2.11	BR	Els components han de proporcionar la capacitat de crear marques de temps (incloent-hi data i hora) per al seu ús en els registres d'auditoria.
	RE1	Els components han de proporcionar la capacitat de crear marques de temps que estiguin sincronitzades amb una font de temps de tot el sistema.
CR 2.12	BR	Si un component proporciona una interfície per a un usuari humà, el component ha de proporcionar la capacitat de determinar si un determinat usuari humà ha realitzat una determinada acció. Els elements de control que no puguin permetre aquesta capacitat s'han d'enumerar en els documents dels components.
FR3. Integritat del sistema		
CR 3.1	BR	Els components han de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el component per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
	RE1	Els components han de proporcionar la capacitat de verificar l'autenticitat de la informació rebuda durant la comunicació.
CR 3.3	BR	Els components han de proporcionar la capacitat de permetre la verificació de l'operació prevista de les funcions de seguretat d'acord amb el requisit del sistema.
CR 3.4	BR	Els components han de proporcionar la capacitat de fer o permetre verificacions d'integritat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'integritat.
	RE1	Els components han de proporcionar la capacitat de fer o permetre verificacions d'autenticitat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'autenticitat.
	RE2	Si el component està verificant la integritat, ha de poder notificar automàticament una entitat configurable quan descobreixi que s'ha intentat fer un canvi no autoritzat.
CR 3.5	BR	Els components han de validar la sintaxi, la longitud i el contingut de qualsevol dada d'entrada que s'utilitzi com a entrada de control de processos industrials o entrada a través d'interfícies externes que tinguin un impacte directe en l'acció del component.
CR 3.6	BR	Els components que es connecten físicament o lògicament a un procés d'automatització han de proporcionar la capacitat d'establir sortides a un estat predeterminat si no es pot mantenir el funcionament normal definit pel proveïdor de components.

CR 3.7	BR	Els components han d'identificar i tractar les condicions d'error de manera que no proporcionin informació que pugui ser aprofitada per adversaris per atacar el sistema de control.
CR 3.8	BR	Els components han de proporcionar mecanismes per protegir la integritat de les sessions de comunicació, incloent-hi: a) la capacitat d'invalidar identificadors de sessió quan l'usuari tanqui la sessió o després de qualsevol altre tipus de tancament de sessió (incloses les sessions de navegació); b) la capacitat de generar un identificador de sessió únic per a cada sessió i reconèixer només els identificadors de sessió generats pel sistema, i c) la capacitat de generar identificadors de sessió únics amb fonts d'aleatorietat comunament acceptades.
CR 3.9	BR	Els components han de protegir la informació d'auditoria, els registres d'auditoria i les eines d'auditoria (si n'hi ha) contra l'accés, la modificació i l'eliminació no autoritzats.
FR4. Confidencialitat de les dades		
CR 4.1	BR	Els components han de: a) proporcionar la capacitat de protegir la confidencialitat de la informació en repòs per a la qual s'admet l'autorització explícita de lectura, i b) permetre la protecció de la confidencialitat de la informació en trànsit, com defineix el requisit del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Els components han de proporcionar la capacitat d'eliminar tota la informació amb autorització explícita de lectura dels components que s'hagin d'alliberar del servei actiu i/o posar fora de servei.
	RE1	Els components han de proporcionar la capacitat de protegir contra la transferència d'informació no autoritzada i no intencionada a través de recursos de memòria compartida volàtils.
	RE2	Els components han de proporcionar la capacitat de verificar que s'ha produït l'esborrament de la informació.
CR 4.3	BR	Si es requereix l'ús de criptografia, el component ha d'utilitzar mecanismes de seguretat criptogràfica d'acord amb pràctiques i recomanacions de seguretat internacionalment reconegudes i provades.
FR5. Flux de dades restringides		
CR 5.1	BR	Els components han de permetre una xarxa segmentada que admeti zones i conductes, segons sigui necessari, per permetre una arquitectura de xarxa més àmplia basada en la segmentació lògica i la criticitat.
FR6. Resposta oportuna als incidents		
CR 6.1	BR	Els components han de proporcionar la capacitat perquè les persones i/o les eines autoritzades puguin accedir als registres d'auditoria de només lectura.
	RE1	Els components han de proporcionar accés mitjançant programació als registres d'auditoria utilitzant una interfície de programació d'aplicacions (API) o enviant els registres d'auditoria a un sistema centralitzat.

CR 6.2	BR	Els components han de proporcionar la capacitat de ser contínuament supervisats utilitzant pràctiques i recomanacions comunament acceptades en el sector de la seguretat per detectar, caracteritzar i reportar infraccions de seguretat de manera oportuna.
FR7. Disponibilitat dels recursos		
CR 7.1	BR	Els components han de proporcionar la capacitat de mantenir les funcions essencials quan operin en mode degradat com a resultat d'un esdeveniment de denegació de servei.
	RE1	Els components han de proporcionar la capacitat de mitigar els efectes dels tipus d'esdeveniments de denegació de servei de desbordament d'informació i/o missatges.
CR 7.2	BR	Els components han de proporcionar la capacitat de limitar l'ús de recursos en les funcions de seguretat per protegir contra l'esgotament dels recursos.
CR 7.3	BR	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
	RE1	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
CR 7.4	BR	Els components han de proporcionar la capacitat de poder-se recuperar i reconstituir fins a un estat segur conegut després d'una interrupció o fallada.
CR 7.6	BR	Els components han de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El component ha de proporcionar una interfície amb els ajustos de configuració de xarxa i seguretat actualment desplegats.
	RE1	Els components han de proporcionar la capacitat de generar un informe que enumeri els ajustos de seguretat actualment desplegats en un format llegible per una màquina.
CR 7.7	BR	Els components han de proporcionar la capacitat de restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.
CR 7.8	BR	Els components han de proporcionar la capacitat de permetre un inventari de components del sistema de control d'acord amb el requisit del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisits de seguretat del component pel que fa a programari

ID req	BR/RE	Explicació
SAR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
	RE1	L'aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat que permeti al dispositiu controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
SAR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.

Requisits de seguretat per als dispositius integrats (PLC, IED)

ID req	BR/RE	Explicació
EDR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
	RE1	El dispositiu integrat ha de proporcionar la capacitat d'aplicar una política de seguretat que li permeti controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
EDR 2.13	BR	Els dispositius integrats han de protegir contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, depuració JTAG).
	RE1	Els dispositius integrats han de proporcionar una supervisió activa de les interfícies de diagnòstic i assaig del dispositiu i generar una entrada de registre d'auditoria quan es detectin intents d'accés a aquestes interfícies.
EDR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.
EDR 3.10	BR	El dispositiu integrat ha d'admetre la capacitat de ser actualitzat i sotmetre's a una pujada de nivell.
	RE1	El dispositiu integrat ha de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell del programari abans de la instal·lació.

EDR 3.11	BR	El dispositiu integrat ha d'oferir mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
	RE1	El dispositiu integrat ha d'oferir mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
EDR 3.12	BR	Els dispositius integrats han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
EDR 3.13	BR	Els dispositius integrats han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
EDR 3.14	BR	Els dispositius integrats han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per a l'arrencada del component i els processos en temps d'execució abans del seu ús.
	RE1	Els dispositius integrats han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.

Requisits de seguretat per als dispositius host

ID req	BR/RE	Explicació
HDR 2.4	BR	En cas que un dispositiu host utilitzi tecnologies de codi mòbil, aquest dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu host: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a carregar codi mòbil en el dispositiu host, i c) controlar l'execució del codi basant-se en comprovacions d'integritat en el codi mòbil i abans que el codi s'executi.
	RE1	El dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat que li permeti controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
HDR 2.13	BR	Els dispositius host han de protegir-se contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, la depuració JTAG).
	RE1	Els dispositius host han de proporcionar una supervisió activa de les interfícies de diagnòstic i assaig del dispositiu i generar una entrada de registre d'auditoria quan es detectin intents d'accés a aquestes interfícies.
HDR 3.2	BR	Els dispositius host han de comptar amb mecanismes homologats pel proveïdor de productes del sistema de control que garanteixin la protecció contra codis maliciosos. El proveïdor del producte del sistema de control ha de documentar qualsevol requisit especial de configuració relacionat amb la protecció contra el codi maliciós.

	RE1	El dispositiu host ha d'informar automàticament de les versions del programari i dels arxius de protecció contra el codi maliciós en ús (com a part de la funció de registre general).
HDR 3.10	BR	Els dispositius host han de comptar amb la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
	RE1	Els dispositius host han de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell de programari abans de la instal·lació.
HDR 3.11	BR	Els dispositius host han d'oferir la capacitat d'admetre mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
	RE1	Els dispositius host han de poder notificar automàticament un conjunt configurable de destinataris si descobreixen que s'ha intentat realitzar un accés físic no autoritzat. Totes les notificacions de manipulació s'han de registrar com a part de la funció general de registre d'auditoria.
HDR 3.12	BR	Els dispositius host han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
HDR 3.13	BR	Els dispositius host han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
HDR 3.14	BR	Els dispositius host han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.
	RE1	Els dispositius host han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.

Requisits de seguretat per als dispositius de xarxa

ID req	BR/RE	Explicació
NDR 1.6	BR	Un dispositiu de xarxa que permeti la gestió d'accés sense fil ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris (persones, processos de programari o dispositius) que participen en la comunicació sense fil.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris (persones, processos o dispositius de programari) que participin en la comunicació sense fil.
NDR 1.13	BR	El dispositiu de xarxa que permeti l'accés de dispositius a una xarxa ha de poder supervisar i controlar tots els mètodes d'accés al dispositiu de xarxa a través de xarxes que no són de confiança.

	RE1	El dispositiu de xarxa ha de proporcionar la capacitat de denegar les sol·licituds d'accés a través de xarxes que no siguin de confiança, tret que s'aprovi explícitament mitjançant un rol assignat.
NDR 2.4	BR	En cas que un dispositiu de xarxa utilitzi tecnologies de codi mòbil, ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu de xarxa: a) controlar l'execució del codi mòbil; b) controlar quins usuaris (persona, procés de programari o dispositiu) estan autoritzats a transferir codi mòbil cap a / des del dispositiu de xarxa, i c) controlar l'execució del codi basant-se en verificacions d'integritat abans que el codi s'executi.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat d'aplicar una política de seguretat que permeti al dispositiu controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
NDR 2.13	BR	Els dispositius de xarxa han de protegir-se contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, la depuració JTAG).
	RE1	Els dispositius de xarxa han de proporcionar una supervisió activa de les interfícies de diagnòstic i assaig del dispositiu i generar una entrada de registre d'auditoria quan es detectin intents d'accés a aquestes interfícies.
NDR 3.2	BR	El dispositiu de xarxa ha de proporcionar protecció contra codis maliciosos.
NDR 3.10	BR	Els dispositius de xarxa han d'admetre la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
	RE1	Els dispositius de xarxa han de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell de programari abans de la instal·lació.
NDR 3.11	BR	Els dispositius de xarxa han d'oferir mecanismes de detecció i resistència a la manipulació per protegir contra l'accés físic no autoritzat al dispositiu.
	RE1	Els dispositius de xarxa han de poder notificar automàticament un conjunt configurable de destinataris si descobreixen que s'ha intentat realitzar un accés físic no autoritzat. Totes les notificacions de manipulació s'han de registrar com a part de la funció general de registre d'auditoria.
NDR 3.12	BR	Els dispositius de xarxa han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
NDR 3.13	BR	Els dispositius de xarxa han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
NDR 3.14	BR	Els dispositius de xarxa han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.

	RE1	Els dispositius de xarxa han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.
NDR 5.2	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones de risc i conductes.
	RE1	El component de xarxa ha de proporcionar la capacitat de denegar trànsit de xarxa per defecte i permetre trànsit de xarxa per excepció (també denominat "denegar-ho tot, permís per excepció").
	RE2	El component de xarxa ha d'oferir la capacitat de protegir contra qualsevol comunicació a través del límit del sistema de control (també denominat mode illa).
NDR 5.3	RE3	El component de xarxa ha de proporcionar la capacitat de protegir contra qualsevol comunicació a través del límit del sistema de control quan es produeixi una fallada operativa dels mecanismes de protecció de límits (també denominat tancament en cas de fallada).
	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de protegir contra la recepció de missatges de propòsit general entre persones rebuts d'usuaris o sistemes externs al sistema de control.

ANNEX IV: REQUISITS PER A NIVELL SL4

Requisits de seguretat del sistema

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
SR 1.1	BR	Tots els usuaris que accedeixin al sistema han de ser identificats i autenticats tant a escala de sistemes com d'aplicació; pot ser a través de contrasenyes, dispositius d'accés o multifactor (combinació de les anteriors).
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris humans.
	RE2	El sistema de control ha de proporcionar la capacitat d'emprar l'autenticació multifactor per permetre l'accés d'usuaris humans al sistema de control a través d'una xarxa que no és de confiança.
	RE3	El sistema de control ha de proporcionar la capacitat d'emprar l'autenticació multifactor per permetre l'accés de tots els usuaris humans al sistema de control.
SR 1.2	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els processos de programari i dispositius. Aquesta capacitat ha de fer complir aquesta identificació i autenticació en totes les interfícies que proporcionin accés al sistema de control per permetre els privilegis mínims, de conformitat amb les polítiques i procediments de seguretat aplicables.
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els processos de programari i dispositius.
SR 1.3	BR	El sistema de control ha de tenir la capacitat de gestionar comptes d'usuaris (agregar-ne, eliminar-ne, modificar-ne o desactivar-ne) establint condicions per pertànyer a un grup i l'assignació d'autoritzacions. Només s'admetran comptes compartits quan, per condicions del sistema, s'estableixi en l'anàlisi de risc, encara que s'hauran d'establir contramesures i documentar-les.
	RE1	El sistema de control ha de proporcionar la capacitat d'admetre la gestió de comptes unificada.
SR 1.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la gestió dels identificadors (permet operar dins d'un domini o zona de control específic del sistema) per usuari, grup, rol o interfície del sistema de control.
SR 1.5	BR	El sistema de control ha de proporcionar la capacitat de: 1) iniciar el contingut de l'autenticador; 2) canviar tots els autenticadors predeterminats; 3) canviar/actualitzar els autenticadors; 4) protegir-los contra la divulgació i modificació no autoritzada. Exemples d'autenticadors són claus físiques, targetes d'accés, claus privades, entre d'altres.
	RE1	Per als usuaris de processos de programari i dispositius, el sistema de control ha de proporcionar la capacitat de protegir els autenticadors pertinents a través de mecanismes de maquinari.

SR 1.6	BR	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris que participin en una comunicació sense fil. Exemples de tecnologies sense fils són Bluetooth, infrarojos, encaminadors mòbils, etc.
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris (persones, processos de programari o dispositius) que participin en la comunicació sense fil.
SR 1.7	BR	En els sistemes de control que utilitzin la contrasenya com a mitjà d'autenticació, s'ha d'aplicar una fortalesa configurable sobre la base de la longitud mínima i la varietat de caràcters. S'aplicarà vigència màxima per a les contrasenyes i es notificarà quan aquesta expiri. Aquesta protecció es pot millorar limitant la reutilització de les contrasenyes.
	RE1	El sistema de control ha de proporcionar la capacitat d'evitar que un compte d'un usuari humà determinat reutilitzi una contrasenya per a un nombre configurable de generacions. A més, el sistema de control ha de proporcionar la capacitat d'aplicar restriccions de vigència mínimes i màximes de les contrasenyes als usuaris humans. Aquestes capacitats s'han d'ajustar a les pràctiques comunament acceptades en el sector de la seguretat.
	RE2	El sistema de control ha de proporcionar la capacitat d'aplicar restriccions de vigència mínimes i màximes de les contrasenyes a tots els usuaris.
SR 1.8	BR	En els casos en què s'utilitzi una PKI, el sistema de control ha de proporcionar la capacitat que una PKI funcioni conformement a les millors pràctiques comunament acceptades o obtenir certificats de clau pública d'una PKI existent. El registre d'aquesta ha d'incloure l'autorització d'un supervisor que verifiqui la identitat del titular del certificat i que garanteixi que s'emet a l'usuari previst.
SR 1.9	BR	En el cas dels sistemes de control que utilitzin autenticació de clau pública (PKI), el sistema de control ha de proporcionar la capacitat de: l) validar els certificats comprovant la validesa de la signatura d'un certificat determinat; m) validar els certificats a través d'una ruta de certificació a una CA acceptada o, en el cas dels certificats autosignats, desplegant certificats d'entitat final a tots els hosts que es comuniquen amb el subjecte al qual s'emet el certificat; n) validar els certificats comprovant l'estat de revocació d'un certificat determinat; o) establir el control de l'usuari sobre la clau privada corresponent, i p) assignar la identitat autenticada a un usuari.
	RE1	El sistema de control ha de proporcionar la capacitat de protegir les claus privades pertinents a través de mecanismes de maquinari conformement a les pràctiques i recomanacions comunament acceptades en el sector de la seguretat.
SR 1.10	BR	El sistema de control ha de proporcionar la capacitat d'ocultar la retroalimentació de la informació d'autenticació durant el procés. No ha de donar pistes sobre les fallades d'autenticació com, per exemple, “nom d'usuari desconegut”.
SR 1.11	BR	El sistema de control ha de proporcionar la capacitat d'aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per qualsevol usuari dins d'un període configurable de temps.
SR 1.12	BR	El sistema de control ha de proporcionar la capacitat de mostrar un missatge d'avís del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge d'avís d'ús del sistema.

SR 1.13	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança. Ha de permetre l'accés només quan s'hi estigui autoritzat i restringir l'accés des de connexions telefòniques o no autoritzades. És possible que els procediments requereixin l'autenticació multifactor per permetre l'accés remot.
	RE1	El sistema de control ha de proporcionar la capacitat de supervisar i controlar tots els mètodes d'accés al sistema de control a través de xarxes que no són de confiança.
FR2. Control d'ús		
SR 2.1	BR	El sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris humans per controlar l'ús del sistema de control a fi d'admetre el repartiment de tasques i el privilegi mínim. Cal verificar que les accions de l'usuari estan permeses segons el rol assignat i permetre que només les persones qualificades i autoritzades facin canvis en els components del sistema.
	RE1	En totes les interfícies, el sistema de control ha de proporcionar la capacitat d'aplicar les autoritzacions assignades a tots els usuaris (persones, processos de programari i dispositius) per controlar l'ús del sistema de control amb la finalitat d'admetre el repartiment de tasques i el privilegi mínim.
	RE2	El sistema de control ha de proporcionar la capacitat que un usuari o rol autoritzat defineixi i modifiqui l'assignació de permisos a rols per a tots els usuaris humans.
	RE3	El sistema de control ha d'admetre el permís manual del supervisor de les autoritzacions actuals dels usuaris humans per a un temps o seqüència d'esdeveniments configurables.
	RE4	El sistema de control ha d'admetre la doble aprovació quan l'acció pugui ocasionar un impacte greu en el procés industrial.
SR 2.2	BR	El sistema de control ha de proporcionar la capacitat d'autoritzar, supervisar i aplicar les restriccions d'ús per a les connexions sense fils al sistema de control conformement a les pràctiques comunament acceptades en el sector de la seguretat.
	RE1	El sistema de control ha de proporcionar la capacitat d'identificar i informar de la presència de dispositius sense fils no autoritzats que transmetin dins de l'entorn físic del sistema de control.
SR 2.3	BR	El sistema de control ha de proporcionar la capacitat d'aplicar automàticament les restriccions d'ús configurables, que inclouen: a) prevenir l'ús de dispositius portàtils i mòbils; b) requerir autorització basada en un context específic, i c) restringir la transferència de codis i dades a/de dispositius portàtils i mòbils.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar que els dispositius portàtils i mòbils que intenten connectar-se a la zona en compleixin els requisits de seguretat.
SR 2.4	BR	El sistema de control ha de proporcionar la capacitat d'aplicar restriccions d'ús per a les tecnologies de codi mòbil basades en la possibilitat que causin danys al sistema de control, incloent-hi: a) prevenir l'execució del codi mòbil; b) requerir processos

		d'autenticació i autorització adequats per a l'origen del codi; c) restringir la transferència del codi mòbil al/del sistema de control, i d) supervisar l'ús del codi mòbil.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar la integritat del codi mòbil abans d'autoritzar que s'executi el codi.
SR 2.5	BR	El sistema de control ha de proporcionar la capacitat d'evitar un accés posterior iniciant un bloqueig de la sessió després d'un període de temps configurable d'inactivitat o mitjançant iniciació manual. La sessió ha de continuar bloquejada fins que l'usuari autoritzat restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats. En els casos en els quals el sistema de control no pugui admetre el bloqueig de la sessió, l'entitat responsable hauria d'emprar les contramesures compensatòries que es considerin adequades, com majors mesures de seguretat física i auditories.
SR 2.6	BR	El sistema de control ha de proporcionar la capacitat de finalitzar una sessió remota, sigui automàticament després d'un període d'inactivitat configurable o manualment per part de l'usuari que va iniciar la sessió.
SR 2.7	BR	El sistema de control ha de proporcionar la capacitat de limitar el nombre de sessions simultànies per interfície per a qualsevol usuari determinat a un nombre configurable de sessions.
SR 2.8	BR	El sistema de control ha de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: control d'accés, errors de sol·licitud, esdeveniments del sistema operatiu, esdeveniments del sistema de control, esdeveniments de còpies de seguretat i restauració, canvis en la configuració, activitat potencial de reconeixement i esdeveniments del registre d'auditoria. Els registres individuals d'auditoria han d'incloure la marca de temps, font (dispositiu, procés de programari o compte d'usuari humà d'origen), categoria, tipus, identificador de l'esdeveniment i resultat de l'esdeveniment.
	RE1	El sistema de control ha de proporcionar la capacitat de gestionar de manera centralitzada els esdeveniments d'auditoria i d'elaborar registres d'auditoria de múltiples components a través del sistema de control en una pista d'auditoria per a tot el sistema (lògica o física) amb correlació de temps. El sistema de control ha de proporcionar la capacitat d'exportar aquests registres d'auditories en formats habituals per a la indústria perquè s'analitzin amb les eines comercials habituals d'anàlisis de registres, com per exemple l'administració d'esdeveniments i informació de seguretat (SIEM).
SR 2.9	BR	El sistema de control ha d'assignar una capacitat suficient d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres i la configuració del sistema. El sistema de control ha de proporcionar mecanismes d'auditoria per reduir la possibilitat que s'excedeixi aquesta capacitat.
	RE1	El sistema de control ha de proporcionar la capacitat d'emetre un avís quan el volum d'emmagatzematge de registres d'auditoria assignat assoleixi un percentatge configurable de capacitat màxima d'emmagatzematge de registres d'auditoria.
SR 2.10	BR	El sistema de control ha de proporcionar la capacitat d'alertar el personal i evitar la pèrdua de serveis i funcions essencials en cas que falli el processament d'auditories. El sistema de control ha de proporcionar la capacitat d'admetre les accions apropiades en

		resposta a una fallada en el processament d'auditories d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
SR 2.11	BR	El sistema de control ha de proporcionar marques de temps (data i hora) per a la generació de registres d'auditoria. Cal evitar que les fonts horàries sofreixin alteracions no autoritzades.
	RE1	El sistema de control ha de proporcionar la capacitat de sincronitzar els rellotges interns del sistema a una freqüència configurable.
	RE2	S'ha d'evitar que la font horària sofreixi alteracions no autoritzades i, en cas que se'n produeixi una, s'ha d'iniciar un esdeveniment d'auditoria.
SR 2.12	BR	El sistema de control ha de proporcionar la capacitat de determinar si un usuari humà ha realitzat una acció concreta.
	RE1	El sistema de control ha de proporcionar la capacitat de determinar si un usuari específic (persona, procés de programari o dispositiu) ha realitzat una acció concreta.
FR3. Integritat del sistema		
SR 3.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el sistema per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes criptogràfics per reconèixer canvis d'informació durant la comunicació.
SR 3.2	BR	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció per prevenir, detectar, mitigar i informar dels efectes d'un codi maliciós o de programari no autoritzat. El sistema de control ha de proporcionar la capacitat d'actualitzar els mecanismes de protecció.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes de protecció contra codis maliciosos en tots els punts d'entrada i sortida.
	RE2	El sistema de control ha de proporcionar la capacitat de gestionar els mecanismes de protecció contra codis maliciosos.
SR 3.3	BR	El sistema de control ha de proporcionar la capacitat d'admetre la verificació del funcionament previst de les funcions de seguretat (mesures d'antivirus, identificació, detecció d'intrusos i auditories) i informar de les anomalies que es produeixin durant els assajos d'acceptació en fàbrica i en emplaçament i durant el manteniment programat. Les funcions de seguretat han d'incloure totes les funcions que siguin necessàries per complir els requisits de seguretat especificats en aquesta norma.

	RE1	El sistema de control ha de proporcionar la capacitat d'emprar mecanismes automàtics per facilitar la gestió de la verificació de la seguretat durant els assajos d'acceptació en fàbrica i en emplaçament i durant el manteniment programat.
	RE2	El sistema de control ha de proporcionar la capacitat d'admetre la verificació del funcionament previst de les funcions de seguretat durant les operacions normals.
SR 3.4	BR	El sistema de control ha de proporcionar la capacitat de detectar, registrar, informar i protegir contra canvis no autoritzats en el programari i en la informació en repòs.
	RE1	El sistema de control ha de proporcionar la capacitat d'emprar eines automatitzades que notifiquin un conjunt configurable de receptors quan es produeixin discrepàncies durant la verificació de la integritat.
SR 3.5	BR	El sistema de control ha de validar la sintaxi i el contingut de qualsevol entrada que s'utilitzi com a entrada de control de processos industrials o entrada que tingui un impacte directe en l'acció del sistema de control. Les directrius que cal tenir en compte haurien d'incloure la Code Review Guide de l'Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control ha de proporcionar la capacitat d'establir el valor de sortida a un estat predeterminat si no es pot mantenir el funcionament normal com a resultat d'un atac.
SR 3.7	BR	El sistema de control ha d'identificar i tractar les condicions d'error de manera que s'hi pugui aplicar un remei efectiu. Això s'ha de fer sense proporcionar informació que pugui ser aprofitada per adversaris per atacar el sistema de control, tret que sigui necessari per resoldre els problemes de manera oportuna.
SR 3.8	BR	El sistema de control ha de proporcionar la capacitat de protegir la integritat de les sessions. El sistema de control ha de rebutjar qualsevol ús per part d'identificadors de sessió no vàlids.
	RE1	El sistema de control ha de proporcionar la capacitat d'anul·lar els identificadors de sessió quan l'usuari tanqui la sessió o després de qualsevol altre tipus de tancament de sessió (incloses les sessions de navegació).
	RE2	El sistema de control ha de proporcionar la capacitat de generar un identificador de sessió únic per a cada sessió i considerar no vàlids tots els identificadors de sessió imprevists.
	RE3	El sistema de control ha de proporcionar la capacitat de generar identificadors de sessió únics amb fonts d'aleatorietat comunament acceptades.
SR 3.9	BR	El sistema de control ha de protegir la informació i les eines d'auditoria (si n'hi ha) contra l'accés, la modificació i l'eliminació no autoritzats.
	RE1	El sistema de control ha de proporcionar la capacitat de generar registres d'auditoria en mitjans d'una única escriptura mitjançant maquinari.

FR4. Confidencialitat de les dades		
SR 4.1	BR	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació (especialment en dispositius portàtils) per a la qual s'admet l'autorització explícita de lectura, estigui en repòs o en trànsit. La tècnica triada ha de tenir en compte les possibles ramificacions en el rendiment del sistema de control i la capacitat de recuperar-se després d'una fallada del sistema o un atac.
	RE1	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació en repòs i en sessions amb accés remot a través d'una xarxa que no és de confiança.
	RE2	El sistema de control ha de proporcionar la capacitat de protegir la confidencialitat de la informació que travessi qualsevol límit de la zona.
SR 4.2	BR	El sistema de control ha de proporcionar la capacitat d'eliminar tota la informació amb autorització explícita de lectura dels components que s'hagin d'alliberar del servei actiu i/o llocs fora de servei.
	RE1	El sistema de control ha de proporcionar la capacitat d'evitar la transferència d'informació no autoritzada i no intencionada a través de recursos de memòria compartida volàtils (no retenen la informació després de ser alliberats per a la gestió de la memòria).
SR 4.3	BR	Si es requereix l'ús de criptografia, el sistema de control ha d'usar algorismes criptogràfics, grandàries de clau i mecanismes per a l'establiment i gestió de claus conformement a les pràctiques i recomanacions de seguretat comunament acceptades en el sector que es troben en documents com la publicació especial NIST SP800-57.
FR5. Flux de dades restringides		
SR 5.1	BR	El sistema de control ha de proporcionar la capacitat de segmentar de manera lògica les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control d'altres xarxes del sistema de control.
	RE1	El sistema de control ha de proporcionar la capacitat de segmentar físicament les xarxes del sistema de control de xarxes no pertanyents al sistema de control, així com xarxes crítiques del sistema de control de les xarxes no crítiques del sistema de control.
	RE2	El sistema de control ha de proporcionar serveis de xarxa a xarxes el sistema de control, siguin crítiques o no, sense que s'estableixi una connexió amb xarxes no pertanyents al sistema de control.
	RE3	El sistema de control ha de proporcionar la capacitat d'aïllar lògicament i físicament les xarxes crítiques del sistema de control de xarxes no crítiques del sistema de control.
SR 5.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones i conductes de risc. Com a part d'una estratègia de protecció de defensa total, s'haurien de dividir els sistemes de control de major impacte en zones separades utilitzant conductes per restringir o prohibir l'accés a la xarxa conformement a les polítiques i procediments de seguretat i a una avaluació de riscos.

	RE1	El sistema de control ha de proporcionar serveis de xarxa a xarxes el sistema de control, siguin crítiques o no, sense que s'estableixi una connexió amb xarxes no pertanyents al sistema de control.
	RE2	El sistema de control ha de proporcionar la capacitat d'evitar qualsevol comunicació a través del límit del sistema de control (també denominat mode illa).
	RE3	El sistema de control ha de proporcionar la capacitat d'evitar qualsevol comunicació a través del límit del sistema de control quan es produeixi una fallada operativa dels mecanismes de protecció de límits (també denominat tancament en cas de fallada). Aquesta funció de "tancament en cas de fallada" ha de dissenyar-se de tal forma que no interfereixi en el funcionament d'un sistema instrumentat de seguretat (SIS) o en altres funcions relacionades amb la seguretat.
SR 5.3	BR	Un sistema de control ha de proporcionar la capacitat d'evitar la recepció de missatges de propòsit general (correu electrònic, xarxes socials o qualsevol altre sistema de missatgeria) entre persones procedents d'usuaris o sistemes externs al sistema de control.
	RE1	El sistema de control ha de proporcionar la capacitat d'evitar tant la transmissió com la recepció de missatges entre persones de propòsit general.
SR 5.4	BR	El sistema de control ha de proporcionar la capacitat d'admetre la partició de dades (per mitjans físics o lògics), aplicacions i serveis sobre la base de la seva criticitat per facilitar la implementació d'un model de zonificació.
FR6. Resposta oportuna als incidents		
SR 6.1	BR	El sistema de control ha de proporcionar la capacitat que les persones i/o les eines autoritzades accedeixin als registres d'auditoria en mode de lectura.
	RE1	El sistema de control ha de permetre l'accés mitjançant programació als registres d'auditoria utilitzant una interfície de programació d'aplicacions (API).
SR 6.2	BR	El sistema de control ha de proporcionar la capacitat de supervisar contínuament el rendiment del mecanisme de seguretat utilitzant pràctiques i recomanacions comunament acceptades en el sector de la seguretat per detectar, caracteritzar i reportar infraccions de seguretat de manera oportuna.
FR7. Disponibilitat dels recursos		
SR 7.1	BR	El sistema de control ha de proporcionar la capacitat de funcionar en mode degradat durant un esdeveniment de denegació de servei. Un esdeveniment de denegació de servei en el sistema de control no hauria d'afectar negativament cap sistema relacionat amb la seguretat.
	RE1	El sistema de control ha de proporcionar la capacitat de gestionar les càrregues de comunicació (per exemple, limitant la taxa) per mitigar els efectes dels tipus de desbordament d'informació dels esdeveniments de denegació de servei.
	RE2	El sistema de control ha de proporcionar la capacitat de restringir la possibilitat que qualsevol usuari provoqui esdeveniments de denegació de servei que puguin afectar altres sistemes de control o xarxes.

SR 7.2	BR	El sistema de control ha de proporcionar la capacitat de limitar l'ús de recursos per part de les funcions de seguretat per evitar l'esgotament dels recursos.
SR 7.3	BR	El sistema de control ha de facilitar la identitat i ubicació dels arxius crítics i la capacitat de dur a terme còpies de seguretat de la informació de l'usuari i del sistema (incloent-hi informació sobre l'estat del sistema) sense que això afecti les operacions habituals.
	RE1	El sistema de control ha de proporcionar la capacitat de verificar la fiabilitat dels mecanismes de còpies de seguretat.
	RE2	El sistema de control ha de proporcionar la capacitat d'automatitzar la funció de còpia de seguretat sobre la base d'una freqüència configurable.
SR 7.4	BR	El sistema de control ha de proporcionar la capacitat de recuperar-se i reconstituir-se fins a un estat segur conegut després d'una interrupció o fallada. Un estat segur conegut significa que s'atribueixen a tots els paràmetres del sistema (siguin predeterminats o configurables) valors segurs, es reinstal·len els pedaços crítics per a la seguretat, es restableixen els ajustos de configuració relacionats amb la seguretat, es disposa de la documentació i els procediments operatius del sistema, es reinstal·la i configura l'aplicació i el programari del sistema amb ajustos segurs, es carrega la informació de les còpies de seguretat més recents i conegudes, i se sotmet a assaig i es comprova el funcionament del sistema íntegrament.
SR 7.5	BR	El sistema de control ha de proporcionar la capacitat de canviar d'una font d'alimentació d'emergència i a aquesta sense que això afecti l'estat de seguretat existent o un mode degradat documentat.
SR 7.6	BR	El sistema de control ha de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El sistema de control ha de proporcionar una interfície als ajustos de configuració de xarxa i seguretat desplegats actualment.
	RE1	El sistema de control ha de proporcionar la capacitat de generar un informe que enumeri els ajustos de seguretat desplegats actualment en un format llegible per una màquina.
SR 7.7	BR	El sistema de control ha de proporcionar la capacitat de prohibir i/o restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.
SR 7.8	BR	El sistema de control ha de proporcionar la capacitat d'informar de la llista actual de components instal·lats i de les seves propietats associades.

Requisits de seguretat dels components generals

ID req	BR/RE	Explicació
FR1. Control d'identificació i autenticació		
CR 1.1	BR	Els components han de proporcionar la capacitat d'identificar i autenticar tots els usuaris en totes les interfícies que permetin el repartiment de tasques i els privilegis mínims. Es pot proporcionar a escala component o a escala sistema.
	RE1	Els components han de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris humans.
	RE2	Els components han de proporcionar la capacitat d'emprar l'autenticació multifactor per a tot l'accés d'usuaris humans al component.
CR 1.2	BR	Els components han de proporcionar la capacitat d'identificar-se a si mateixos i autenticar qualsevol altre component d'acord amb el requisit del sistema SR 1.2 de la Norma IEC62443-3-3. Si el component, com en el cas d'una aplicació, s'executa en el context d'un usuari humà, a més, la identificació i autenticació de l'usuari humà d'acord amb el requisit del sistema SR1.1 de la Norma IEC62443-3-3 pot formar part del procés d'identificació i autenticació del component cap als altres components.
	RE1	Els components han de proporcionar la capacitat d'identificar i autenticar de manera única qualsevol altre component.
CR 1.3	BR	Els components han de proporcionar la capacitat de permetre la gestió de tots els comptes de forma directa o integrant-se en un sistema que gestioni els comptes.
CR 1.4	BR	Els components han de proporcionar la capacitat d'integrar-se en un sistema que admeti la gestió d'identificadors i/o la capacitat de permetre la gestió d'identificadors.
CR 1.5	BR	Els components han de proporcionar la capacitat de: a) permetre l'ús del contingut inicial de l'autenticador; b) permetre el reconeixement dels canvis en els autenticadors predeterminats realitzats al moment de la instal·lació; c) funcionar correctament amb operacions periòdiques de modificació/actualització dels autenticadors, i d) protegir els autenticadors de la divulgació i modificació no autoritzada quan s'emmagatzemen, utilitzen i transmeten.
	RE1	Els autenticadors en els quals es recolza el component han d'estar protegits mitjançant mecanismes de maquinari (memòria protegida per contrasenya, memòria OTP, comprovacions d'integritat de maquinari de dades i mecanisme d'arrencada de seguretat de dispositius.).
CR 1.7	BR	Els components que utilitzin autenticació basada en contrasenya, han de proporcionar o integrar-se en un sistema que proporcioni la capacitat d'aplicar la fortalesa de les contrasenyes configurables d'acord amb directrius de contrasenyes reconegudes i provades internacionalment.
	RE1	Els components han de proporcionar la capacitat de protegir un compte d'usuari humà determinat contra la reutilització d'una contrasenya per a un nombre configurable de generacions, o integrar-se en un sistema que la proporcioni. A més, el component ha

		de proporcionar la capacitat d'aplicar les restriccions de vigència mínimes i màximes de les contrasenyes per als usuaris humans. Aquestes capacitats s'han d'ajustar a les pràctiques comunament acceptades en el sector de la seguretat. El component hauria de proporcionar la capacitat de sol·licitar a l'usuari que canviï la seva contrasenya en un temps configurable abans de la caducitat.
	RE2	Els components han de proporcionar la capacitat d'aplicar les restriccions mínimes i màximes de vigència de les contrasenyes per a tots els usuaris, o integrar-se en un sistema que la proporcioni.
CR 1.8	BR	Quan s'utilitzi una infraestructura de clau pública (PKI), el component ha de proporcionar un sistema que ofereixi la capacitat d'interactuar i funcionar de conformitat amb el requisit del sistema SR 1.8 de la Norma IEC62443-3-3 o integrar-se en aquest sistema.
CR 1.9	BR	Els components que utilitzin autenticació basada en clau pública han de subministrar-se directament o integrar-se en un sistema que ofereixi la capacitat en el mateix entorn del sistema de control per: a) validar els certificats comprovant la validesa de la signatura d'un certificat determinat; b) validar la cadena de certificats o, en el cas dels certificats autosignats, desplegar certificats d'entitat final a tots els hosts que es comuniquen amb el subjecte al qual s'emet el certificat; c) validar els certificats comprovant l'estat de revocació d'un certificat determinat; d) establir el control de l'usuari sobre la clau privada corresponent; e) assignar la identitat autenticada a un usuari, i f) garantir que els algorismes i claus utilitzats per a l'autenticació de clau pública compleixen els requisits establerts.
	RE1	Els components han de proporcionar la capacitat de protegir les claus privades crítiques de llarga durada mitjançant mecanismes de maquinari.
CR 1.10	BR	Quan un component ofereixi la capacitat d'autenticació, el component ha d'oferir la capacitat d'ocultar la retroalimentació de la informació de l'autenticador durant el procés d'autenticació.
CR 1.11	BR	Quan un component ofereixi una capacitat d'autenticació, el component ha de proporcionar la capacitat de: a) aplicar un límit d'un nombre configurable d'intents d'accés no vàlids consecutius per part de qualsevol usuari durant un període de temps configurable; b) denegar l'accés durant un període de temps específic o fins que un administrador el desbloquegi, quan s'hagi arribat a aquest límit. Un administrador pot desbloquejar un compte abans de la caducitat del període de temps d'espera.
CR 1.12	BR	Quan un component proporcioni un accés d'usuari humà local/IHM, ha de proporcionar la capacitat de mostrar un missatge de notificació d'ús del sistema abans de l'autenticació. El personal autoritzat ha de poder configurar el missatge de notificació d'ús del sistema.
CR 1.14	BR	Per als components que utilitzin claus simètriques, el component ha de proporcionar la capacitat de: a) establir la confiança mútua utilitzant la clau simètrica; b) emmagatzemar de forma segura el secret compartit; c) restringir l'accés al secret compartit, i d) garantir que els algorismes i les claus utilitzats per a l'autenticació de clau simètrica compleixen els requisits establerts.
	RE1	Els components han de proporcionar la capacitat de protegir claus simètriques crítiques i de llarga durada mitjançant mecanismes de maquinari.

FR2. Control d'ús		
CR 2.1	BR	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris identificats i autenticats en funció de les responsabilitats que se'ls hagin assignat.
	RE1	Els components han de proporcionar un mecanisme d'aplicació de l'autorització per a tots els usuaris en funció de les responsabilitats que se'ls assignin i del privilegi mínim.
	RE2	Els components, directament o a través d'un mecanisme de compensació de seguretat, han de proporcionar un rol autoritzat per definir i modificar l'assignació de permisos a rols per a tots els usuaris humans. Els rols no haurien de limitar-se a jerarquies fixes niades en les quals un rol de nivell superior sigui un superconjunt d'un rol menys privilegiat. Per exemple, un administrador de sistema no hauria d'incloure necessàriament privilegis d'operador.
	RE3	Els components han de proporcionar el permís manual del supervisor durant un temps o seqüència d'esdeveniments configurables. La implementació d'un permís manual, controlat i auditat de mecanismes automatitzats en cas d'emergència o altres esdeveniments greus permet a un supervisor autoritzar un operador perquè reaccioni ràpidament davant condicions inusuals sense tancar la sessió actual i establir una nova sessió com un usuari humà amb majors privilegis.
	RE4	Els components han de permetre la doble aprovació quan l'acció pugui tenir un impacte greu en el procés industrial. La doble aprovació hauria de limitar-se a les accions que requereixin un nivell molt elevat de confiança que es duguin a terme de manera fiable i correcta. No s'haurien d'emprar mecanismes de doble aprovació quan sigui necessària una resposta immediata per protegir la salut, la seguretat i l'entorn, per exemple, la parada d'emergència d'un procés industrial.
CR 2.2	BR	Si un component admet l'ús a través d'interfícies sense fils, ha de proporcionar la capacitat d'integrar-se en el sistema que admet l'autorització d'ús, la supervisió i les restriccions d'acord amb les pràctiques industrials comunament acceptades.
CR 2.5	BR	Si un component proporciona una interfície per a un usuari humà, tant si s'hi accedeix localment com a través d'una xarxa, el component ha de proporcionar la capacitat de: a) protegir-se contra l'accés posterior iniciant un bloqueig de sessió després d'un període de temps configurable d'inactivitat o mitjançant la iniciació manual per part de l'usuari, i b) mantenir el bloqueig de la sessió fins que l'usuari propietari de la sessió, o un altre usuari humà autoritzat, restableixi l'accés utilitzant els procediments d'identificació i autenticació adequats.
CR 2.6	BR	Si un component admet sessions remotes, ha de proporcionar la capacitat de finalitzar una sessió remota automàticament després d'un període d'inactivitat configurable manualment per part d'una autoritat local o manualment per part de l'usuari que va iniciar la sessió.
CR 2.7	BR	Els components han de proporcionar la capacitat de limitar el nombre de sessions simultànies per interfície per a qualsevol usuari determinat (persona, procés de programari o dispositiu).
CR 2.8	BR	Els components han de proporcionar la capacitat de generar registres d'auditoria pertinents per a la seguretat de les següents categories: a) control d'accés; b) errors de sol·licitud; c) esdeveniments del sistema de control; d) esdeveniment de còpia de seguretat

		i restauració; e) canvis de configuració, i f) esdeveniments de registre d'auditoria. Els registres d'auditoria individuals han d'incloure: a) marca de temps; b) font (dispositiu d'origen, procés de programari o compte d'usuari humà); c) categoria; d) tipus; e) ID de l'esdeveniment, i f) resultat de l'esdeveniment.
CR 2.9	BR	Els components han de: a) proporcionar la capacitat d'assignar una capacitat d'emmagatzematge de registres d'auditoria d'acord amb les recomanacions comunament reconegudes per a la gestió de registres, i b) proporcionar mecanismes per protegir contra una fallada del component quan arribi a la capacitat d'emmagatzematge de dades d'auditoria o la superi.
	RE1	Els components han de proporcionar la capacitat d'emetre un avís quan l'emmagatzematge de registres d'auditoria assignat arribi a un llindar de capacitat configurable.
CR 2.10	BR	Els components han de: a) proporcionar la capacitat de protegir contra la pèrdua de serveis i funcions essencials en cas que falli el processament d'una auditoria, i b) proporcionar la capacitat per permetre les accions apropiades en resposta a una fallada en el processament d'una auditoria d'acord amb les pràctiques i recomanacions comunament acceptades del sector.
CR 2.11	BR	Els components han de proporcionar la capacitat de crear marques de temps (incloent-hi data i hora) per al seu ús en els registres d'auditoria.
	RE1	Els components han de proporcionar la capacitat de crear marques de temps que estiguin sincronitzades amb una font de temps de tot el sistema.
	RE2	El mecanisme de sincronització de temps ha de proporcionar la capacitat de detectar alteracions no autoritzades i causar un esdeveniment d'auditoria després de l'alteració.
CR 2.12	BR	Si un component proporciona una interfície per a un usuari humà, el component ha de proporcionar la capacitat de determinar si un determinat usuari humà ha realitzat una determinada acció. Els elements de control que no puguin permetre aquesta capacitat s'han d'enumerar en els documents dels components.
	RE1	Els components han de proporcionar la capacitat de verificar l'autenticitat de la informació rebuda durant la comunicació.
FR3. Integritat del sistema		
CR 3.1	BR	Els components han de proporcionar la capacitat de protegir la integritat de la informació transmesa, configurant el component per a la millora de la seguretat tant cibernètica, utilitzant protocols segurs, com física, fent servir maquinari adequat per al context en el qual es troba.
	RE1	Els components han de proporcionar la capacitat de verificar l'autenticitat de la informació rebuda durant la comunicació.
CR 3.3	BR	Els components han de proporcionar la capacitat de permetre la verificació de l'operació prevista de les funcions de seguretat d'acord amb el requisit del sistema.

	RE1	Els components han de proporcionar la capacitat per permetre la verificació del funcionament previst de les funcions de seguretat durant les operacions normals. Aquesta RE ha de ser implementada acuradament per evitar efectes perjudicials. Pot no ser adequada per a sistemes de seguretat.
CR 3.4	BR	Els components han de proporcionar la capacitat de fer o permetre verificacions d'integritat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'integritat.
	RE1	Els components han de proporcionar la capacitat de fer o permetre verificacions d'autenticitat del programari, la configuració i una altra informació, així com el registre i la notificació dels resultats d'aquests controls, o bé integrar-se en un sistema que pugui fer o permetre les verificacions d'autenticitat.
	RE2	Si el component està verificant la integritat, ha de poder notificar automàticament una entitat configurable quan descobreixi que s'ha intentat fer un canvi no autoritzat.
CR 3.5	BR	Els components han de validar la sintaxi, la longitud i el contingut de qualsevol dada d'entrada que s'utilitzi com a entrada de control de processos industrials o entrada a través d'interfícies externes que tinguin un impacte directe en l'acció del component.
CR 3.6	BR	Els components que es connecten físicament o lògicament a un procés d'automatització han de proporcionar la capacitat d'establir sortides a un estat predeterminat si no es pot mantenir el funcionament normal definit pel proveïdor de components.
CR 3.7	BR	Els components han d'identificar i tractar les condicions d'error de manera que no proporcionin informació que pugui ser aprofitada per adversaris per atacar el sistema de control.
CR 3.8	BR	Els components han de proporcionar mecanismes per protegir la integritat de les sessions de comunicació, incloent-hi: a) la capacitat d'invalidar identificadors de sessió quan l'usuari tanqui la sessió o després de qualsevol altre tipus de tancament de sessió (incloses les sessions de navegació); b) la capacitat de generar un identificador de sessió únic per a cada sessió i reconèixer només els identificadors de sessió generats pel sistema, i c) la capacitat de generar identificadors de sessió únics amb fonts d'aleatorietat comunament acceptades.
CR 3.9	BR	Els components han de protegir la informació d'auditoria, els registres d'auditoria i les eines d'auditoria (si n'hi ha) contra l'accés, la modificació i l'eliminació no autoritzats.
	RE1	Els components han de proporcionar la capacitat d'emmagatzemar registres d'auditoria en mitjans d'una única escriptura.

FR4. Confidencialitat de les dades		
CR 4.1	BR	Els components han de: a) proporcionar la capacitat de protegir la confidencialitat de la informació en repòs per a la qual s'admet l'autorització explícita de lectura, i b) permetre la protecció de la confidencialitat de la informació en trànsit, com defineix el requisit del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Els components han de proporcionar la capacitat d'eliminar tota la informació amb autorització explícita de lectura dels components que s'hagin d'alliberar del servei actiu i/o posar fora de servei.
	RE1	Els components han de proporcionar la capacitat de protegir contra la transferència d'informació no autoritzada i no intencionada a través de recursos de memòria compartida volàtils.
	RE2	Els components han de proporcionar la capacitat de verificar que s'ha produït l'esborrament de la informació.
CR 4.3	BR	Si es requereix l'ús de criptografia, el component ha d'utilitzar mecanismes de seguretat criptogràfica d'acord amb pràctiques i recomanacions de seguretat internacionalment reconegudes i provades.
FR5. Flux de dades restringides		
CR 5.1	BR	Els components han de permetre una xarxa segmentada que admeti zones i conductes, segons sigui necessari, per permetre una arquitectura de xarxa més àmplia basada en la segmentació lògica i la criticitat.
FR6. Resposta oportuna als incidents		
CR 6.1	BR	Els components han de proporcionar la capacitat perquè les persones i/o les eines autoritzades puguin accedir als registres d'auditoria de només lectura.
	RE1	Els components han de proporcionar accés mitjançant programació als registres d'auditoria utilitzant una interfície de programació d'aplicacions (API) o enviant els registres d'auditoria a un sistema centralitzat.
CR 6.2	BR	Els components han de proporcionar la capacitat de ser contínuament supervisats utilitzant pràctiques i recomanacions comunament acceptades en el sector de la seguretat per detectar, caracteritzar i reportar infraccions de seguretat de manera oportuna.
FR7. Disponibilitat dels recursos		
CR 7.1	BR	Els components han de proporcionar la capacitat de mantenir les funcions essencials quan operin en mode degradat com a resultat d'un esdeveniment de denegació de servei.
	RE1	Els components han de proporcionar la capacitat de mitigar els efectes dels tipus d'esdeveniments de denegació de servei de desbordament d'informació i/o missatges.
CR 7.2	BR	Els components han de proporcionar la capacitat de limitar l'ús de recursos en les funcions de seguretat per protegir contra l'esgotament dels recursos.

CR 7.3	BR	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
	RE1	Els components han de proporcionar la capacitat de participar en operacions de còpia de seguretat a escala de sistema amb la finalitat de salvaguardar l'estat dels components (informació d'usuari i de sistema). El procés de còpia de seguretat no ha d'afectar les operacions normals dels components.
CR 7.4	BR	Els components han de proporcionar la capacitat de poder-se recuperar i reconstituir fins a un estat segur conegut després d'una interrupció o fallada.
CR 7.6	BR	Els components han de poder-se configurar d'acord amb les configuracions de xarxa i seguretat recomanades, tal com descriuen les directrius proporcionades pel proveïdor del sistema de control. El component ha de proporcionar una interfície amb els ajustos de configuració de xarxa i seguretat actualment desplegats.
	RE1	Els components han de proporcionar la capacitat de generar un informe que enumeri els ajustos de seguretat actualment desplegats en un format llegible per una màquina.
CR 7.7	BR	Els components han de proporcionar la capacitat de restringir específicament l'ús de funcions, ports, protocols i/o serveis innecessaris.
CR 7.8	BR	Els components han de proporcionar la capacitat de permetre un inventari de components del sistema de control d'acord amb el requisit del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisits de seguretat del component pel que fa a programari

ID req	BR/RE	Explicació
SAR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
	RE1	L'aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat que permeti al dispositiu controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
SAR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.

Requisits de seguretat per als dispositius integrats (PLC, IED)

ID req	BR/RE	Explicació
EDR 2.4	BR	En cas que una aplicació de programari utilitzi tecnologies de codi mòbil, aquesta aplicació ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en l'aplicació de programari: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a transferir codi mòbil des de / cap a l'aplicació; c) controlar l'execució de codi mòbil basant-se en els resultats d'una verificació de la integritat prèvia a l'execució del codi.
	RE1	El dispositiu integrat ha de proporcionar la capacitat d'aplicar una política de seguretat que li permeti controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
EDR 2.13	BR	Els dispositius integrats han de protegir contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, depuració JTAG).
	RE1	Els dispositius integrats han de proporcionar una supervisió activa de les interfícies de diagnòstic i assaig del dispositiu i generar una entrada de registre d'auditoria quan es detectin intents d'accés a aquestes interfícies.
EDR 3.2	BR	El proveïdor del producte d'aplicació ha de qualificar i documentar quina protecció contra els mecanismes de codi maliciós són compatibles amb l'aplicació i ha de considerar qualsevol requisit especial de configuració.
EDR 3.10	BR	El dispositiu integrat ha d'admetre la capacitat de ser actualitzat i sotmetre's a una pujada de nivell.
	RE1	El dispositiu integrat ha de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell del programari abans de la instal·lació.
EDR 3.11	BR	El dispositiu integrat ha d'oferir mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
	RE1	El dispositiu integrat ha d'oferir mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
EDR 3.12	BR	Els dispositius integrats han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
EDR 3.13	BR	Els dispositius integrats han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
EDR 3.14	BR	Els dispositius integrats han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per a l'arrencada del component i els processos en temps d'execució abans del seu ús.

	RE1	Els dispositius integrats han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.

Requisits de seguretat per als dispositius host

ID req	BR/RE	Explicació
HDR 2.4	BR	En cas que un dispositiu host utilitzi tecnologies de codi mòbil, aquest dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu host: a) controlar l'execució del codi mòbil; b) controlar quins usuaris estan autoritzats a carregar codi mòbil en el dispositiu host, i c) controlar l'execució del codi basant-se en comprovacions d'integritat en el codi mòbil i abans que el codi s'executi.
	RE1	El dispositiu host ha de proporcionar la capacitat d'aplicar una política de seguretat que li permeti controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
HDR 2.13	BR	Els dispositius host han de protegir-se contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, la depuració JTAG).
	RE1	Els dispositius host han de proporcionar una supervisió activa de les interfícies de diagnòstic i assaig del dispositiu i generar una entrada de registre d'auditoria quan es detectin intents d'accés a aquestes interfícies.
HDR 3.2	BR	Els dispositius host han de comptar amb mecanismes homologats pel proveïdor de productes del sistema de control que garanteixin la protecció contra codis maliciosos. El proveïdor del producte del sistema de control ha de documentar qualsevol requisit especial de configuració relacionat amb la protecció contra el codi maliciós.
	RE1	El dispositiu host ha d'informar automàticament de les versions del programari i dels arxius de protecció contra el codi maliciós en ús (com a part de la funció de registre general).
HDR 3.10	BR	Els dispositius host han de comptar amb la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
	RE1	Els dispositius host han de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell de programari abans de la instal·lació.
HDR 3.11	BR	Els dispositius host han d'oferir la capacitat d'admetre mecanismes de resistència a la manipulació i de detecció per protegir contra l'accés físic no autoritzat al dispositiu.
	RE1	Els dispositius host han de poder notificar automàticament un conjunt configurable de destinataris si descobreixen que s'ha intentat realitzar un accés físic no autoritzat. Totes les notificacions de manipulació s'han de registrar com a part de la funció general de registre d'auditoria.

HDR 3.12	BR	Els dispositius host han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
HDR 3.13	BR	Els dispositius host han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
HDR 3.14	BR	Els dispositius host han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.
	RE1	Els dispositius host han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.

Requisits de seguretat per als dispositius de xarxa

ID req	BR/RE	Explicació
NDR 1.6	BR	Un dispositiu de xarxa que permeti la gestió d'accés sense fil ha de proporcionar la capacitat d'identificar i autenticar tots els usuaris (persones, processos de programari o dispositius) que participen en la comunicació sense fil.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat d'identificar i autenticar de manera única tots els usuaris (persones, processos o dispositius de programari) que participin en la comunicació sense fil.
NDR 1.13	BR	El dispositiu de xarxa que permeti l'accés de dispositius a una xarxa ha de poder supervisar i controlar tots els mètodes d'accés al dispositiu de xarxa a través de xarxes que no són de confiança.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat de denegar les sol·licituds d'accés a través de xarxes que no siguin de confiança, tret que s'aprovi explícitament mitjançant un rol assignat.
NDR 2.4	BR	En cas que un dispositiu de xarxa utilitzi tecnologies de codi mòbil, ha de proporcionar la capacitat d'aplicar una política de seguretat per a l'ús de tecnologies de codi mòbil. La política de seguretat ha de permetre, com a mínim, les següents accions per a cada tecnologia de codi mòbil utilitzada en el dispositiu de xarxa: a) controlar l'execució del codi mòbil; b) controlar quins usuaris (persona, procés de programari o dispositiu) estan autoritzats a transferir codi mòbil cap a / des del dispositiu de xarxa, i c) controlar l'execució del codi basant-se en verificacions d'integritat abans que el codi s'executi.
	RE1	El dispositiu de xarxa ha de proporcionar la capacitat d'aplicar una política de seguretat que permeti al dispositiu controlar l'execució del codi mòbil basant-se en els resultats d'una comprovació d'autenticitat abans que s'executi el codi.
NDR 2.13	BR	Els dispositius de xarxa han de protegir-se contra l'ús no autoritzat de la/les interfície/s física/ques de diagnòstic i assaig de fàbrica (per exemple, la depuració JTAG).

	RE1	Els dispositius de xarxa han de proporcionar una supervisió activa de les interfícies de diagnòstic i assaig del dispositiu i generar una entrada de registre d'auditoria quan es detectin intents d'accés a aquestes interfícies.
NDR 3.2	BR	El dispositiu de xarxa ha de proporcionar protecció contra codis maliciosos.
NDR 3.10	BR	Els dispositius de xarxa han d'admetre la capacitat de ser actualitzats i sotmetre's a una pujada de nivell.
	RE1	Els dispositius de xarxa han de validar l'autenticitat i integritat de qualsevol actualització o pujada de nivell de programari abans de la instal·lació.
NDR 3.11	BR	Els dispositius de xarxa han d'oferir mecanismes de detecció i resistència a la manipulació per protegir contra l'accés físic no autoritzat al dispositiu.
	RE1	Els dispositius de xarxa han de poder notificar automàticament un conjunt configurable de destinataris si descobreixen que s'ha intentat realitzar un accés físic no autoritzat. Totes les notificacions de manipulació s'han de registrar com a part de la funció general de registre d'auditoria.
NDR 3.12	BR	Els dispositius de xarxa han de poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del proveïdor del producte que s'utilitzaran com una o més "arrels de confiança" al moment de la fabricació del dispositiu.
NDR 3.13	BR	Els dispositius de xarxa han de: a) poder proporcionar i protegir la confidencialitat, integritat i autenticitat de les claus i dades del propietari de l'actiu que s'han d'utilitzar com a "arrels de confiança", i b) permetre la capacitat d'aprovisionament sense dependre de components que puguin estar fora de la zona de seguretat del dispositiu.
NDR 3.14	BR	Els dispositius de xarxa han de verificar la integritat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans d'utilitzar-lo en aquest procés d'arrencada.
	RE1	Els dispositius de xarxa han d'utilitzar les arrels de confiança del proveïdor del producte del component per verificar l'autenticitat del microprogramari, el programari i les dades de configuració necessaris per al procés d'arrencada del component abans que s'utilitzi en aquest procés d'arrencada.
NDR 5.2	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de supervisar i controlar les comunicacions en els límits de la zona per aplicar la compartimentació definida en el model de zones de risc i conductes.
	RE1	El component de xarxa ha de proporcionar la capacitat de denegar trànsit de xarxa per defecte i permetre trànsit de xarxa per excepció (també denominat "denegar-ho tot, permís per excepció").
	RE2	El component de xarxa ha d'oferir la capacitat de protegir contra qualsevol comunicació a través del límit del sistema de control (també denominat mode illa).

	RE3	El component de xarxa ha de proporcionar la capacitat de protegir contra qualsevol comunicació a través del límit del sistema de control quan es produeixi una fallada operativa dels mecanismes de protecció de límits (també denominat tancament en cas de fallada).
NDR 5.3	BR	Un dispositiu de xarxa en un límit de zona ha de proporcionar la capacitat de protegir contra la recepció de missatges de propòsit general entre persones rebuts d'usuaris o sistemes externs al sistema de control.