



ATL

Ens d'Abastament
d'Aigua Ter-Llobregat

1.7 DIRECTRIUS DE SEGURETAT

21.11.2024

1.7 Directrius de Seguretat

Índex de continguts

1.	Introducció	5
1.1.	Objectiu del document.....	5
1.2.	Abast i limitacions	5
1.3.	Metodologia d'anàlisis	6
1.4.	Importància de la ciberseguretat en infraestructures crítiques	6
1.5.	Marc normatiu.....	6
1.5.1.	Esquema Nacional de Seguretat (ENS)	7
1.5.2.	Normativa europea: Directiva NIS2.....	7
1.5.3.	Normes internacionals de ciberseguretat industrial	7
1.5.4.	Requisits específics per als sistemes SCADA	8
2.	Punt de partida	9
2.1.	Abast de la seguretat dintre del projecte	9
2.2.	Millors previstes.....	10
3.	Amenaces i vulnerabilitats.....	12
3.1.	Principals amenaces cibernètiques en plantes de tractament d'aigua	12
3.2.	Atacs comuns.....	14
4.	Compliment normatiu	16
4.1.	Política de Seguretat i Normatives (ORG.1, ORG.2, ORG.3, ORG.4)	16
4.2.	Anàlisi i Gestió de Riscos (OP.PL.1, OP.PL.2, OP.PL.3, OP.PL.4, OP.PL.5)	16
4.3.	Control d'Accés i Autenticació (OP.ACC.1, OP.ACC.2, OP.ACC.3, OP.ACC.4, OP.ACC.5, OP.ACC.6, OP.ACC.7)	17
4.4.	Protecció dels Sistemes i Xarxes (OP.EXP.1, OP.EXP.2, OP.EXP.3, OP.EXP.4, OP.EXP.5, OP.EXP.6, OP.EXP.7, OP.EXP.8, OP.EXP.9, OP.EXP.10, OP.EXP.11).....	17
4.5.	Gestió d'Incidents i Continuitat del Negoci (OP.EXP.7, OP.EXP.9, OP.EXP.10, OP.EXP.11, OP.CONT.1, OP.CONT.2, OP.CONT.3).....	17
4.6.	Seguretat Física i Infraestructura (MP.IF.1, MP.IF.2, MP.IF.3, MP.IF.4, MP.IF.5, MP.IF.6, MP.IF.7, MP.IF.9)	18
4.7.	Protecció de la Informació i Criptografia (MP.INFO.1, MP.INFO.2, MP.INFO.3, MP.INFO.4, MP.INFO.5, MP.INFO.6, MP.INFO.9).....	18

1.7 Directrius de Seguretat

4.8.	Relació amb Proveïdors i Seguretat en la Cadena de Subministrament (OP.EXT.1, OP.EXT.2, OP.EXT.9).....	18
4.9.	Formació i Conscienciació (MP.PER.1, MP.PER.2, MP.PER.3, MP.PER.4, MP.PER.9).....	18
5.	Anàlisi de riscos.....	19
5.1.	Identificació d'actius crítics.....	19
5.2.	Avaluació de riscos cibernètics.....	20
5.3.	Probabilitat i impacte dels atacs cibernètics.....	23
6.	Estratègies de protecció i mitigació.....	26
6.1.	Mesures preventives i bones pràctiques sistemes telecontrol	26
6.1.1.	Phishing	26
6.1.2.	Malware, Ransomware i Spyware	26
6.1.3.	Denegació de Servei (DoS)	26
6.1.4.	Home en el Medi (MitM)	27
6.1.5.	Força Bruta	27
6.1.6.	Explotació de Vulnerabilitats.....	27
6.1.7.	Injecció SQL.....	28
6.2.	PROTECCIÓ DE SISTEMES SCADA I PLCs	28
6.2.1.	Configurar Usuaris, Grups i Permisos	28
6.2.2.	Utilitzar el mecanisme d'autenticació de usuaris més adequat (Digest, IdP, AD, etc.).....	28
6.2.3.	Configurar el Control d'Accés per a cada part de l'aplicació SCADA	29
6.2.4.	Restringir l'accés a la eina d'enginyeria	29
6.2.5.	Xifrar les comunicacions amb TLS v1.2 o v1.3.....	29
6.2.6.	Securitzar l'accés remot (clients externs).....	29
6.2.7.	Protegir les comunicacions que no es puguin xifrar (Edge Computing)	30
6.2.8.	Protegir els directoris del SCADA en el sistema operatiu, així com l'accés al servidor	30
6.2.9.	Restricció de ports en el Firewall	30
6.2.10.	Gestió centralitzada dels actius.....	30
6.2.11.	Detecció de vulnerabilitats	30
6.2.12.	Tenir un pla de recuperació (redundància, snapshots, backups en directoris segurs...)	31

1.7 Directrius de Seguretat

6.2.13.	Mantenir el programari actualitzat	31
6.2.14.	Implantació d'un sistema SIEM + SOC per a detecció i resposta 24x7	31
6.2.15.	Control centralitzat de les versions instal·lades en els equips PLC	31
6.2.16.	Realització de pentesting específics de la xarxa d'operacions cada dos anys	32
6.2.17.	Segmentació de la xarxa	32
6.2.18.	Control dels dispositius de memòria portàtils	32
6.3.	Arquitectura de xarxa	40
6.4.	Nivell 0 – Dispositius físics i sensors	41
6.5.	Nivell 1 – Controladors i PLCs	41
6.6.	Nivell 2 – Sistemes HMI i SCADA locals.....	41
6.7.	Nivell 3 – Xarxa d'operacions (OT)	41
6.8.	Nivell 3.5 – DMZ Industrial	41
6.9.	Nivell 4 – Xarxa corporativa (IT)	42
6.10.	Nivell 5 – Nivell de Nube i Serveis Externs	42
6.11.	Definició dels components principals	42
7.	Conclusions i recomanacions finals	43
7.1.	Recomanacions	43
Annex 1.	Coordinació d'aplicabilitat de les mesures de seguretat de l'ens.	46
Llista de taules		
Taula 5-1:	Actius identificats	19
Taula 5-2:	Avaluació de riscos.....	23
Taula 6-1:	Mesures de protecció als riscos detectats.	40
Llista de figures		
Figura 3-1:	Atacs comuns en sistemes SCADA	12
Figura 5-1:	Distribució de la probabilitat dels riscos.....	24
Figura 5-2:	Distribució de l'impacte dels riscos.....	25
Figura 6-1:	Arquitectura Purdue	40

1.7 Directrius de Seguretat

1. INTRODUCCIÓ

La seguretat cibernètica en les infraestructures crítiques és un aspecte fonamental per garantir la fiabilitat i disponibilitat dels serveis essencials. En aquest context, l'Ens d'Abastament d'Aigües Ter-Llobregat (ATL) ha iniciat un projecte de renovació i actualització del sistema d'automatització i telecomandament (SATEL) per millorar l'eficiència operativa i reforçar la seva resiliència davant ciberamenaces. Aquest document estableix les bases tècniques per a la protecció del nou SCADA i dels PLCs Rockwell Automation i Siemens PCS7, seguint els estàndards de ciberseguretat industrial i el marc normatiu de l'Esquema Nacional de Seguretat (ENS).

1.1. Objectiu del document

Aquest document té com a objectiu establir les bases tècniques i metodològiques per a l'anàlisi i implementació de mesures de ciberseguretat en el Sistema d'Automatització i Telecomandament (SATEL) de l'Ens d'Abastament d'Aigües Ter-Llobregat (ATL). Aquesta infraestructura gestiona la captació, el tractament i la distribució d'aigua potable a una població d'aproximadament 5 milions de persones.

Donat que la infraestructura de control actual, basada en sistemes SCADA i PLCs, és un component crític de l'operació diària, la seva renovació suposa un repte tant des del punt de vista de seguretat operativa com de seguretat cibernètica. L'objectiu del present document és establir un marc d'anàlisi de riscos, identificar les principals vulnerabilitats, establir una estratègia de protecció i garantir el compliment de les normatives aplicables, incloent-hi l'Esquema Nacional de Seguretat (ENS).

1.2. Abast i limitacions

Aquest document analitza els riscos associats als sistemes de control industrial (ICS) de plantes potabilitzadores o plantes de tractament i la xarxa de distribució, incloent-hi:

- El SCADA, utilitzat per al monitoratge i control dels processos industrials.
- Els PLCs Rockwell Automation i Siemens PCS7, responsables de l'execució de la lògica de control.
- La infraestructura de comunicacions, basada en connexions Ethernet IP, ControlNet, Profibus i protocols de telecontrol com DNP3 i IEC104.
- Els sistemes de telecomandament i la seva interacció amb la xarxa corporativa d'ATL.

L'anàlisi inclou aspectes com la protecció contra atacs cibernètics, la implementació d'estratègies de resiliència i resposta davant incidents, i la seva integració amb els requeriments de l'ENS. No obstant això, el document no aborda aspectes relacionats amb la seguretat física de les instal·lacions ni la protecció contra amenaces naturals.

1.7 Directrius de Seguretat

1.3. Metodologia d'anàlisi

L'anàlisi de ciberseguretat es realitza seguint un enfocament basat en riscos, estructurat en les següents fases:

- Identificació d'actius crítics: inventari dels dispositius, programari i sistemes connectats a la xarxa scada.
- Avaluació de vulnerabilitats: anàlisi dels punts febles dels sistemes de control i la seva exposició a possibles ciberatacs.
- Anàlisi de l'impacte i la probabilitat: classificació de les amenaces segons el seu nivell de risc i les possibles conseqüències en l'operació de la planta.
- Mesures de mitigació: definició d'estratègies per minimitzar riscos, incloent-hi la segmentació de xarxes, control d'accessos i reforç de protocols de seguretat.
- Implementació del marc ENS: adaptació del sistema a les directrius de l'esquema nacional de seguretat per garantir el compliment normatiu i la protecció davant amenaces avançades.

1.4. Importància de la ciberseguretat en infraestructures crítiques

Les plantes potabilitzadores, plantes de tractament i les xarxes de distribució d'aigua són infraestructures crítiques que, en cas de ser atacades, poden provocar:

- Alteracions en la qualitat de l'aigua subministrada, posant en risc la salut pública.
- Interrupcions en el servei, afectant milions de persones i provocant danys econòmics i reputacionals.
- Manipulació de dades operacionals, generant errors en la gestió del subministrament i en la presa de decisions.
- Sabotatge d'infraestructures crítiques, que podria comprometre la seguretat física de les instal·lacions.
- En els darrers anys, s'han detectat atacs cibernètics dirigits a sistemes SCADA en diverses infraestructures d'aigua a escala mundial, cosa que posa en relleu la necessitat d'adoptar estratègies proactives de protecció i seguretat en entorns OT (Operational Technology).

Aquest document serveix com a guia per a la implementació d'un model de ciberseguretat robust, resiliència i alineat amb les polítiques internes de seguretat de la informació d'ATL i l'ENS, assegurant així la continuïtat del servei i la protecció de la infraestructura crítica.

1.5. Marc normatiu

La ciberseguretat en les infraestructures crítiques, com les plantes de tractament i distribució d'aigua, està subjecta a un conjunt de normatives i regulacions tant a nivell nacional com internacional. L'objectiu és garantir

1.7 Directrius de Seguretat

la protecció dels sistemes d'automatització i telecomandament davant possibles amenaces cibernètiques que puguin posar en risc la continuïtat del servei i la seguretat pública.

A continuació, es detallen les principals normatives aplicables a les plantes potabilitzadores de tractament de l'Ens d'Abastament d'Aigües Ter-Llobregat (ATL) en matèria de seguretat de la informació i protecció dels sistemes industrials.

1.5.1. Esquema Nacional de Seguretat (ENS)

L'Esquema Nacional de Seguretat (ENS), regulat pel Reial Decret 311/2022, estableix els requisits de seguretat que han de complir les entitats públiques i aquelles empreses privades que gestionen serveis essencials, com el subministrament d'aigua. L'ENS classifica els sistemes d'informació en diferents nivells de seguretat (bàsic, mitjà i alt), en funció del seu impacte en cas de ciberatac.

Per a ATL, que gestiona una infraestructura crítica, és essencial l'aplicació de l'ENS en els seus sistemes SCADA i d'automatització industrial, garantint la implantació de controls de seguretat en àrees com:

- Protecció de xarxes i sistemes de control industrial (OT)
- Gestió d'accés i autenticació forta
- Monitoratge continu i resposta davant incidents
- Seguretat en la comunicació entre sistemes SCADA i xarxes corporatives
- Plans de continuïtat i recuperació davant ciberatacs

1.5.2. Normativa europea: Directiva NIS2

La Directiva NIS2 (Network and Information Security Directive) és la normativa europea per a la ciberseguretat en infraestructures essencials i substitueix la Directiva NIS original. Aquesta normativa exigeix als operadors d'infraestructures crítiques com ATL:

- Avaluar i mitigar riscos cibernètics en els seus sistemes industrials.
- Garantir una resposta eficaç davant incidents mitjançant plans d'acció i protocols de recuperació.
- Aplicar mesures de seguretat en la cadena de subministrament per protegir-se de possibles vulnerabilitats derivades de proveïdors externs.
- Reportar incidents de seguretat a l'autoritat competent en un termini màxim de 24 hores.

1.5.3. Normes internacionals de ciberseguretat industrial

A més de l'ENS i la Directiva NIS2, la renovació del sistema SCADA d'ATL ha d'alinejar-se amb els següents estàndards internacionals en ciberseguretat industrial:

1.7 Directrius de Seguretat

- ISO/IEC 27001: Norma internacional per a la gestió de la seguretat de la informació, que estableix controls per protegir dades i sistemes d'informació.
- IEC 62443: Estàndard específic per a la seguretat en sistemes d'automatització industrial (ICS/SCADA), que cobreix aspectes com la segmentació de xarxes, control d'accés i protecció contra atacs cibernètics.
- NIST Cybersecurity Framework: Model desenvolupat pel National Institute of Standards and Technology dels EUA per avaluar riscos i implantar mesures de protecció en infraestructures crítiques.

1.5.4. Requisits específics per als sistemes SCADA

D'acord amb aquestes normatives, la implementació del nou SCADA i la renovació dels PLCs Rockwell Automation i Siemens PCS7 hauran de contemplar:

- Segmentació de xarxes OT i IT per minimitzar el risc d'atacs laterals.
- Autenticació multifactor (MFA) per als operadors del sistema.
- Encriptació de comunicacions entre PLCs i el sistema SCADA.
- Control de dispositius USB i altres vectors d'entrada de malware.
- Monitoratge i detecció de tràfic anòmal en les comunicacions SCADA.

1.7 Directrius de Seguretat

2. PUNT DE PARTIDA

El sistema SCADA d'ATL ha evolucionat al llarg dels anys per convertir-se en una eina robusta i essencial per a la gestió i supervisió del subministrament d'aigua potable a milions de persones. Aquest sistema integra tecnologies avançades d'automatització i telecomandament, permetent un control eficient de les plantes de tractament i estacions remotes. ATL compta amb un equip tècnic altament qualificat, especialitzat en sistemes d'automatització i telecontrol, que garanteix el correcte funcionament i la millora contínua del sistema.

Una de les grans forteses del sistema SCADA actual és la seva capacitat per operar en temps real i gestionar una àmplia xarxa d'actius distribuïts. La infraestructura disposa de diversos centres de control autònoms però interconnectats, cosa que permet una supervisió descentralitzada i una resposta ràpida davant qualsevol eventualitat. A més, l'ús d'equips de primer nivell com els PLC d'Allen-Bradley i Siemens assegura una alta fiabilitat en el processament de dades i en la gestió de les instal·lacions.

El sistema SCADA també destaca per la seva capacitat d'adaptació a noves tecnologies i estàndards industrials, fet que ha permès incorporar servidors virtualitzats a l'any 2017 i sistemes de comunicació eficients com Ethernet IP, ControlNet i Modbus. L'ús de solucions SCADA avançades, com Aspen InfoPlus.21®, proporciona als operadors eines potents per la supervisió i anàlisi de dades, facilitant una presa de decisions informada. A més, el sistema ja disposa de monitorització amb Nagios, una eina clau per garantir la disponibilitat i el rendiment dels servidors i la infraestructura de xarxa.

Tot i aquestes forteses, encara hi ha àrees de millora que ATL ha identificat i que s'estan considerant per a futures actualitzacions. Entre els aspectes a reforçar, cal millorar la redundància del sistema SCADA, implementant solucions que garanteixin la continuïtat del servei en cas de fallades. També és necessari reforçar la seguretat de les comunicacions, incorporant xifratge i mecanismes d'autenticació més robustos per protegir la transmissió de dades. Finalment, ATL pot potenciar la detecció i resposta a incidents cibernètics, mitjançant la implementació de sistemes SIEM i protocols avançats de seguretat.

En definitiva, el sistema SCADA d'ATL és una infraestructura sòlida i ben gestionada que assegura el subministrament d'aigua amb garanties d'eficiència i fiabilitat. Amb les millores planificades en matèria de ciberseguretat, redundància i gestió d'accessos, ATL continuarà sent una referència en la gestió intel·ligent de xarxes de distribució d'aigua, consolidant-se com un model de modernització i innovació en el sector.

2.1. Abast de la seguretat dintre del projecte

Des de el punt de vista de seguretat i addicionalment el compliment normatiu de l'Esquema Nacional de Seguretat (en endavant ENS) nivell mig/alt, el telecontrols i xarxes del PLC de les plantes tractament d'aigua potable (ETAP) de PTT i PTLL i la xarxa de distribució.

1.7 Directrius de Seguretat

Per aquest proveïdor la seguretat en fonamental en qualsevol projecte i/o servei, per aquest motiu realitzarem les següents activitats orientades a l'increment de la seguretat i compliment normatiu :

- Identificació d'actius.
- Avaluació de riscos del telecontrols i xarxes d'operació : Realitzar una avaluació de riscos de ciberseguretat als quals està exposat el telecontrol i estació remota. Això implica identificar les possibles amenaces, vulnerabilitats i possibles impactes en el sistema.
- Disseny i planificació de la seguretat: Desenvolupar un pla per l'increment de la seguretat en els telecontrol i estacions remotes que contempli les mesures necessàries per protegir els sistemes.
- Implementació de mesures de seguretat: Posar en pràctica les mesures de seguretat definides en el pla i/o recomanacions al client, assegurant-se que es configuren correctament i es realitzen proves de funcionalitat i seguretat.
- Monitoratge i detecció d'incidents: Implementar sistemes de monitoratge i detecció de possibles incidents de seguretat, que permetin identificar activitat sospitosa i respondre de manera oportuna a qualsevol anomalia.
- Radar tecnològic i millora contínua: Mantenir el pla de ciberseguretat actualitzat i realitzar revisions periòdiques per incorporar noves amenaces i tecnologies emergents.
- Queda exclòs del projecte la seguretat de la xarxa, aquesta quedarà en mans del departament de sistemes d'ATL.

2.2. Millores previstes

El sistema d'informació actual d'ATL presenta una arquitectura de control i telemetria distribuïda en diverses plantes i estacions remotes, amb una interconnectivitat que permet la gestió centralitzada de dades i processos. No obstant això, l'anàlisi de ciberseguretat indica que el sistema SCADA opera amb un entorn de seguretat que requereix millores en termes de segmentació de xarxa, autenticació d'usuaris i monitoratge d'esdeveniments. Actualment, la infraestructura no disposa de redundància distribuïda per a la continuïtat del servei en cas d'incidents cibernètics o fallades de maquinari, fet que podria comprometre la disponibilitat operativa dels processos crítics de subministrament d'aigua.

En l'àmbit de les comunicacions, el sistema es basa en protocols d'intercanvi de dades com OPC UA, Modbus i Ethernet IP, amb connexions establertes a través de GPRS, VSAT i fibra òptica. Tot i que aquests protocols són àmpliament utilitzats a la indústria, no tots incorporen xifratge d'extrem a extrem ni mecanismes avançats d'autenticació i autorització. La manca d'una gestió centralitzada de credencials i permisos en els equips de camp representa un risc potencial d'accessos no autoritzats, fet que podria derivar en manipulacions indegudes del sistema o en atacs de denegació de servei (DoS).

1.7 Directrius de Seguretat

Des del punt de vista del monitoratge i resposta davant d'incidents, ATL utilitza eines com Nagios per supervisar l'estat de servidors i xarxes, tot i que la cobertura de la plataforma és limitada pel que fa a la detecció d'anomalies avançades i correlació d'esdeveniments en temps real. L'absència d'un Security Information and Event Management (SIEM) impedeix una visibilitat completa dels intents d'accés sospitosos, canvis en la infraestructura o activitat inusual dins de l'entorn SCADA. Això dificulta la implementació d'estratègies de detecció primerenca i resposta automatitzada davant de ciberatacs o fallades de seguretat.

Finalment, en termes de continuïtat operativa, el sistema actual no disposa de mecanismes robustos de recuperació davant de desastres en cas d'interrupcions prolongades del servei o atacs a la infraestructura. No existeix un procediment documentat de recuperació de dades en cas de pèrdua de comunicacions entre els PLC i el SCADA, fet que implica que certs esdeveniments crítics podrien no registrar-se ni analitzar-se posteriorment. La implementació de mesures com la redundància geogràfica, l'emmagatzematge descentralitzat de registres i proves regulars de restauració de còpies de seguretat són essencials per mitigar aquests riscos i garantir la seguretat i estabilitat del sistema d'informació en el futur.

1.7 Directrius de Seguretat

3. AMENACES I VULNERABILITATS

3.1. Principals amenaces cibernètiques en plantes de tractament d'aigua

El sistema SCADA d'ATL és una infraestructura crítica per a la gestió i supervisió del subministrament d'aigua potable a milions de persones. No obstant això, en l'actualitat presenta diverses vulnerabilitats en termes de seguretat de la informació, que poden comprometre la seva disponibilitat, integritat i confidencialitat. Aquestes mancances afecten tant la protecció de les comunicacions entre equips i centres de control com el control d'accés a la informació, la resiliència del sistema davant de fallades o atacs cibernètics i la capacitat de resposta a incidents. A més, s'ha detectat una falta d'estandardització en la gestió d'alarmes i en els mecanismes de recuperació de dades en cas d'interrupcions, així com absència de polítiques clares de ciberseguretat i protocols d'actuació davant d'amenaces. Aquest informe analitza en profunditat les principals problemàtiques detectades i la seva implicació en la seguretat operativa d'ATL, destacant la necessitat d'una modernització urgent per adaptar-se als estàndards internacionals de seguretat en sistemes industrials. Seguidament s'identifiquen les mancances més importants.

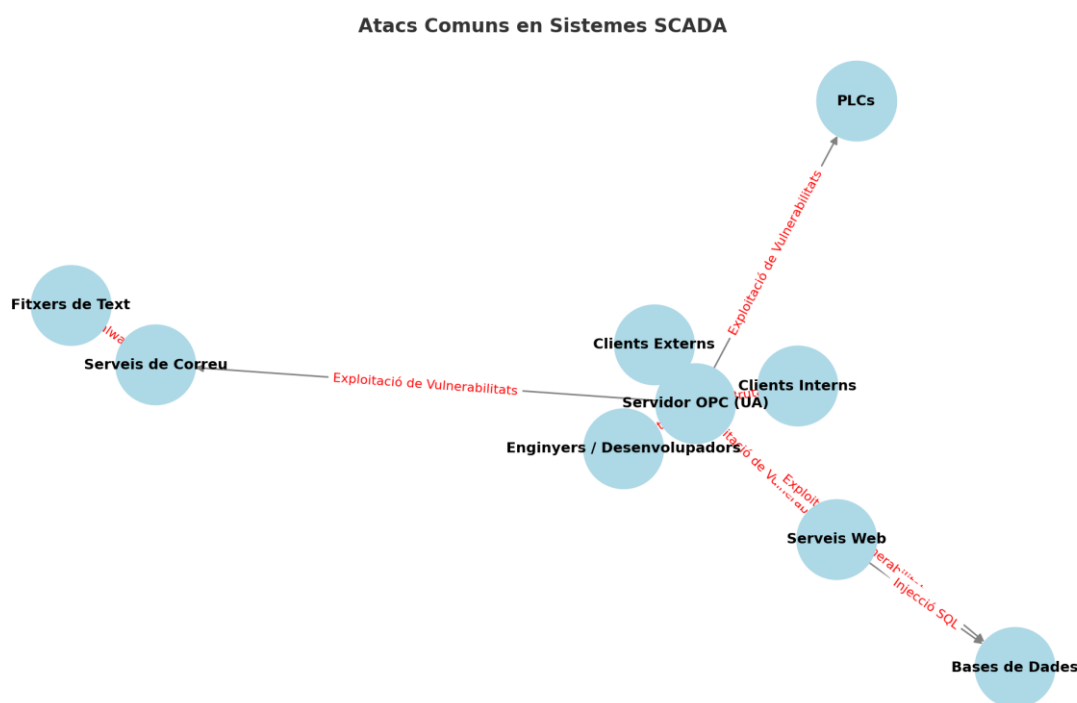


Figura 3-1: Atacs comuns en sistemes SCADA

1.7 Directrius de Seguretat

- **Manca de redundància i resiliència.** Actualment, el sistema SCADA no disposa d'un mecanisme de redundància complet. Això significa que en cas de fallada d'un servidor o d'un component clau, els operadors podrien perdre el control de les instal·lacions crítiques, afectant la gestió del subministrament d'aigua. Aquest escenari posa en risc la disponibilitat del servei i pot ocasionar situacions operatives difícils de gestionar. Un altre aspecte preocupant és la manca d'un sistema de recuperació de dades entre els autòmats programables (PLC) i el SCADA. Quan es produeixen interrupcions en les comunicacions, les dades històriques no es conserven ni es poden recuperar posteriorment. Aquesta situació impedeix als operadors conèixer amb exactitud què ha passat durant el període de fallada, la qual cosa pot afectar tant la presa de decisions com la qualitat del servei.
- **Vulnerabilitat en la seguretat en les comunicacions.** El sistema de telecontrol fa servir diferents protocols de comunicació, com Ethernet IP, ControlNet, Modbus i Profibus. Tot i que aquests protocols són àmpliament utilitzats en la indústria, molts d'ells no incorporen mecanismes de xifratge ni autenticació robusta. Això vol dir que la informació que circula per la xarxa podria ser interceptada o manipulada per un agent extern. Pel que fa a les estacions remotes, la comunicació es basa principalment en GPRS i VSAT, tecnologies que, si no es protegeixen adequadament, poden ser vulnerables a atacs de man-in-the-middle (MitM) o altres tècniques d'intrusió. La manca d'un sistema de segmentació de xarxa també suposa un risc, ja que permetria que un atac en un punt de la infraestructura es propagui a altres sistemes.
- **Vulnerabilitat en el control d'accés.** Una de les principals mancances de seguretat identificades és la falta d'un control d'accés centralitzat. Actualment, no existeix un sistema uniforme de gestió de credencials i permisos per als diferents usuaris i equips de camp. Això pot facilitar accessos no autoritzats, tant de manera interna com externa, i augmenta el risc de manipulació no controlada del sistema.
- **Vulnerabilitat en la monitorització de la seguretat.** En termes de supervisió i detecció d'incidents, ATL utilitza Nagios per monitoritzar el rendiment dels servidors i la xarxa. Tot i això, aquesta eina només ofereix una vigilància bàsica, sense capacitats avançades per correlacionar esdeveniments ni detectar patrons anòmals de comportament. La manca d'un sistema SIEM (Security Information and Event Management) dificulta la identificació d'activitats sospitoses i retarda la resposta davant d'un ciberatac.
- **Vulnerabilitats en la gestió d'alarmes i dades.** Un altre aspecte crític és la falta d'un model estandarditzat de gestió d'alarmes, ja que no es segueixen estàndards com ISA-18.2, que ajuden a millorar la prioritització i identificació d'incidents rellevants. Això pot portar a situacions de sobrecàrrega d'alarmes, generant confusió en els operadors i dificultant la resposta ràpida a incidents reals. A més, no hi ha mecanismes de validació de la integritat de les dades en el sistema SCADA. Això significa que no es pot verificar si les dades han estat alterades, intencionadament o per error, afectant la fiabilitat de la informació utilitzada per a la presa de decisions operatives. La manca de controls de registre i auditories sistemàtiques pot dificultar la detecció de possibles manipulacions indegudes.

1.7 Directrius de Seguretat

- **Manca d'un pla de seguretat i resposta a incidents.** No s'ha identificat l'existència d'un pla formal de ciberseguretat per protegir la infraestructura SCADA contra possibles atacs o fallades de seguretat. La manca d'un marc regulador clar per a la protecció de dades, el xifratge de comunicacions i l'autenticació d'usuaris augmenta el risc d'atacs i de pèrdua d'informació crítica. D'altra banda, no hi ha constància de l'existència d'un equip de resposta a incidents de seguretat (CSIRT o OT-SOC) dedicat a gestionar ciberatacs o fallades crítiques en la infraestructura de telecontrol. Això significa que, en cas d'una intrusió o una amenaça interna, ATL no disposaria d'un protocol establert per contenir, analitzar i mitigar l'impacte de l'atac de manera eficient.

3.2. Atacs comuns

Els sistemes SCADA són fonamentals per a la gestió i automatització d'infraestructures crítiques com la distribució d'aigua, i per aquest motiu són objectiu de diferents tipus d'atacs cibernètics. Entre els més freqüents trobem atacs dirigits al personal, atacs al sistema i atacs a les comunicacions, que poden comprometre la disponibilitat, la integritat i la confidencialitat de les dades.

- Un dels atacs més comuns és el phishing, on els ciberdelinqüents enganyen els operadors interns o externs mitjançant correus electrònics fraudulents o pàgines web falsificades per robar credencials d'accés. Per exemple, un tècnic d'ATL podria rebre un correu aparentment legítim amb un enllaç a un portal fals on se li demana introduir la seva contrasenya. Si cau en el parany, els atacants podrien obtenir accés al sistema SCADA i alterar els seus paràmetres.
- D'altra banda, el malware, el ransomware i l'spyware són amenaces que poden infectar els servidors SCADA i afectar el seu funcionament. Per exemple, si un operador descarrega un fitxer maliciós sense adonar-se'n, un virus podria xifrar totes les dades del sistema (ransomware) i exigir un rescat per desbloquejar-les, deixant ATL sense capacitat de monitoritzar i controlar les seves plantes.
- Els atacs de denegació de servei (DoS) també són una amenaça greu per als sistemes SCADA. Aquests atacs consisteixen a enviar un volum massiu de peticions al servidor de control, fent que es col·lapsi i deixi de respondre. Un atacant podria, per exemple, saturar el sistema de telecontrol amb milers de sol·licituds falses, impedit que els operadors puguin gestionar els processos de distribució d'aigua de manera efectiva.
- En l'àmbit de les comunicacions, els atacs de Man-in-the-Middle (MitM) suposen un risc significatiu. Aquest tipus d'atac permet a un intrús interceptar i modificar missatges entre el SCADA i els PLC sense que els operadors se n'adonin. Això podria ser utilitzat per alterar valors crítics com el cabal d'aigua o els nivells de pressió, provocant disrupcions en el servei o manipulant les dades per encobrir una fallada.
- L'explotació de vulnerabilitats és una altra tècnica utilitzada pels atacants per aprofitar errors o mancances de seguretat en el sistema SCADA. Si el sistema no s'actualitza regularment, un atacant podria utilitzar una vulnerabilitat coneguda per accedir al servidor i prendre el control remot de les estacions de tractament d'aigua.

1.7 Directrius de Seguretat

- Els atacs per força bruta també són una amenaça, ja que consisteixen a provar automàticament múltiples combinacions de contrasenyes fins a trobar la correcta. Si els comptes d'usuari d'ATL utilitzen contrasenyes febles o per defecte, un atacant podria accedir fàcilment al sistema. Per exemple, si un operador manté la contrasenya per defecte d'un PLC, un atacant podria accedir-hi i alterar la seva configuració sense permís.
- Finalment, la injecció SQL és una tècnica que permet als atacants inserir codi maliciós en bases de dades connectades al SCADA. Això podria permetre a un ciberdelinqüent modificar registres crítics, com les dades d'operació dels sistemes de distribució d'aigua, alterant així el seu comportament o eliminant informació essencial per al control del servei.

Per fer front a aquestes amenaces, és essencial implementar bones pràctiques de seguretat com l'ús de contrasenyes robustes, actualitzacions periòdiques, segmentació de xarxa, xifratge de dades i formació contínua dels operadors. Un sistema SCADA segur és clau per garantir la continuïtat i fiabilitat del servei de distribució d'aigua i protegir-lo davant d'amenaces cibernètiques cada cop més sofisticades.

1.7 Directrius de Seguretat

4. COMPLIMENT NORMATIU

L'actualització del sistema d'automatització i telecontrol de l'Ens d'Abastament d'Aigües Ter-Llobregat s'emmarca dins d'un entorn normatiu que regula la seguretat d'infraestructures crítiques i xarxes d'operació. En aquest context, destaquen l'Esquema Nacional de Seguretat (ENS), que estableix els principis i requisits de ciberseguretat en l'àmbit del sector públic i operadors estratègics, i la Directiva NIS2, que reforça la resiliència de les infraestructures essencials davant els ciberatacs. La NIS2 amplia l'abast dels requisits de seguretat, exigint la implementació de mesures de gestió de riscos, supervisió contínua i resposta davant incidents en infraestructures industrials, com els sistemes SCADA i PLCs. En compliment amb aquestes normatives, el nou sistema garantirà la protecció de la informació i la continuïtat operativa, aplicant principis de seguretat des del disseny, segmentació de xarxes IT/OT i controls d'accés reforçats. S'establiran estratègies de detecció i resposta a amenaces, alineades amb els estàndards europeus i nacionals en ciberseguretat per a infraestructures crítiques.

La implementació d'un marc de ciberseguretat sòlid en infraestructures crítiques com les gestionades per ATL requereix una estratègia integral que garanteixi la protecció, la disponibilitat i la resiliència dels sistemes. Per assegurar el compliment de l'**Esquema Nacional de Seguretat (ENS)** i altres normatives aplicables, s'han establert un conjunt de directrius que abasten diversos àmbits fonamentals de la seguretat de la informació. Aquestes directrius inclouen la definició d'una política de seguretat clara, l'anàlisi i gestió de riscos, el control d'accés, la protecció de sistemes i xarxes, la gestió d'incidentes, la seguretat física, la protecció de la informació, la relació amb proveïdors i la formació contínua del personal. A continuació, es detallen aquests nou blocs estratègics, incorporant les mesures específiques que ATL i els seus proveïdors han d'adoptar per garantir un entorn segur i resilient davant les amenaces cibernètiques.

4.1. Política de Seguretat i Normatives (ORG.1, ORG.2, ORG.3, ORG.4)

Per garantir la protecció adequada del sistema, es definirà o adaptarà la política de seguretat (ORG.1) aprovada per ATL, que cobreix tant la infraestructura IT com la d'operacions (OT). Aquesta política estableix els rols i responsabilitats dels diferents actors involucrats, així com el marc normatiu aplicable. També es requereix una normativa de seguretat (ORG.2) documentada, que reguli l'ús correcte dels actius de la xarxa d'operacions i les responsabilitats del personal, incloent-hi drets, deures i mesures disciplinàries. A més, es documenten els procediments de seguretat (ORG.3) per a la instal·lació, operació i manteniment dels sistemes, així com un procés d'autorització (ORG.4) per garantir que només personal autoritzat pugui accedir a determinats sistemes.

4.2. Anàlisi i Gestió de Riscos (OP.PL.1, OP.PL.2, OP.PL.3, OP.PL.4, OP.PL.5)

Es realitzarà una anàlisi de riscos en profunditat (OP.PL.1) que identifica els actius crítics, les principals amenaces i les salvaguardes aplicables per mitigar els riscos. Aquesta anàlisi es revisa periòdicament i es

1.7 Directrius de Seguretat

documenta en la Guia d'Instal·lació Segura. A més, s'especifica l'arquitectura de seguretat (OP.PL.2) mitjançant diagrames que detallen les connexions i fluxos de dades, així com les proteccions implementades. La gestió de nous components (OP.PL.3) garanteix que qualsevol nova adquisició compleixi amb els estàndards de seguretat de l'arquitectura del sistema. Per mantenir la coherència en la seguretat, s'estableix un pla de capacitat i dimensionament (OP.PL.4), assegurant que el sistema pugui gestionar el volum d'informació i tràfic requerits. Addicionalment, es prioritza l'ús de components certificats (OP.PL.5) per garantir la seguretat de la infraestructura TIC.

4.3. Control d'Accés i Autenticació (OP.ACC.1, OP.ACC.2, OP.ACC.3, OP.ACC.4, OP.ACC.5, OP.ACC.6, OP.ACC.7)

La identificació i gestió d'usuaris es realitza a través d'un sistema centralitzat Active Directory (OP.ACC.1), assegurant la traçabilitat i l'administració eficient dels permisos. S'estableixen requisits estrictes d'accés (OP.ACC.2), limitant les credencials als recursos estrictament necessaris. La segregació de funcions i tasques (OP.ACC.3) evita que un sol usuari pugui realitzar accions crítiques sense supervisió. El procés de gestió de drets d'accés (OP.ACC.4) garanteix que es revisin periòdicament les altes, modificacions i baixes d'usuaris. Els mecanismes d'autenticació (OP.ACC.5) inclouen l'ús de contrasenyes robustes i autenticació multifactor (MFA). L'accés local (OP.ACC.6) es limita a dispositius autoritzats, mentre que l'accés remot (OP.ACC.7) es protegeix mitjançant VPN i altres mecanismes de seguretat.

4.4. Protecció dels Sistemes i Xarxes (OP.EXP.1, OP.EXP.2, OP.EXP.3, OP.EXP.4, OP.EXP.5, OP.EXP.6, OP.EXP.7, OP.EXP.8, OP.EXP.9, OP.EXP.10, OP.EXP.11)

Es prioritza la segmentació de xarxes (MP.COM.4) per evitar que un atac comprometi simultàniament sistemes IT i OT. La comunicació entre dispositius i sistemes industrials ha d'estar protegida amb protocols segurs (MP.COM.2) com TLS v1.2 o v1.3. També es restringeixen els ports oberts (MP.COM.1) mitjançant polítiques de firewall, permetent només aquells necessaris per a l'operació. Per detectar amenaces, s'implementa un sistema SIEM i SOC 24/7 (OP.EXP.8), que permet la detecció i resposta ràpida davant incidents. La protecció contra codi maliciós es reforça amb eines de detecció i prevenció d'intrusions (OP.EXP.6), i l'ús controlat de dispositius USB i altres mitjans extraïbles (MP.IF.7).

4.5. Gestió d'Incidents i Continuitat del Negoci (OP.EXP.7, OP.EXP.9, OP.EXP.10, OP.EXP.11, OP.CONT.1, OP.CONT.2, OP.CONT.3)

Es documenta un pla de gestió d'incidents (OP.EXP.7) per a la detecció, resposta i mitigació de ciberamenaces, amb protocols d'escalat i comunicació a ATL. També es defineix un pla de continuïtat del negoci (OP.CONT.2) que garanteix la recuperació dels sistemes en cas d'interrupció. Aquest pla inclou còpies de seguretat (MP.INFO.9) periòdiques, l'ús de sistemes redundants i proves periòdiques de recuperació (OP.CONT.3).

1.7 Directrius de Seguretat

4.6. Seguretat Física i Infraestructura (MP.IF.1, MP.IF.2, MP.IF.3, MP.IF.4, MP.IF.5, MP.IF.6, MP.IF.7, MP.IF.9)

Per protegir els actius físics, es requereixen controls d'accés físic (MP.IF.1, MP.IF.2) a les instal·lacions, identificant i registrant el personal autoritzat. Es garanteix la protecció contra incendis (MP.IF.5), inundacions (MP.IF.6) i interrupcions elèctriques (MP.IF.4) amb sistemes de suport energètic i SAIs.

4.7. Protecció de la Informació i Criptografia (MP.INFO.1, MP.INFO.2, MP.INFO.3, MP.INFO.4, MP.INFO.5, MP.INFO.6, MP.INFO.9)

S'implementen mesures per garantir la confidencialitat, integritat i disponibilitat de la informació. Es requereix el xifrat de dades (MP.INFO.3) tant en trànsit com en repòs. La gestió de claus criptogràfiques (OP.EXP.11) està documentada i se'n regula l'ús, rotació i emmagatzematge segur. També es defineixen polítiques de còpies de seguretat (MP.INFO.9).

4.8. Relació amb Proveïdors i Seguretat en la Cadena de Subministrament (OP.EXT.1, OP.EXT.2, OP.EXT.9)

Es formalitzen acords de nivell de servei (SLA) (OP.EXT.1) per garantir que els proveïdors compleixen els requisits de seguretat establerts per ATL. La gestió de canvis (OP.EXP.5) es realitza seguint un procediment documentat.

4.9. Formació i Conscienciació (MP.PER.1, MP.PER.2, MP.PER.3, MP.PER.4, MP.PER.9)

Per reduir el risc d'errors humans, es duen a terme programes de formació (MP.PER.4) i sensibilització en ciberseguretat per a tot el personal involucrat. També s'inclouen simulacions d'atacs i auditories (MP.PER.3).

L'**Annex 1** del present document recull de manera detallada tots els **punts de control de l'Esquema Nacional de Seguretat (ENS)** aplicables al projecte, incloent-hi les mesures específiques que han de ser implementades per garantir el compliment normatiu. En aquest annex s'especifiquen les **responsabilitats tant del proveïdor com d'ATL**, així com les accions necessàries per assegurar la protecció dels sistemes d'informació, la gestió de riscos, el control d'accessos, la protecció de xarxes i altres aspectes fonamentals de la seguretat. A més, s'inclouen les referències als controls de seguretat corresponents, facilitant així la seva aplicació i verificació dins del marc establert per l'ENS.

1.7 Directrius de Seguretat

5. ANÀLISI DE RISCOS

5.1. Identificació d'actius crítics

En el marc del projecte de renovació del sistema d'automatització i telecomandament d'ATL, s'han identificat un conjunt d'actius crítics que constitueixen la base operativa del sistema SCADA. Aquests actius inclouen controladors lògics programables (PLC), sistemes SCADA, interfícies HMI, infraestructura de comunicacions, xarxa de distribució, estacions remotes, centres de control, instrumentació especialitzada i equips industrials. La correcta gestió i protecció d'aquests actius és essencial per garantir la fiabilitat, seguretat i eficiència en l'operació de les plantes i la xarxa de distribució d'aigua. A continuació, es detallen els actius identificats i la seva ubicació dins de l'arquitectura del sistema, assegurant així una visió clara dels elements que requereixen especial atenció.

Categoria	Tipus	Quantitat aproximada	Ubicació
PLC	Allen Bradley PLC-5	9	Centres de control
PLC	Allen Bradley SLC-500	201	Estacions remotes
PLC	Allen Bradley ControlLogix	59	Centres de control i plantes
PLC	Allen Bradley CompactLogix	82	Centres de control i estacions remotes
PLC	Siemens PCS7	6	ITAMs
SCADA	Aspen InfoPlus.21	3	Centres de control
SCADA	Siemens PCS7	2	ITAMs
SCADA	Wonderware Intouch	1	ETAP Cardener
HMI	PanelView	5	Plantes i centres de control
HMI	HMI industrial	10	Estacions remotes
Infraestructura de comunicacions	Comunicacions fixes (fibra, coure)	3	Plantes i xarxa de distribució
Infraestructura de comunicacions	Comunicacions sense fils (GPRS, VSAT)	2	Plantes i xarxa de distribució
Xarxa de distribució	Conduccions d'aigua	500	Xarxa de distribució
Estacions remotes	Dipòsits i estacions de bombeig	300	Estacions remotes
Centres de control	SCADA de cada centre	5	Centres de control
Instrumentació	Transmissors de cabal	100	Xarxa de distribució
Instrumentació	Transmissors de nivell i pressió	150	Xarxa de distribució
Instrumentació	Analitzadors de clor residual	80	Xarxa de distribució
Instrumentació	Analitzadors de xarxa elèctrica	50	Xarxa de distribució
Equips industrials	Vàlvules, bombes i altres equips	200	Plantes i xarxa de distribució

Taula 5-1: Actius identificats

1.7 Directrius de Seguretat

5.2. Avaluació de riscos cibernètics

L'anàlisi de riscos és una part fonamental de la gestió de la seguretat en infraestructures crítiques com el sistema SCADA. Identificar, avaluar i mitigar els possibles riscos permet garantir la disponibilitat, integritat i confidencialitat de les operacions, minimitzant l'impacte de possibles incidents. En aquest document es presenta una taula amb 30 riscos identificats, que inclouen amenaces relacionades amb fallades de PLCs, obsolescència de sistemes, ciberatacs, errors humans, problemes de comunicació i manca de redundància. Per a cada risc es detalla la seva descripció, impacte, probabilitat i les accions de mitigació recomanades, amb l'objectiu de reforçar la seguretat i la resiliència del sistema SCADA davant possibles amenaces.

Risc	Descripció del Risc	Impacte	Probabilitat	Accions de Mitigació
Fallada de PLC	Un error en un PLC pot aturar processos crítics de producció i distribució d'aigua.	Alt	Mitjà	Implementar PLCs redundants i establir protocols de manteniment preventiu.
Obsolescència de SCADA	L'obsolescència del sistema SCADA pot generar incompatibilitats i vulnerabilitats.	Alt	Alt	Planificar una renovació escalonada del SCADA i assegurar suport del fabricant.
Intrusió en comunicacions	Intercepció o manipulació de comunicacions per accés no autoritzat.	Molt Alt	Alt	Xifratge de comunicacions, ús de VPN i monitoratge de tràfic de xarxa.
Pèrdua de dades d'instrumentació	Sensors defectuosos o atacs poden provocar la pèrdua de dades operacionals.	Mitjà	Mitjà	Implementar sistemes de validació de dades i redundància en sensors crítics.
Ciberatac a centres de control	Un atac a un centre de control pot provocar el bloqueig del sistema de telecomandament.	Molt Alt	Baix	Segmentació de xarxa, aplicació de controls d'accés i monitoratge en temps real.
Fallada d'estacions remotes	La fallada d'una estació remota pot afectar la supervisió i control d'actius productius.	Alt	Mitjà	Establir procediments de resposta ràpida i mecanismes d'accés alternatius.
Atac a dispositius HMI	Un atac a les interfícies HMI pot comprometre la	Alt	Mitjà	Monitorització contínua de sessions i aplicació de

1.7 Directrius de Seguretat

Risc	Descripció del Risc	Impacte	Probabilitat	Accions de Mitigació
	seguretat operativa del sistema.			polítiques de seguretat HMI.
Falta de redundància en xarxa	L'absència de redundància a la xarxa pot deixar el sistema SCADA inoperatiu.	Molt Alt	Baix	Implementació d'una arquitectura de xarxa amb redundància geogràfica.
Desconfiguració de PLCs	Modificacions incorrectes als PLC poden alterar el funcionament de l'automatització.	Alt	Alt	Control de versions, autenticació forta i registres d'auditoria en PLCs.
Pèrdua de dades històriques	La pèrdua d'històrics pot afectar la presa de decisions i l'anàlisi de tendències.	Mitjà	Mitjà	Còpies de seguretat freqüents i emmagatzematge segur de dades històriques.
Error de programació en PLC	Error de programació poden provocar funcionaments incorrectes dels processos industrials.	Mitjà	Mitjà	Aplicar metodologies de programació segura i proves abans de desplegament.
Mala configuració de permisos d'usuari	Permisos mal configurats poden donar accés no autoritzat a operadors o atacants.	Alt	Mitjà	Configurar permisos mínims necessaris per als usuaris i monitoritzar accessos.
Absència de còpies de seguretat	La manca de còpies de seguretat pot provocar la pèrdua permanent de dades en cas d'incident.	Alt	Alt	Realitzar còpies de seguretat automàtiques i provar la seva restauració periòdicament.
Obsolescència de hardware industrial	Hardware obsolet pot no ser compatible amb noves implementacions i generar vulnerabilitats.	Alt	Alt	Planificar la renovació d'equips industrials segons el seu cicle de vida.
Fallada en els protocols de comunicació	Protocols mal implementats poden provocar errors en la transmissió de dades operatives.	Mitjà	Mitjà	Establir proves periòdiques dels protocols i mecanismes de recuperació.

1.7 Directius de Seguretat

Risc	Descripció del Risc	Impacte	Probabilitat	Accions de Mitigació
Manipulació de dades operatives	La manipulació de dades pot portar a decisions incorrectes en l'operació del sistema.	Alt	Mitjà	Aplicar sistemes de protecció i verificació de la integritat de les dades.
Denegació de servei als sistemes SCADA	Un atac DDoS pot bloquejar la supervisió i el control del sistema SCADA.	Molt Alt	Mitjà	Utilitzar sistemes anti-DDoS i limitar accessos externs al SCADA.
Compromís de credencials d'operadors	Si les credencials d'operadors són compromeses, un atacant pot accedir a la infraestructura crítica.	Alt	Mitjà	Implementar autenticació multifactor i gestió segura de credencials.
Mal funcionament de l'alimentació elèctrica	Una fallada elèctrica pot deixar inoperatius sistemes crítics sense fonts d'alimentació secundàries.	Molt Alt	Baix	Instal·lar sistemes d'alimentació ininterrompuda (SAI) i redundància energètica.
Accés físic no autoritzat a sistemes crítics	L'accés físic a sistemes pot permetre manipulacions malicioses o sabotatges.	Alt	Alt	Implementar controls físics com targetes d'accés i videovigilància.
Virus o malware en infraestructures SCADA	Malware industrial pot comprometre PLCs, SCADA i altres sistemes operacionals.	Alt	Mitjà	Utilitzar antivirus i sistemes de detecció d'intrusions específics per entorns SCADA.
Pèrdua de sincronització en sistemes distribuïts	La manca de sincronització entre sistemes distribuïts pot provocar errors en el control de processos.	Mitjà	Alt	Implementar mecanismes de sincronització horària robustos.
Mala gestió d'actualitzacions i pegats	Si els sistemes no s'actualitzen correctament, poden mantenir vulnerabilitats explotables.	Mitjà	Mitjà	Definir un pla de gestió d'actualitzacions i provar pegats abans del desplegament.
No compliment de regulacions de seguretat	No complir amb normatives de seguretat pot comportar sancions i	Alt	Baix	Auditar periòdicament el compliment de normatives

1.7 Directrius de Seguretat

Risc	Descripció del Risc	Impacte	Probabilitat	Accions de Mitigació
	augmentar els riscos operatius.			i reforçar mesures de seguretat.
Dependència excessiva de proveïdors externs	Una alta dependència de proveïdors externs pot comprometre la resiliència del sistema.	Alt	Mitjà	Diversificar proveïdors i establir plans de contingència.
Error humans en operacions crítiques	Error humans poden provocar fallades operacionals amb conseqüències crítiques.	Alt	Mitjà	Establir protocols d'operació clara i formació contínua del personal.
Fallades en sistemes de monitorització	Si els sistemes de monitorització fallen, es poden perdre alertes crítiques per seguretat.	Mitjà	Alt	Redundar sistemes de monitorització i establir alertes d'autocontrol.
Riscos en l'ús de tecnologies IoT industrials	L'ús d'IoT industrial pot introduir noves superfícies d'atac a la infraestructura SCADA.	Alt	Mitjà	Segregar IoT de les xarxes crítiques i aplicar seguretat per capes.
Interferències en les comunicacions sense fils	Interferències electromagnètiques poden afectar la fiabilitat de les comunicacions sense fils.	Mitjà	Alt	Monitoritzar interferències i utilitzar protocols de comunicació robustos.
Error en la gestió d'alarmes i esdeveniments	Una mala gestió de les alarmes pot generar saturació i dificultar la detecció d'incidents reals.	Alt	Mitjà	Optimitzar la gestió d'alarmes per evitar falsos positius i sobrecàrrega.

Taula 5-2: Avaluació de riscos

5.3. Probabilitat i impacte dels atacs cibernètics

L'anàlisi de la **probabilitat i l'impacte** dels riscos identificats en el sistema SCADA permet prioritzar les amenaces més crítiques i establir estratègies efectives de mitigació. A través d'aquesta avaluació, es poden identificar els riscos que tenen una **alta probabilitat d'ocórrer** i que, al mateix temps, poden generar un **impacte significatiu** en la disponibilitat, seguretat i operació del sistema. L'objectiu d'aquesta anàlisi és proporcionar una visió clara de la gravetat de cada risc i facilitar la presa de decisions en matèria de seguretat.

1.7 Directrius de Seguretat

L'anàlisi de probabilitat permet determinar la freqüència amb la qual un risc podria materialitzar-se. En els resultats obtinguts, s'observa que un nombre significatiu de riscos es classifiquen amb probabilitat mitjana o alta, la qual cosa indica que moltes amenaces tenen una possibilitat real d'afectar el sistema. Els riscos amb probabilitat baixa són menys freqüents, però no per això menys importants, ja que poden tenir un impacte crític si arriben a ocórrer. Aquestes dades ressalten la necessitat d'implementar controls preventius i sistemes de detecció precoç.

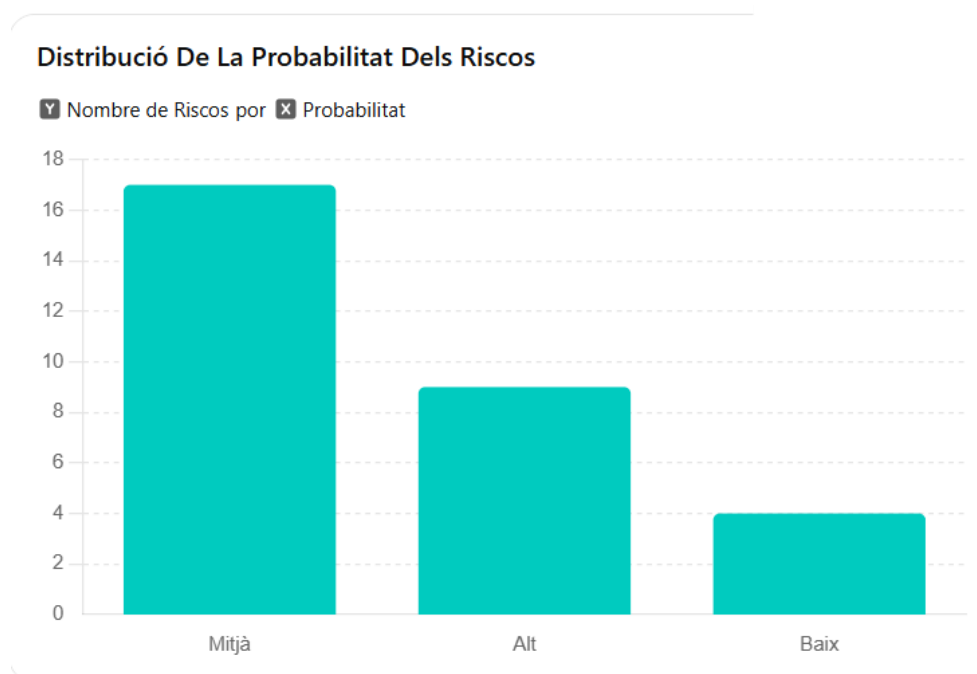


Figura 5-1: Distribució de la probabilitat dels riscos

1.7 Directrius de Seguretat

L'impacte d'un risc determina la magnitud de les conseqüències que podria tenir sobre el sistema SCADA i les seves operacions. L'anàlisi mostra que una part important dels riscos tenen un **impacte alt o molt alt**, fet que posa en evidència la necessitat de mesures de seguretat robustes per evitar interrupcions en els processos industrials i possibles afectacions a la xarxa de distribució. Els riscos amb **impacte mitjà** poden no ser tan crítics immediatament, però poden desencadenar problemes més greus si no es gestionen adequadament.

Distribució De L'Impacte Dels Riscos

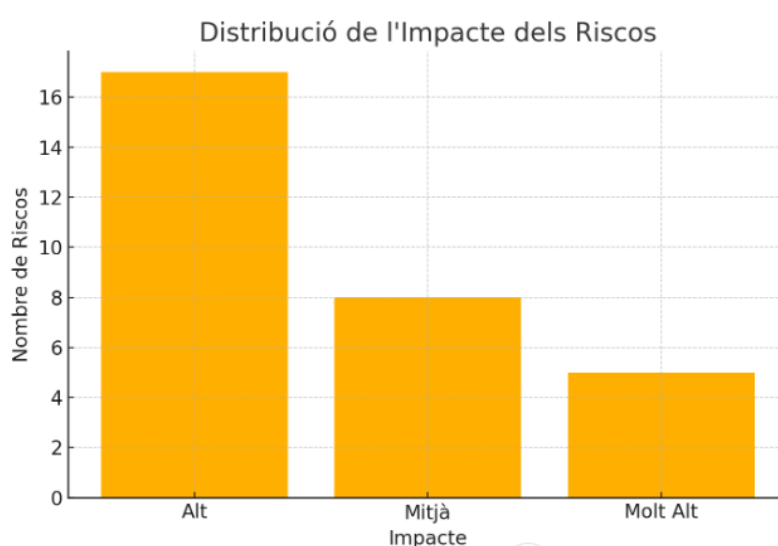


Figura 5-2: Distribució de l'impacte dels riscos

L'avaluació conjunta de **probabilitat i impacte** permet identificar els riscos que requereixen una acció prioritària. Els riscos amb **probabilitat alta i impacte molt alt** són els que representen **una major amenaça per a la seguretat i la continuïtat del servei** i, per tant, han de ser objecte d'actuacions immediates, com l'enduriment de mesures de seguretat, la implementació de sistemes de resposta ràpida i la millora dels protocols de protecció. D'altra banda, els riscos amb **probabilitat mitjana i impacte alt** també requereixen una atenció especial per evitar que evolucionin cap a incidents de gran gravetat. Aquest anàlisi permet a ATL millorar la seva estratègia de seguretat, enfocant esforços en aquelles àrees que poden generar majors vulnerabilitats en el sistema SCADA.

1.7 Directrius de Seguretat

6. ESTRATÈGIES DE PROTECCIÓ I MITIGACIÓ

6.1. Mesures preventives i bones pràctiques sistemes telecontrol

Els sistemes SCADA són fonamentals per a la gestió d'infraestructures crítiques i, per tant, són un objectiu freqüent d'atacs cibernètics. A continuació, es detallen els atacs més comuns i les mesures de protecció adequades per mitigar-ne els riscos.

6.1.1. Phishing

El phishing és un atac basat en enganys dirigits als usuaris per robar credencials d'accés o informació sensible. Els atacants envien correus electrònics fraudulents que simulen ser de fonts legítimes, amb enllaços a pàgines falsificades o fitxers maliciosos.

- Mesures de protecció:
 - Formació i conscienciació: És fonamental que els operadors i empleats rebin formació periòdica sobre com identificar intents de phishing i bones pràctiques de seguretat.
 - Filtrat de correus electrònics i missatges: Implementar sistemes de filtratge de correus per detectar i bloquejar missatges sospitosos abans que arribin als usuaris.

6.1.2. Malware, Ransomware i Spyware

Aquest tipus de programari maliciós pot infectar els sistemes SCADA, provocar el bloqueig de dades i interrompre operacions crítiques.

- Mesures de protecció:
 - Antivirus robust i actualitzat: Disposar de solucions de seguretat actualitzades per detectar i eliminar amenaces abans que afectin el sistema.
 - Control d'accés i privilegis: Aplicar polítiques d'accés restringit per evitar que usuaris no autoritzats puguin instal·lar programari maliciós o accedir a dades sensibles.

6.1.3. Denegació de Servei (DoS)

Un atac DoS consisteix a saturar un servidor SCADA amb múltiples peticions fins que es col·lapsa, impedit-ne el funcionament normal.

- Mesures de protecció:
 - Prevenció i mitigació de DoS: Utilitzar sistemes de detecció d'atacs per bloquejar peticions anòmales i evitar la saturació de la xarxa.
 - Monitoratge i alertes de rendiment: Implementar eines de supervisió en temps real per detectar i actuar ràpidament en cas d'augment sospitós de trànsit.

1.7 Directrius de Seguretat

6.1.4. Home en el Medi (MitM)

Aquest atac es produeix quan un intrús intercepta i modifica les comunicacions entre dos dispositius sense que els afectats se'n adonin.

- Mesures de protecció:
 - Xifratge de comunicacions: Assegurar que les dades enviades entre els dispositius SCADA i els PLC estan protegides mitjançant protocols segurs com TLS o VPNs.
 - Edge Computing: Implementar computació a la vora per reduir la dependència de les comunicacions externes i evitar possibles interceptacions.

6.1.5. Força Bruta

Aquest atac consisteix a provar múltiples combinacions de contrasenyes fins a trobar la correcta i obtenir accés no autoritzat als sistemes SCADA.

- Mesures de protecció:
 - Bloqueig de comptes: Configurar sistemes per bloquejar un compte després de diversos intents fallits de connexió.
 - Autenticació multifactor (MFA): Implementar un sistema d'autenticació addicional (com SMS, aplicacions d'autenticació o claus de seguretat) per evitar que una contrasenya compromesa permeti accedir al sistema.

6.1.6. Explotació de Vulnerabilitats

Els atacants poden aprofitar debilitats en el programari o el maquinari per accedir als sistemes i executar accions malicioses.

- Mesures de protecció:
 - Anàlisi del programari i vulnerabilitats: Realitzar auditories de seguretat periòdiques per identificar possibles punts febles en el sistema SCADA.
 - Aplicació de pegats i actualitzacions: Mantenir sempre actualitzat el programari per corregir possibles vulnerabilitats i evitar que siguin explotades.

1.7 Directrius de Seguretat

6.1.7. Injecció SQL

Aquest atac es basa en la inserció de codi maliciós en les consultes SQL per manipular bases de dades i accedir a informació sensible.

- Mesures de protecció:
 - Validació d'entrades de formulari: Implementar filtres per assegurar que les dades introduïdes pels usuaris no continguin codi maliciós.
 - Ús de consultes SQL predefinides i autoritzades: Configurar el sistema perquè només accepti consultes estructurades i validades, evitant la possibilitat d'executar instruccions malicioses.

6.2. PROTECCIÓ DE SISTEMES SCADA I PLCS

Els sistemes SCADA i HMI són fonamentals per al control d'infraestructures crítiques, com el subministrament d'aigua. Per tant, han de disposar de mecanismes de seguretat robustos per evitar ciberatacs i garantir la disponibilitat del servei. A continuació, es desenvolupen detalladament les mesures de seguretat amb exemples concrets relacionats amb el projecte SCADA d'ATL.

6.2.1. Configurar Usuaris, Grups i Permisos

És fonamental establir una jerarquia clara d'usuaris, grups i permisos per garantir que cada operador només tingui accés a les funcions necessàries per al seu rol. Per exemple, en el projecte SCADA d'ATL, els operadors només haurien de tenir accés a la supervisió del sistema, mentre que els tècnics d'enginyeria podrien realitzar configuracions avançades. Això evita errors operatius i minimitza l'impacte en cas de robatori de credencials.

Exemple: Un atacant que obtingui les credencials d'un operador no podria modificar la configuració de les estacions de tractament d'aigua si els permisos han estat adequadament restringits.

Aquestes referències als controls ENS correspon als punts de control OP.ACC.1, OP.ACC.2, OP.ACC.3, OP.ACC.4.

6.2.2. Utilitzar el mecanisme d'autenticació de usuaris més adequat (Digest, IdP, AD, etc.)

El sistema ha d'utilitzar mètodes d'autenticació segurs per evitar accessos no autoritzats. Per exemple, es pot implementar Active Directory (AD) perquè tots els usuaris utilitzin un inici de sessió únic i centralitzat. Això permet aplicar polítiques de contrasenyes fortes i auditories d'accés.

Exemple: Un sistema SCADA amb integració a AD podria bloquejar automàticament un compte d'usuari si detecta múltiples intents fallits d'accés, protegint-se contra atacs de força bruta.

1.7 Directrius de Seguretat

Aquest apartat respon als punts de control OP.ACC.5, OP.ACC.6, OP.ACC.7.

6.2.3. Configurar el Control d'Accés per a cada part de l'aplicació SCADA

Cada secció de l'aplicació SCADA hauria de tenir un nivell diferenciat d'accés segons les necessitats de cada usuari. Per exemple, la configuració d'alertes només hauria d'estar disponible per als administradors del sistema.

Exemple: En el cas d'ATL, la interfície SCADA podria configurar-se perquè només els tècnics autoritzats puguin modificar els llindars d'alertes de pressió i cabal, evitant errors humans o manipulacions malicioses.

Aquest apartat respon als punts de control OP.ACC.5, OP.ACC.6, OP.ACC.7.

6.2.4. Restringir l'accés a la eina d'enginyeria

Les eines d'enginyeria permeten modificar el comportament dels PLC i la infraestructura SCADA. Això significa que només el personal altament qualificat hauria de tenir-hi accés.

Exemple: Si un operador sense experiència modifica paràmetres de control a la planta de tractament d'aigua d'ATL, podria desconfigurar els nivells de tractament químic, afectant la qualitat de l'aigua distribuïda.

Aquest apartat respon als punts de control OP.ACC.3, MP.COM.4.

6.2.5. Xifrar les comunicacions amb TLS v1.2 o v1.3

El xifratge de comunicacions evita que un atacant pugui interceptar i modificar dades sensibles. TLS v1.2 o v1.3 hauria d'utilitzar-se per totes les comunicacions entre els servidors SCADA, PLC i clients externs.

Exemple: Sense TLS, un atac de Man-in-the-Middle podria modificar els valors de pressió d'una canonada d'aigua a la xarxa d'ATL, generant errors en la regulació del subministrament.

Aquest apartat respon als punts de control MP.INFO.3, MP.INFO.4, MP.COM.2, MP.COM.3.

6.2.6. Securitzar l'accés remot (clients externs)

L'accés remot hauria d'estar restringit a VPNs segures amb autenticació multifactor (MFA). Només el personal autoritzat hauria de poder accedir-hi des de fora de la xarxa corporativa.

Exemple: Un tècnic d'ATL que treballa des de fora hauria d'utilitzar una VPN amb MFA per accedir al sistema SCADA, evitant que actors no autoritzats puguin connectar-s'hi des d'internet.

1.7 Directrius de Seguretat

6.2.7. Protegir les comunicacions que no es puguin xifrar (Edge Computing)

Quan el xifratge no és viable per limitacions tecnològiques, es poden processar les dades en local abans d'enviar-les a la xarxa (Edge Computing). Això redueix la quantitat de dades exposades.

Exemple: A les estacions remotes d'ATL, es poden realitzar càlculs locals per evitar que dades crítiques viatgin per xarxes públiques sense protecció.

6.2.8. Protegir els directoris del SCADA en el sistema operatiu, així com l'accés al servidor

Els arxius i directoris essencials del SCADA han d'estar protegits amb permisos estrictes i accessos restringits.

Exemple: Un atacant que obtingui accés a un servidor de l'ATL no hauria de poder modificar fitxers crítics del SCADA si aquests estan protegits amb permisos d'escriptura només per a administradors.

6.2.9. Restricció de ports en el Firewall

Només els ports essencials han de romandre oberts per reduir la superfície d'atac del sistema.

Exemple: Si un servidor SCADA d'ATL només necessita els ports 502 (Modbus TCP) i 443 (HTTPS), tots els altres ports han de ser bloquejats al firewall per evitar accessos no desitjats.

Aquest apartat respon als punts de control MP.COM.1, MP.COM.4.

6.2.10. Gestió centralitzada dels actius

Un sistema de gestió centralitzada permet tenir un inventari actualitzat de tots els dispositius, sistemes i aplicacions de la infraestructura SCADA. Això facilita la identificació de dispositius obsolets, vulnerabilitats i components crítics que requereixen mesures de seguretat específiques.

Exemple: Un sistema de gestió d'actius a ATL podria alertar els responsables de seguretat quan un dispositiu connectat a la xarxa SCADA no ha rebut actualitzacions durant un període determinat, facilitant-ne la supervisió i la seva posterior actualització o substitució.

6.2.11. Detecció de vulnerabilitats

L'anàlisi contínua de vulnerabilitats en el sistema SCADA permet identificar i mitigar possibles riscos abans que siguin explotats per atacants. Això inclou l'ús d'eines automatitzades per escanejar vulnerabilitats en sistemes operatius, aplicacions, PLC i dispositius de xarxa.

1.7 Directrius de Seguretat

Exemple: Si es detecta que un servidor SCADA d'ATL utilitza una versió antiga d'Apache amb una vulnerabilitat crítica, es podria aplicar un pegat de seguretat immediatament per evitar possibles intrusions.

Aquest apartat respon als punts de control OP.ExP.6, OP.EXP.3, OP.EXP.4.

6.2.12. Tenir un pla de recuperació (redundància, snapshots, backups en directoris segurs...)

El sistema ha de comptar amb còpies de seguretat freqüents i mecanismes de redundància per garantir la continuïtat del servei en cas de fallada o atac.

Exemple: Si el servidor SCADA principal d'ATL es veu compromès per un atac de ransomware, un sistema de snapshots i backups permetria restaurar-lo sense pèrdua de dades crítiques.

Aquest apartat respon als punts de control OP.CONT.2, MP.INFO.9.

6.2.13. Mantenir el programari actualitzat

Les actualitzacions periòdiques del programari SCADA i dels sistemes operatius corregeixen vulnerabilitats i milloren la seguretat.

Exemple: Un SCADA d'ATL que no s'actualitza podria ser vulnerable a exploits coneguts. Aplicar pegats de seguretat redueix aquests riscos i millora la protecció contra atacs.

6.2.14. Implantació d'un sistema SIEM + SOC per a detecció i resposta 24x7

Per garantir una vigilància constant de la seguretat del sistema SCADA i HMI, és essencial la implementació d'un SIEM (Security Information and Event Management) combinat amb un SOC (Security Operations Center). Aquest sistema recopila, analitza i correlaciona esdeveniments de seguretat en temps real, permetent detectar activitats sospitoses i respondre immediatament a possibles incidents cibernètics.

Exemple: En el sistema SCADA d'ATL, un SIEM podria detectar múltiples intents fallits d'accés a una estació remota i alertar el SOC per iniciar una investigació. Això podria evitar un atac de força bruta que intenti comprometre el sistema.

6.2.15. Control centralitzat de les versions instal·lades en els equips PLC

La diversitat de versions de firmware en els PLC pot generar problemes de compatibilitat i deixar vulnerabilitats sense corregir. Per aquest motiu, és fonamental tenir un sistema centralitzat que monitoritzi i controli les versions del firmware i del programari dels equips PLC, assegurant que sempre estiguin actualitzats i alineats amb els requisits de seguretat.

1.7 Directrius de Seguretat

Exemple: En el projecte SCADA d'ATL, si es detecta que un PLC funciona amb una versió obsoleta del firmware amb vulnerabilitats conegudes, el sistema de control centralitzat pot alertar els tècnics perquè planifiquin una actualització sense afectar l'operació del servei d'aigua.

6.2.16. Realització de pentesting específics de la xarxa d'operacions cada dos anys

Les proves de penetració (pentesting) són simulacions d'atacs cibernètics controlats que permeten avaluar la seguretat de la xarxa d'operacions i identificar possibles punts febles. Realitzar aquestes proves cada dos anys assegura que la infraestructura SCADA estigui preparada per fer front a les amenaces emergents.

Exemple: En un pentest realitzat al sistema SCADA d'ATL, els auditors podrien detectar que certes credencials d'accés es transmeten sense xifrar, proposant la implementació de TLS per millorar la seguretat de les comunicacions.

Aquestes referències als controls ENS correspon als punts de control MP.PER.3, MP.SW.2

6.2.17. Segmentació de la xarxa

La segmentació de la xarxa és una estratègia essencial per limitar l'impacte d'un atac cibernètic. Separar la xarxa d'operacions (OT) de la xarxa corporativa (IT) impedeix que una infecció en la xarxa administrativa afecti els sistemes crítics del SCADA. A més, s'han d'implementar VLANs i zones de seguretat diferenciades dins de la xarxa OT per aïllar diferents components.

Exemple: Si un atacant aconsegueix accedir a la xarxa administrativa d'ATL mitjançant phishing, la segmentació de la xarxa impediria que aquest moviment lateral afectés els PLC o les estacions de telecontrol, evitant així la interrupció del servei.

6.2.18. Control dels dispositius de memòria portàtils

Els dispositius USB i altres suports de memòria portàtil poden ser un vector d'atac important, ja que poden introduir malware en el sistema SCADA si no es controlen adequadament. És fonamental establir polítiques estrictes que restringeixin l'ús de dispositius USB no autoritzats i implementar solucions de seguretat que analitzin aquests suports abans que es connectin als sistemes.

Exemple: Si un tècnic d'ATL necessita utilitzar un USB per actualitzar el firmware d'un PLC, aquest hauria de passar per un escàner de seguretat específic abans de ser connectat al sistema, evitant així possibles infeccions per malware.

Seguidament s'incorpora una taula amb les mesures de protecció als riscos detectats :

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
Fallada de PLC	Implementació de PLCs redundants, plans de manteniment preventiu i simulacions de fallades per validar resiliència.	Monitoritzar l'estat dels PLCs, aplicar actualitzacions només després de proves rigoroses i establir polítiques de canvi controlades.	Realitzar inspeccions periòdiques als PLCs, establir un pla de manteniment i validar redundància en proves operatives.
Obsolescència de SCADA	Planificació de la renovació del sistema SCADA, actualitzacions regulars i compatibilitat amb sistemes moderns.	Realitzar auditories de compatibilitat de SCADA amb nous components, assegurar la interoperabilitat i documentar modificacions.	Actualitzar el sistema SCADA seguint un pla gradual, verificar compatibilitat i assegurar suport tècnic continuat.
Intrusió en comunicacions	Ús de protocols segurs com TLS i VPN, segmentació de xarxes i implementació de sistemes d'autenticació robustos.	Utilitzar solucions de seguretat per a tràfic xifrat, inspecció de comunicacions en temps real i monitorització d'accessos no autoritzats.	Configurar VPN per a connexions remotes, aplicar polítiques de xifratge i monitoritzar tràfic de xarxa en temps real.
Pèrdua de dades d'instrumentació	Instal·lació de sensors redundants, verificació periòdica de dades i implementació d'alarmes per anomalies.	Implementar mecanismes de detecció de valors anòmals en sensors, registre d'històrics i alarmes predictives per fallades imminents.	Instal·lar sistemes de validació de dades en sensors, realitzar manteniment predictiu i proves d'integritat de dades.
Ciberatac a centres de control	Segmentació de xarxa, ús de sistemes de detecció d'intrusions,	Auditar els registres de xarxa periòdicament, establir alertes per intents d'intrusió i segmentar zones crítiques.	Implementar firewalls industrials, auditories d'accessos i monitoratge d'amenaces en temps real a la xarxa SCADA.

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
	autenticació multifactor i restricció d'accessos.		
Fallada d'estacions remotes	Implementació de sistemes de redundància en estacions remotes, manteniment proactiu i establiment de canals alternatius.	Definir procediments clars per a la resposta ràpida davant d'una fallada remota, garantir redundància de connexions i proveïdors.	Configurar sistemes de redundància per estacions remotes i establir protocols d'actuació en cas de fallada.
Atac a dispositius HMI	Restricció d'accés a HMI, aplicació de polítiques de seguretat, monitorització constant i bloqueig de connexions sospitoses.	Aplicar polítiques d'accés basades en rols, utilitzar registres detallats d'auditoria i establir temps màxims de sessió.	Definir polítiques estrictes d'accés a HMI, registrar logs d'activitat i aplicar mecanismes d'autenticació robusta.
Falta de redundància en xarxa	Desplegament d'una infraestructura de xarxa redundada, ús de protocols de failover i monitorització en temps real.	Realitzar simulacions de fallades de xarxa, aplicar proves de resistència i validar protocols de recuperació en condicions adverses.	Reconfigurar l'arquitectura de xarxa per incloure redundància, provar failover i validar mecanismes de recuperació.
Desconfiguració de PLCs	Definició de polítiques estrictes de gestió de versions, autenticació robusta i control d'accés segmentat.	Estandarditzar la documentació de configuració de PLCs, gestionar versions i assegurar còpies segures en repositoris segregats.	Documentar i aplicar polítiques de gestió de versions per PLCs, establir control d'accés basat en rols i auditories.

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
Pèrdua de dades històriques	Realització de còpies de seguretat periòdiques, emmagatzematge segur, proves de restauració i versions distribuïdes.	Verificar que les còpies de seguretat es poden restaurar correctament, realitzar proves en entorns sandbox i validar integritat.	Realitzar còpies de seguretat automàtiques, verificar integritat i fer proves de restauració en entorns de simulació.
Error de programació en PLC	Formació d'enginyers en programació segura, validació de codi abans del desplegament i revisió periòdica d'algoritmes.	Adoptar metodologies de desenvolupament segur, definir estàndards d'estil per codi i establir processos d'auditoria de software.	Desenvolupar estàndards de programació segura per PLCs i validar el codi abans de desplegar-lo en producció.
Mala configuració de permisos d'usuari	Aplicació del principi de mínims privilegis en la configuració d'usuaris, monitorització d'accessos i alertes de seguretat.	Configurar i revisar periòdicament els permisos d'accés assignats als operadors, evitar credencials compartides i autenticar dispositius.	Revisar permisos d'usuaris periòdicament, aplicar polítiques de bloqueig automàtic i monitoritzar accessos inusuals.
Absència de còpies de seguretat	Implementació d'un sistema de còpies de seguretat automatitzat, distribució en múltiples ubicacions i xifratge de dades.	Provar les còpies de seguretat en entorns de test abans de qualsevol restauració i validar que no s'hagi corromput la informació.	Establir una política de còpies de seguretat en múltiples ubicacions, amb verificacions periòdiques de restauració.

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
Obsolescència de hardware industrial	Planificació de la renovació de maquinari industrial, auditories periòdiques i assegurament de compatibilitat amb SCADA.	Documentar els cicles de vida dels equips, definir estratègies de substitució i garantir compatibilitat entre generacions de hardware.	Realitzar auditories de hardware, planificar la renovació d'equips i definir estratègies d'integració amb SCADA.
Fallada en els protocols de comunicació	Monitoratge actiu dels protocols de comunicació, detecció d'anomalies i verificació d'integritat en transmissions de dades.	Implementar sistemes de redundància en canals de comunicació crítics, definir mecanismes d'error-corrector i protocols d'emergència.	Monitoritzar trànsit de xarxa per detectar anomalies, validar integritat de dades i implementar sistemes de resposta.
Manipulació de dades operatives	Ús de firmes digitals, verificació contínua de la integritat de dades i registre detallat de totes les transaccions crítiques.	Utilitzar registres digitals per auditar qualsevol canvi en els fitxers de dades operatives i aplicar mecanismes de verificació contínua.	Aplicar sistemes de verificació d'integritat a les bases de dades SCADA i establir alertes davant canvis inesperats.
Denegació de servei als sistemes SCADA	Implementació de mecanismes de mitigació de DDoS, ús de proxies reversos i segmentació d'accés a SCADA des de l'exterior.	Realitzar proves periòdiques de resistència davant atacs de denegació de servei, establir mecanismes d'absorció de càrrega.	Configurar mecanismes de protecció contra atacs DDoS i establir límits de connexió en dispositius externs.

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
Compromís de credencials d'operadors	Aplicació de gestió segura de credencials, polítiques de rotació automàtica i autenticació multifactor obligatòria.	Encriptar les credencials d'accés, utilitzar eines de gestió segura de contrasenyes i restringir sessions simultànies.	Aplicar gestió centralitzada de credencials, habilitar autenticació multifactor i registrar accessos sospitosos.
Mal funcionament de l'alimentació elèctrica	Ús de fonts d'alimentació ininterrompuda (SAI), sistemes de backup energètic i simulacions de tall de subministrament.	Revisar l'estat dels SAI, realitzar proves de càrrega i substituir bateries abans que arribin al final de la seva vida útil.	Verificar el correcte funcionament dels SAI, establir proves de càrrega i programar manteniment preventiu.
Accés físic no autoritzat a sistemes crítics	Control d'accés físic amb sistemes de videovigilància, sensors de presència, identificació biomètrica i protocols de registre.	Restringir l'accés físic només al personal autoritzat, realitzar auditories periòdiques i establir controls de presència.	Implementar sistemes de videovigilància, controlar l'accés físic amb targetes i establir protocols de seguretat.
Virus o malware en infraestructures SCADA	Utilització de sistemes de detecció i resposta contra malware industrials, llistes blanques d'aplicacions i SIEM dedicat.	Aplicar controls d'integritat i llistes blanques per evitar execució de codi maliciós en sistemes industrials.	Configurar sistemes antivirus específics per SCADA, auditar trànsit de xarxa i utilitzar llistes blanques d'aplicacions.
Pèrdua de sincronització	Mecanismes de sincronització robustos per	Mantenir sincronització amb servidors horaris fiables, establir mecanismes de control	Definir mecanismes de sincronització amb NTP segur,

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
en sistemes distribuïts	garantir coherència en sistemes distribuïts i redundància en NTP externs.	i validar regularment la coherència horària.	monitoritzar desajustos horaris i validar registres temporals.
Mala gestió d'actualitzacions i pegats	Desplegament d'un pla d'actualitzacions, proves de pegats abans de la seva aplicació i control d'impacte en entorns productius.	Aplicar criteris d'anàlisi de riscos abans de cada actualització, validar compatibilitat i establir processos d'homologació.	Aplicar un sistema d'actualitzacions controlades, provar pegats abans del desplegament i mantenir documentació tècnica.
No compliment de regulacions de seguretat	Auditories regulars per verificar el compliment normatiu, adaptació a noves regulacions i implementació de millores contínues.	Documentar tots els canvis realitzats en el sistema, establir protocols de signatura digital i auditar-ne el compliment.	Realitzar auditories anuals de compliment normatiu i establir protocols d'adaptació a noves regulacions.
Dependència excessiva de proveïdors externs	Diversificació de proveïdors, establiment de contractes amb garanties de suport i definició de protocols de contingència.	Establir acords amb proveïdors per garantir continuïtat del servei, definir SLA clars i mecanismes de resposta immediata.	Diversificar proveïdors per evitar dependències crítiques, establir acords de nivell de servei (SLA) i plans de contingència.
Error humans en operacions crítiques	Formació contínua dels operadors en seguretat, capacitat en resposta a incidents i	Fer ús de simulacions d'errors humans, establir protocols de resposta i documentar errors per evitar la seva repetició.	Capacitar el personal en protocols de seguretat, establir simulacions de resposta a incidents i actualitzar documentació.

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
	avaluació d'habilitats mitjançant simulacions.		
Fallades en sistemes de monitorització	Implementació de sistemes de monitoratge redundant, alertes en temps real i registres per detecció d'anomalies operacionals.	Configurar alertes automàtiques per detectar anomalies en sistemes de monitorització, establir límits operatius i alertes personalitzades.	Configurar sistemes de monitorització doble, establir alertes en temps real i definir procediments d'escalat d'incidents.
Riscos en l'ús de tecnologies IoT industrials	Aïllament de dispositius IoT de les xarxes crítiques, segmentació de comunicacions i aplicació de control d'accés rigorós.	Crear entorns de proves per validar seguretat d'IoT abans de la seva integració i establir polítiques de revisió contínua.	Aïllar dispositius IoT del sistema SCADA principal, aplicar autenticació forta i monitoritzar connexions en temps real.
Interferències en les comunicacions sense fils	Protecció de comunicacions sense fils mitjançant xifrat robust, monitorització d'interferències i ús de canals protegits.	Monitoritzar en temps real possibles interferències en comunicacions i utilitzar tècniques de mitigació de soroll electromagnètic.	Xifrar comunicacions sense fils, utilitzar canals protegits i monitoritzar interferències electromagnètiques.
Errors en la gestió d'alarmes i esdeveniments	Gestió eficient de les alarmes per evitar saturació d'esdeveniments, classificació de	Configurar sistemes d'alerta intel·ligents per prioritzar alarmes crítiques, eliminar falsos positius i evitar saturació d'informació.	Millorar la classificació d'alarmes, implementar filtres intel·ligents i prioritzar alertes crítiques en sistemes de resposta.

1.7 Directrius de Seguretat

Risc	Mesures de prevenció	Bones pràctiques	Descripció dels treballs a realitzar
	prioritats i correlació d'alertes.		

Taula 6-1: Mesures de protecció als riscos detectats.

6.3. Arquitectura de xarxa

L'arquitectura de seguretat basada en el model Purdue és un enfocament estàndard en la protecció de sistemes industrials i infraestructures crítiques, com el sistema SCADA d'ATL. Aquest model defineix una segmentació jeràrquica de la xarxa en diversos nivells, facilitant la compartimentació del trànsit de dades, l'aïllament de segments crítics i l'aplicació de polítiques de seguretat rigoroses.

Mitjançant l'aplicació del model Purdue, es millora la protecció contra ciberamenaces, es limita la superfície d'atac i es garanteix la integritat i disponibilitat dels processos industrials. A continuació, es detallen els nivells de l'arquitectura Purdue i els seus components.

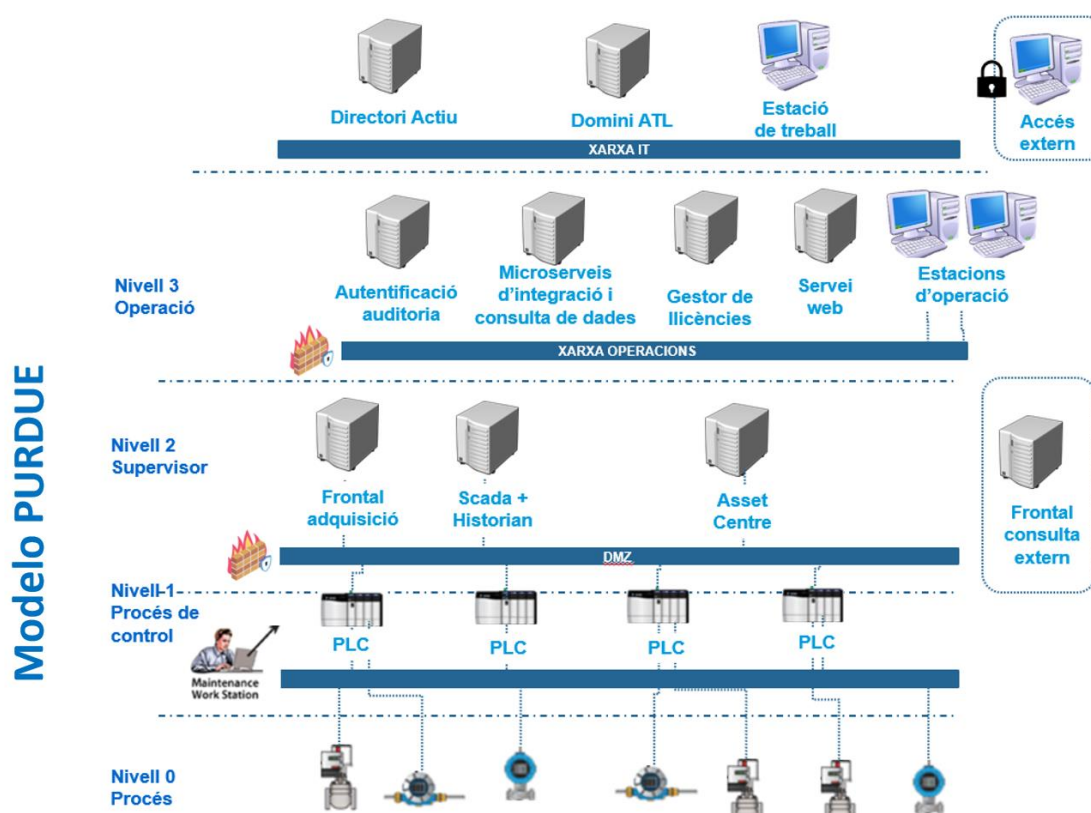


Figura 6-1: Arquitectura Purdue

1.7 Directrius de Seguretat

El model Purdue segmenta la xarxa industrial en sis nivells principals, cadascun dels quals té funcions específiques i requisits de seguretat diferenciats. Aquesta segmentació permet restringir el trànsit entre nivells, assegurar la protecció dels sistemes crítics i reduir la probabilitat d'accés no autoritzat o propagació d'amenaçes.

6.4. Nivell 0 – Dispositius físics i sensors

Aquest nivell inclou sensòrica, actuadors i dispositius físics encarregats de mesurar i controlar variables del procés industrial. Exemples d'aquests dispositius són els transmissors de cabal, pressió, temperatura i vàlvules de control. La seva protecció es basa en evitar accessos físics no autoritzats i garantir la seva operació contínua.

6.5. Nivell 1 – Controladors i PLCs

En aquest nivell es troben els PLC (Programmable Logic Controllers) i altres dispositius de control industrial que gestionen la informació recollida pels sensors i actuen sobre els processos productius. Aquests sistemes han d'estar protegits contra manipulacions no autoritzades, errors de configuració i vulnerabilitats en la seva programació.

6.6. Nivell 2 – Sistemes HMI i SCADA locals

Aquest nivell inclou les HMI (Human-Machine Interfaces) i els SCADA locals, que permeten als operadors monitoritzar i controlar els processos en temps real. Per protegir aquests sistemes, es recomana restricció d'accessos, autenticació forta i monitoratge de sessions d'usuari.

6.7. Nivell 3 – Xarxa d'operacions (OT)

Aquest nivell connecta els sistemes SCADA amb altres dispositius de control i comunicació. Aquí s'integren serveis d'històrics, gestió d'alarmes i supervisió d'estats. La protecció d'aquest nivell es basa en segmentació de xarxa, ús de VLANs i firewalls industrials per evitar comunicacions innecessàries.

6.8. Nivell 3.5 – DMZ Industrial

Aquest és un nivell intermedi que serveix de barrera entre les xarxes operacionals (OT) i la xarxa corporativa (IT). La DMZ (Zona Desmilitaritzada) permet establir passarel·les segures, proxies i servidors d'accés controlat per intercanviar informació de manera segura.

1.7 Directrius de Seguretat

6.9. Nivell 4 – Xarxa corporativa (IT)

Aquí es troben els sistemes de gestió empresarial, com ERP, gestió de recursos i aplicacions d'anàlisi de dades. Per garantir la seguretat, és fonamental limitar la interconnexió amb la xarxa OT, aplicant polítiques d'accés estrictes i control de trànsit.

6.10. Nivell 5 – Nivell de Nube i Serveis Externs

Aquest nivell inclou servidors al núvol, aplicacions de monitoratge remot i serveis de tercers. Per garantir-ne la seguretat, s'han d'implementar VPN segures, xifratge de comunicacions i mecanismes d'autenticació robusta.

6.11. Definició dels components principals

- PLC (Programmable Logic Controller): Dispositiu programable encarregat de l'automatització de processos industrials. La seva seguretat es basa en la configuració adequada dels permisos i l'ús d'autenticació per accedir-hi.
- SCADA (Supervisory Control and Data Acquisition): Sistema que supervisa i controla processos industrials mitjançant la recollida de dades en temps real. La seva protecció inclou segmentació de xarxa i polítiques estrictes d'accés.
- HMI (Human-Machine Interface): Interfícies que permeten la interacció entre operadors i processos industrials. La seguretat es basa en autenticació multifactor i restriccions d'accés.
- Històrics i bases de dades OT: Sistemes encarregats d'emmagatzemar dades operacionals i registres de processos. Han de comptar amb sistemes de còpies de seguretat i control d'integritat per evitar manipulacions.
- DMZ Industrial: Espai intermedi que separa xarxes OT i IT per garantir que les comunicacions es realitzen de manera segura, mitjançant firewalls, proxies i mecanismes de segmentació.
- Firewalls i IDS/IPS: Dispositius de seguretat encarregats de monitoritzar el trànsit de xarxa i bloquejar possibles intrusions. És essencial configurar polítiques de filtratge per aïllar segments de xarxa OT.
- Servidors de gestió empresarial (ERP, MES): Sistemes ubicats a la xarxa corporativa que gestionen recursos, planificació i producció. S'ha de limitar el seu accés a la xarxa OT per evitar riscos.
- Connexions remotes i VPN: Accés extern a la xarxa SCADA, utilitzat per proveïdors o personal tècnic. Ha de ser protegit mitjançant xifratge robust, autenticació multifactor i registre d'activitats.

1.7 Directrius de Seguretat

7. CONCLUSIONS I RECOMANACIONS FINALS

L'anàlisi de seguretat del Sistema d'Automatització i Telecomandament (SATEL) de l'Ens d'Abastament d'Aigües Ter-Llobregat (ATL) ha permès identificar una sèrie de vulnerabilitats crítiques i riscos que podrien comprometre la disponibilitat, integritat i confidencialitat dels processos de control i distribució d'aigua. El sistema SCADA i la seva infraestructura associada han evolucionat cap a una arquitectura avançada, però encara presenta mancances en aspectes com la segmentació de xarxes, l'autenticació d'usuaris, la monitorització d'incidents i la gestió de riscos.

Les principals troballes d'aquesta anàlisi indiquen que:

- El sistema actual necessita millores en seguretat de comunicacions, especialment en l'aplicació de protocols de xifratge robustos i la segmentació adequada de xarxes OT i IT per evitar la propagació d'atacs laterals.
- Els mecanismes d'autenticació i control d'accés han de ser reforçats per evitar accessos no autoritzats a dispositius crítics com PLCs, SCADA i sistemes d'operació remots.
- Hi ha una falta de redundància en components clau del sistema, cosa que podria comprometre la disponibilitat del servei en cas de fallada d'infraestructura o ciberatac.
- L'actual capacitat de detecció i resposta a incidents és limitada, ja que el sistema no disposa d'un SIEM (Security Information and Event Management) ni d'un centre SOC (Security Operations Center) 24/7 per monitoritzar amenaces en temps real.
- La gestió de riscos i actualitzacions no està plenament integrada en els processos operatius, fet que augmenta l'exposició a vulnerabilitats conegudes.

Aquestes conclusions evidencien la necessitat de reforçar la seguretat del sistema d'ATL, adoptant un enfocament proactiu i adaptatiu per protegir la infraestructura crítica contra amenaces cibernètiques.

7.1. Recomanacions

Per garantir la seguretat i la resiliència del sistema SCADA d'ATL, és essencial adoptar un enfocament proactiu en la protecció dels seus actius crítics. L'anàlisi de riscos i les vulnerabilitats detectades han posat en evidència la necessitat de reforçar diversos àmbits de seguretat, incloent la segmentació de xarxes, la gestió d'accés, la protecció de comunicacions, la detecció i resposta a incidents i la formació del personal. Les següents recomanacions de millora tenen com a objectiu establir un full de ruta estratègic per elevar el nivell de ciberseguretat de la infraestructura i garantir la continuïtat de les operacions davant possibles amenaces, es recomana implementar les següents accions:

1. Implementació d'una segmentació avançada de xarxes.

1.7 Directrius de Seguretat

- Separar clarament les xarxes IT i OT mitjançant l'ús de DMZ industrials i firewalls específics.
 - Aplicar controls de filtratge i monitorització de tràfic per evitar accessos no autoritzats entre diferents nivells de l'arquitectura Purdue.
2. Reforç de l'autenticació i control d'accés
- Aplicar autenticació multifactor (MFA) per als usuaris amb accés a sistemes SCADA i PLCs.
 - Centralitzar la gestió d'identitats mitjançant Active Directory (AD) o Identity Providers (IdP).
 - Revisar i aplicar la política de principi de mínim privilegi, evitant accessos innecessaris a sistemes crítics.
3. Millora en la gestió d'actualitzacions i pegats de seguretat
- Establir un pla de gestió d'actualitzacions per PLCs, SCADA i servidors, garantint que totes les vulnerabilitats conegudes siguin corregides a temps.
 - Implementar entorns de proves per validar nous pegats abans del desplegament en producció.
4. Capacitat de detecció i resposta a incidents
- Implantació d'un SIEM + SOC 24/7 per monitoritzar i correlacionar esdeveniments de seguretat en temps real.
 - Definició i documentació de procediments d'actuació en cas d'incident cibernètic per garantir una resposta ràpida i efectiva.
5. Protecció de comunicacions i dades
- Xifrar totes les comunicacions sensibles entre PLCs, SCADA i servidors mitjançant protocols segurs com TLS 1.2 o superior.
 - Implementar firewalls industrials, sistemes de detecció i prevenció d'intrusions (IDS/IPS) per evitar atacs en la xarxa OT.
 - Aplicar polítiques de gestió de logs i monitorització de trànsit per detectar activitats sospitoses.
6. Garantia de la disponibilitat i redundància del sistema
- Implementar sistemes de redundància geogràfica per assegurar la continuïtat del servei en cas de fallada.

1.7 Directrius de Seguretat

- Millorar la capacitat de recuperació amb còpies de seguretat automatitzades i plans de restauració verificats periòdicament.
7. Auditories periòdiques i proves de penetració
- Realitzar auditories de seguretat anuals per avaluar l'estat dels sistemes i la seva conformitat amb les normatives.
 - Dur a terme tests d'intrusió (pentesting) en la xarxa OT cada dos anys per detectar possibles vulnerabilitats explotables.
8. Formació i conscienciació del personal
- Establir programes de formació contínua en ciberseguretat per als operadors i tècnics de manteniment.
 - Simulacions periòdiques d'atacs de phishing, malware i resposta a incidents per millorar la preparació del personal.
9. Compliment normatiu i alineació amb estàndards internacionals
- Assegurar que el sistema SCADA compleixi amb els requisits de l'Esquema Nacional de Seguretat (ENS), la Directiva NIS2 i l'estàndard IEC 62443.
 - Establir auditories externes de conformitat per verificar l'aplicació de les polítiques de seguretat.

1.7 Directrius de Seguretat

ANNEX 1. COORDINACIÓ D'APLICABILITAT DE LES MESURES DE SEGURETAT DE L'ENS.

Coordinació de aplicabilitat de les mesures de seguretat del ENS						
Mesures de Seguretat punts control	Categoria	Responsabilitat		Accions necessàries pel proveïdor	Accions necessàries pel client ATL	Notes de implantació
		Proveïdor	Client			
org.1 Política de Seguretat	TOTES	50%	50%	<p>El proveïdor disposa d'una política de seguretat accessible per al client, per exemple, a l'URL: https://www.proveedor.es/politica-de-seguridad, o se us ha donat a conèixer per un altre mitjà.</p>	<p>Hi haurà una política de seguretat aprovada per l'òrgan superior que incorporarà les xarxes d'operació.</p> <ul style="list-style-type: none"> - [org.1.1] Els objectius o la missió de l'organització. - [org.1.2] El marc legal i regulatori en què es desenvoluparan les activitats. - [org.1.3] Els rols o funcions de seguretat, definint per a cadascun els deures i les responsabilitats del càrrec, així com el procediment per a la seva designació i renovació. - [org.1.4] L'estructura del comitè o els comitès per a la gestió i la coordinació de la seguretat, detallant-ne l'àmbit de responsabilitat, les persones integrants i la relació amb altres elements de l'organització. - [org.1.5] Les directrius per a l'estructuració de la documentació de seguretat del sistema, la gestió i l'accés. 	La Política de Seguretat del Proveïdor és necessària només fins que el sistema s'implanta a la infraestructura del client. A partir d'aquell moment, l'única Política de Seguretat és la del client.
org.2 Normativa de Seguretat	TOTES	50%	50%	<p>A la Normativa Interna d'ús de mitjans electrònics a l'organització, s'inclouran capítols o epígrafs específics destinats a sistemes concrets. En aquest apartat, s'hi inclourà la documentació necessària per a la implantació i l'ús correcte de la solució per complir l'ENS.</p> <p>Els usuaris de la solució implantada disposen, per exemple, d'un manual d'usuari, panells d'ajuda, avisos desplegable, banners o missatges emergents, amb normes d'ús que denoten les responsabilitats.</p>	<p>Es disposarà de normativa documentada relacionada amb l'ús correcte i amb la inadequada dels actius, juntament amb les seves responsabilitats, drets, deures i mesures disciplinàries.</p> <ul style="list-style-type: none"> - [org.2.1] L'ús correcte d'equips, serveis i instal·lacions, així com allò que es considerarà ús indegut. - [org.2.2] La responsabilitat del personal pel que fa al compliment o la violació de la normativa: drets, deures i mesures disciplinàries d'acord amb la legislació vigent. 	Els usuaris han de conèixer les funcions de la solució implantada i, si escau, n'acceptaran les condicions d'ús.

1.7 Directrius de Seguretat

org.3 Procediments de seguretat	TOTES	50%	50%	Es troben documentades les accions necessàries per a la instal·lació segura de la solució, els procediments d'administració, així com instruccions i protocols d'ús segur de la solució per part dels usuaris.	S'adequaran/complementaran els procediments de seguretat de tot el sistema d'informació perquè contemplin la solució implantada. – [org.3.1] Com dur a terme les tasques habituals. – [org.3.2] Qui ha de fer cada tasca. – [org.3.3] Com identificar i reportar comportaments anòmals. – [org.3.4.] La manera com s'ha de tractar la informació en consideració al nivell de seguretat que requereix.	
org.4 Procediments de autorització	TOTES	50%	50%	Es troba documentat el procés d'autoritzacions, corresponent tant a administradors com a usuaris, ja sigui a l'entorn d'instal·lació (Guia d'instal·lació), com a l'entorn d'operació (Guia d'ús segur/manual d'usuari).	Hi haurà un procés d'autoritzacions adequat a tot el sistema d'informació, que inclogui la solució implantada. – [org.4.1] Utilització d'instal·lacions, habituals i alternatives. – [org.4.2] Entrada d'equips en producció, en particular equips que involucrin criptografia. – [org.4.3] Entrada d'aplicacions a producció. – [org.4.4] Establiment d'enllaços de comunicacions amb altres sistemes. – [org.4.5] Utilització de mitjans de comunicació, habituals i alternatius. – [org.4.6] Utilització de suports d'informació. – [org.4.7] Utilització d'equips mòbils. S'entendrà per equips mòbils ordinadors portàtils, tauletes, telèfons mòbils o altres de naturalesa anàloga. – [org.4.8] Utilització de serveis de tercers, sota contracte o conveni, concessió, encàrrec, etc.	

op.pl.1 Anàlisi de riscos	B	M	A	Sí	Sí	El proveïdor disposa d'una gestió pròpia de riscos en què ha considerat els processos de desenvolupament, implantació, manteniment i suport de la solució. A la Guia d'instal·lació segura que es facilita al client, el proveïdor inclou una anàlisi de riscos respecte a la solució que proveeix.	L'organització client inclourà la solució implantada com a actiu. L'organització client disposarà d'una Anàlisi de Riscos en què inclourà els riscos. S'incorporaran els riscos identificats pel proveïdor a la Guia d'instal·lació de la solució a la gestió de riscos global de l'organització client. – [op.pl.1.1] Identifiqueu els actius més valuosos del sistema. – [op.pl.1.2] Identifiqueu les amenaces més probables. – [op.pl.1.3] Identifiqueu les salvaguardes que protegeixen d'aquestes amenaces. – [op.pl.1.4] Identifiqueu els principals riscos residuals.	Cal tenir l'anàlisi de riscos actualitzat.
-------------------------------------	----------	----------	----------	----	----	--	--	--

1.7 Directius de Seguretat

op.pl.2 Arquitectura de seguretat	B	M	A	50 %	Es disposa d'un mapa esquemàtic o diagrama amb l'arquitectura de la solució que es facilita a la Guia d'instal·lació de la solució. Es contempla tant a nivell de blocs d'estructuració dels mòduls programari de la solució, com a nivell d'arquitectura recomanada per implementar-la (Balancejadors, servidors web, servidors de BBDD, etc.) i integrar-la a la xarxa del client. S'inclouen diagrames amb indicació de les connexions i interconnexions (fluxos de dades) cap a altres sistemes i cap a l'exterior, amb indicació de com s'han protegit, o poden protegir-se, incloent-hi els protocols d'accés emprats. Es documentaran a la Guia d'instal·lació les recomanacions de configuració i parametrització per mantenir un nivell adequat de seguretat.	L'organització client disposarà de documentació de les instal·lacions, del sistema, d'accessos al sistema, de la(s) xarxa(es), de les línies de defensa... de manera que es faciliti la integració de la solució contractada. <ul style="list-style-type: none"> - [op.pl.2.1] Documentació de les instal·lacions, incloent-hi àrees i punts d'accés. - [op.pl.2.2] Documentació del sistema, incloent-hi equips, xarxes internes i connexions a l'exterior, i punts d'accés al sistema (llocs de treball i consols d'administració). - [op.pl.2.3] Esquema de línies de defensa, incloent-hi punts d'interconnexió a altres sistemes a altres xarxes - [op.pl.2.4] Sistema d'identificació i autenticació d'usuaris. 	
op.pl.3 Adquisició de nous components	TOT ES			0 %	100%	Qan s' incorporin o substituïxin elements que afectin el desenvolupament de programari, com mòduls o llibreries, el proveïdor de la solució verifica que no trenca la seguretat. Si cal estableix accions de formació i sensibilització.	L' organització ATL disposarà d' un procés per planificar les adquisicions de solucions que consideri els riscos, els elements existents en l' arquitectura actual del sistema i les necessitats que poden sorgir de la seva integració. <ul style="list-style-type: none"> - [op.pl.3.1] Atendrà les conclusions de l'anàlisi de riscos ([op.pl.1]). - [op.pl.3.2] Serà d'acord amb l'arquitectura de seguretat escollida ([op.pl.2]). - [op.pl.3.3] Contemplarà les necessitats tècniques, de formació i de finançament, de forma conjunta.
op.pl.4 Dimensionament o / Gestió de la Capacitat	B	M	A	50 %	50%	Se li lliuren a l'organització client de la solució ON-PREMISE, a la Guia d'instal·lació.	L' organització ATL disposarà d' un estudi amb l' evolució històrica de la capacitat del sistema, o Pla de Capacitat, que permeti dimensionar els components en els quals es donarà suport a la solució amb ajuda de les taules proporcionades pel fabricant. <ul style="list-style-type: none"> - [op.pl.4.1] Necessitats de processament. - [op.pl.4.2] Necessitats d'emmagatzematge d'informació:

1.7 Directius de Seguretat

						durant el seu processament i durant el període que s'hagi de retenir. – [op.pl.4.3] Necessitats de comunicació. – [op.pl.4.4] Necessitats de personal: quantitat i qualificació professional. –[op.pl.4.5] Necessitats d'instal·lacions i mitjans auxiliars.	
--	--	--	--	--	--	---	--

op.pl.5 Components certificats	B	M	A	100%	0%	Per a categoria alta, els components addicionals, proporcionats conjuntament amb la solució implantada, estan certificats.	L'organització ATL procurarà que els components de la infraestructura TIC que interactuïn amb la solució implantada estiguin certificats. – [op.pl.5.1]. S'utilitzarà el Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació (CPSTIC) del CCN, per seleccionar els productes o serveis subministrats per un tercer que formin part de l'arquitectura de seguretat del sistema i aquells que es referencin expressament en les mesures d'aquest real decret.	
op.acc.1 Identificació	TOTES			70%	30%	La solució cobreix les necessitats del client facilitant-li la gestió dels usuaris: Identificació, estat, responsable o àrea a la qual pertany, rols assignats, permisos en base a aquests rols, etc.	Es procedimentarà a nivell intern la gestió dels usuaris registrats en els seus sistemes. Els responsables d'ATL hauran de gestionar mitjançant procediments les altes, modificacions i baixes d'usuaris, així com les autoritzacions i notificacions d'aquests canvis.	La solució implantada estarà integrada amb el sistema de gestió d'usuaris Active Directory de ATL. Els usuaris de la solució implantada poden ser donats de baixa o deshabilitats en qualsevol moment i poden tenir definida una data de caducitat prèviament establerta.
op.acc.2 Requisits d'accés	TOTES			50%	50%	La solució no permet que un usuari sense estar donat d'alta, o sense els oportuns permisos, pugui accedir a recursos no habilitats.	L'organització ATL gestionarà els drets d'accés de tot el sistema, inclosos els drets d'accés que puguin correspondre als usuaris a la solució implantada.	
op.acc.3 Segregació de funcions i tasques	B	M	A	70%	30%	La solució implantada permet la segregació de funcions i tasques mitjançant l'assignació de permisos a usuaris específics i a grups d'usuaris. La solució implantada permet la gestió diferenciada de les tasques crítiques per dos o més usuaris mitjançant fluxos, restringint els accessos individuals. Es poden llançar notificacions o alertes a un usuari Administrador. La solució considera la separació de funcions d'	Existirà un procés intern documentat, relacionat amb la segregació de funcions i tasques en el sistema d'informació de l'organització client.	En la solució implantada es poden definir els diferents usuaris i grups d'usuaris. Es gestiona l'assignació de permisos mitjançant opcions de menú, associació de rols als usuaris o grups, etc., la qual cosa permet establir a quines funcionalitats accedeix cada usuari. La solució disposa d'opcions de consulta i llistat d'usuaris i grups, juntament amb les funcionalitats permeses.

1.7 Directrius de Seguretat

					operació, configuració, manteniment i auditoria; no permet accessos a entorns o capes no associades a un perfil d'accés.		
Op.acc.4 Procés de gestió de drets d'accés	TOTES	30%	70%		L'aplicació permet l'assignació i el bloqueig o cancel·lació àgils d'accessos d'usuari.	L'organització ATL disposarà d'un procés intern relacionat amb les altes, modificacions i baixes dels usuaris, associat amb els principis de mínima funcionalitat, necessitat de conèixer i capacitat d'autoritzar.	

op.acc.5 Mecanismes d'autenticació	B	M	A	60%	40%	<p>Perquè les contrasenyes siguin únicament conegudes pel mateix usuari, aquestes es guarden xifrades en la solució implantada; La solució permet establir la robustesa de les contrasenyes segons diferents requisits de seguretat, clarament especificats (d'acord amb la política de contrasenyes de l'organització client).</p> <p>Segons la categoria del sistema on s'integri la solució, s'inclouen mecanismes per implementar un doble factor d'autenticació, o bé es recolza amb un altre factor proporcionat per la xarxa de l'organització client.</p> <p>Per integrar-se en sistemes de categoria alta, la solució admet que les credencials se suspendran després d'un període definit de no utilització.</p>	<p>L'organització ATL ha de definir la seva política de comunicació de claus. Els usuaris han de confirmar la recepció de les credencials i ser notificats de les condicions d'ús del servei.</p> <p>L'organització ATL ha d'establir una política de contrasenyes que inclogui la seva robustesa i la seva data de caducitat, atès que les contrasenyes han de ser canviades periòdicament. Es disposarà d'un procés periòdic de revisió de comptes d'usuari, en especial els que disposen de drets d'administració..</p>	<p>S'associarà el procés d' altes al directori actiu del sistema. Si el sistema és de categoria mitjana o superior. L'aplicació disposa de funcionalitats que permeten a l'organització client parametritzar la qualitat i complexitat de les contrasenyes en base a la política que tingui definida, cobrint:</p> <ul style="list-style-type: none"> Permet seleccionar el nombre mínim de caràcters. Tipologia dels caràcters (alfanumèrics, majúscules / minúscules, caràcters especials). Manté un històric de contrasenyes no permetent repetir les últimes empleades. Permet especificar la periodicitat per a la caducitat de la clau. Permet especificar caducitat de la contrasenya. Permet seleccionar el nombre d'intents fallits abans del seu bloqueig.
--	----------	----------	----------	-----	-----	--	--	--

1.7 Directrius de Seguretat

op.acc.6 Accés local	B	M	A	80%	20%	<p>L'aplicació no revela informació de l'usuari davant intents d'accés (no conserva el nom d'usuari i menys la clau).</p> <p>Es limita el nombre d'intents permesos d'autenticació insatisfactòria.</p> <p>La solució registra tant els intents d'autenticació amb èxit com els fallits.</p> <p>Així mateix, la solució informa els usuaris de les seves obligacions un cop obtingut l'accés. Per complir amb requisits de categoria mitjana, la solució informa l'usuari de l'últim accés efectuat amb la seva identitat.</p>	<p>Per a sistemes de categoria alta, s'estudiarà en el FW o en el WAF la possibilitat de limitar l'accés des de llocs diferents dels que s'hagi d'accedir (per exemple, determinats països).</p>	<p>Per facilitar el suport tècnic, el sistema mostra per pantalla errors per a la resolució d'incidències, sempre codificats, no mostrant-se en cap moment missatges informatius detallats de l'error, o de la seva solució, ni del sistema operatiu o la base de dades sobre la qual està integrat, que puguin ser aprofitats per un atacant per detectar algunes vulnerabilitats.</p>
op.acc.7 Accés remot	B	M	A	60%	40%	<p>La solució s'ha elaborat en base a metodologies de desenvolupament segur que impedeixen els atacs corrents, del tipus injecció de codi, alteració d'URL, etc.</p> <p>Es relacionaran clarament els ports que hagin de romandre oberts, juntament amb la seva justificació, a la Guia d'instal·lació.</p>	<p>L'accés a la solució en remot serà mitjançant mecanismes d'autenticació segurs com IPSec o a través de VPN.</p> <p>Es verificaran els ports oberts necessaris perquè funcioni la solució i la seva influència en altres solucions que coexisteixin en el sistema. S'analitzaran les implicacions de les regles necessàries en el FW en relació a les ja existents i la seguretat global.</p>	<p>Es gestionaran i protegiran els certificats de servidors necessaris per establir accessos remots segurs.</p>
op.exp.1 Inventari d'actius	TOTES			50%	50%	<p>El proveïdor facilita tota la informació relacionada amb la solució implantada i el maquinari aportat per a la instal·lació, amb vista a facilitar el seu inventari al nostre client ATL.</p>	<p>L'organització ATL mantindrà un inventari actualitzat de tots els elements del sistema, detallant la seva naturalesa i identificant el seu responsable.</p>	<p>L'organització ATL acordarà amb el proveïdor el format en què aquest li lliurarà l'inventari corresponent a la solució, per facilitar la seva integració a l'inventari.</p>
op.exp.2 Configuració de seguretat (bastionat)	TOTES			60%	40%	<p>La solució permet complir els requeriments de configuració segura: Assignació de les funcionalitats segons necessitat, control de les funcions crítiques i deshabilitació de les funcions no requerides.</p> <p>Les accions dels usuaris seran segures tret que l'usuari actuï conscientment. La solució disposa de la possibilitat de definir diferents perfils i nivells de seguretat.</p>	<p>Es retiraran els comptes i contrasenyes estàndard i per defecte de la solució.</p> <p>S'atendrà les consideracions de bastionat presents a la Guia d'instal·lació proporcionada pel proveïdor de la solució.</p>	<p>En determinats casos, caldrà seguir les bones pràctiques de organització internacionals.</p>
op.exp.3 Gestió de la configuració	B	M	A	50%	50%	<p>El proveïdor de la solució disposa d'un procediment de gestió del canvi per garantir l'actualització de diagrames d'estructura, inventari, documentació i guies de la solució, sempre</p>	<p>L'organització ATL disposarà d'un procediment per gestionar la configuració, en base a actualitzacions de diagrames, documentació, guies, etc., a partir de les</p>	

1.7 Directrius de Seguretat

					que procedeixi, després de la implementació d'un canvi.	diferents solucions aportades externament i els canvis que s'hi vagin introduint.	
op.exp.4 (Manteniment)		TOT ES	80%	20%	El proveïdor de la solució proporcionarà, avisos de vulnerabilitats, nous pegats, versions, canvis en la configuració, etc.	L'organització ATL disposarà d'un procediment per analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, les millores i noves versions del fabricant de la solució i d'altres fabricants que suporten elements del sistema. L'organització client gestionarà les garanties i contractes de manteniment. L'organització ATL gestionarà les llicències.	S'activarà l'avís automàtic del proveïdor d'alerta de nous pegats del producte.
op.exp.5 Gestió de canvis		B M A	80%	20%	El proveïdor de la solució proporcionarà tota la informació necessària a l'organització ATL, perquè aquesta pugui analitzar un canvi anunciat respecte a la solució implantada, coneixent i avaluant els riscos que implica abans d'aprovar-lo.	Es disposarà d'un procediment de Gestió de canvis que inclogui registre, avaluació, aprovació, etc. Intervenint el Responsable de Seguretat en aquelles peticions de canvi que puguin implicar risc per a la seguretat del sistema.	L'organització ATL disposarà d'una eina per registrar les peticions de canvi i que serveixi de suport per poder avaluar-les abans de la seva aprovació, mantenint la traçabilitat de les mateixes fins a la seva aprovació i implementació o la seva desestimació.
op.exp.6 Protecció enfront de codi danyós		TOT ES	20%	80%	El proveïdor garanteix que la solució podrà funcionar adequadament en l'entorn del client juntament amb els principals programaris de control de codi danyós existents en el mercat.	L'organització client disposarà de mecanismes de protecció enfront de codi danyós i seguirà les indicacions dels fabricats.	Quan per qualsevol circumstància algun mòdul de la solució implantada sigui detectat com a virus, haurà de gestionar la configuració de l'antivirus per declarar-lo com a fals positiu, després d'haver-ho confirmat amb el proveïdor de la solució.
op.exp.7 Gestió d'incidents		B M A	80%	20%	El proveïdor de la solució disposarà d'un procediment de gestió d'incidents conforme a l'ENS i les organitzacions ATL podran fer ús d'un canal establert a l'efecte per comunicar comportaments anòmals o incidents respecte a la solució implantada. El personal de suport del proveïdor assignarà una categorització i escalat segons la criticitat que percebi el client. Els registres d'auditoria de la solució implantada permeten traçar la incidència, bé	En l'organització ATL es disposarà d'un procediment de gestió d'incidents que, en el seu cas, reaccioni i aïlli els serveis proporcionats per la solució en cas de necessitat, escalant el problema al proveïdor de la solució.	S'acordarà entre el proveïdor de la solució i l'organització client un canal per reportar incidents de seguretat.

1.7 Directrius de Seguretat

op.exp.8 Registre de l'activitat dels usuaris	B	M	A	60%	40%	<p>Hi ha un registre d'activitat en la solució implantada que registra les accions més importants que realitzen els usuaris. Aquest registre és configurable, atès que registrar-ho tot podria significar elevats volums d'informació.</p> <p>De forma genèrica es registra tota l'activitat referent a:</p> <ul style="list-style-type: none"> Segregació de funcions i tasques. Gestió de drets d'accés. Mecanismes d'autenticació. 	<p>Per a categoria mitjana, l'organització ATL revisarà informalment els registres d'activitat buscant patrons anormals.</p> <p>Per a categoria alta, s'emprarà un SIEM o correlador d'esdeveniments per tractar els LOGS de manera que permeti gestionar la seguretat de forma centralitzada.</p>	<p>Per a categoria alta, el proveïdor de la solució ha de proporcionar la informació necessària (ubicació, formats, etc.) perquè puguin tractar-se adequadament de forma automatitzada els diferents LOGS proporcionats per la solució implantada i poder establir així les alertes adequades.</p>
op.exp.9 Registre de Gestió d'incidents	B	M	A	70%	30%	<p>El proveïdor de la solució implantada facilitarà informació respecte a la gestió dels incidents al client. Per a això, disposa d'un procés documentat de la gestió per a la gestió d'incidents, recolzat en una eina de registre i seguiment.</p>	<p>Existirà en l'organització ATL un procés de control de les incidències gestionades internament, incloent les derivades al proveïdor de la solució implantada, que permeti verificar el compliment dels Acords de Nivell de Servei (ANS/SLA) respecte al suport proporcionat.</p>	
op.exp.10 Protecció dels registres d'activitat	B	M	A	50%	50%	<p>El proveïdor de la solució especificarà clarament a la Guia d'instal·lació on s'emmagatzemen els diferents LOGS, amb quin format, quan s'esborren, si estan en clar o xifrats, etc.</p> <p>El proveïdor de la solució habilitarà un camp que permeti configurar la ubicació on s'emmagatzemaran aquests registres.</p> <p>Els esdeveniments es registren en un format estandarditzat, comprensible per a la majoria dels correladors d'esdeveniments.</p> <p>S'especifica el període de retenció i conservació dels LOGS, cas de no ser configurable.</p>	<p>Per a categoria alta, l'organització ATL ha de portar una gestió centralitzada de tots els registres de LOGS generats pels seus serveis, que li permetin realitzar-ne una correlació amb l'objecte de detectar activitats inusuals.</p>	<p>L'organització client, en cas de no haver estat previst pel proveïdor, ha d'establir mecanismes per protegir la confidencialitat dels LOGS, la seva integritat i la seva disponibilitat, incloent-los en la política de <i>backup</i>.</p>
op.exp.11 Protecció de claus criptogràfiques	B	M	A	50%	50%	<p>La solució permet l'ús d'elements criptogràfics certificats i acreditats. Les claus caducades seran rebutjades.</p>	<p>Existirà un procés de control de les claus criptogràfiques en tot el seu cicle de vida.</p> <p>Únicament s'empraran elements criptogràfics certificats i acreditats.</p>	

1.7 Directrius de Seguretat

op.ext .1 Contractació i acords de nivell de servei (SLA)	B	M	A	50%	50%	El proveïdor de la solució subscriurà un acord contractual amb l'organització ATL. S'hi detallarà el que es considera qualitat mínima i comportament normalitzat de la solució. El proveïdor respondrà davant comportaments anòmals de la plataforma, mitjançant manteniment correctiu, especialment el que corregeixi incidents de seguretat. Com a part d'aquest contracte, en una addenda al mateix, o en un document a part, s'establiran acords de nivell de servei (SLA). Els SLA almenys cobriran les accions de resposta a incidents reportats per l'organització client i freqüència d'elaborar i facilitar reports de gestió.	En determinades ocasions l'organització ATL s'adscriu a unes condicions generals de contractació, les quals s'han de llegir detalladament amb antelació, en evitació de desagradables sorpreses futures.	S'establiran de forma clara les responsabilitats de les parts, proveïdor i client, en relació a la solució aportada.
op.ext .2 Gestió diària	B	M	A	70%	30%	El proveïdor de la solució implantada facilitarà informació del servei, com poden ser els temps de resposta respecte als incidents	Existirà un procediment intern d'avaluació dels proveïdors, dels nivells de servei i compliment dels requisits establerts.	Poden arribar a acordar-se reunions de seguiment periòdiques, encara que sigui una vegada a l'any.

op.ext.9 Mitjans alternatius	B	M	A	0%	100%	<u>Inicialment no aplica.</u> Llevat que el mateix proveïdor en el seu Pla de Continuitat disposi d'un proveïdor alternatiu per transferir-li el servei. En aquest cas es comunicarà la seva existència, i preferiblement les seves dades, a l'organització client.	Per a sistemes de categoria alta es tindrà elegit, estudiat i, si és possible, compromès contractualment, un proveïdor alternatiu per prestar el servei amb les mateixes garanties de seguretat.	
op.cont.1 Anàlisi d'impacte	B	M	A	60%	40%	El proveïdor de la solució inclou el servei de gestió d'incidents i de suport a les organitzacions client en la seva anàlisi d'impacte (BIA). El proveïdor de la solució facilitarà tota la informació requerida pel client per poder realitzar les seves pròpies anàlisis d'impacte. El proveïdor facilita un esquema de l'arquitectura de la solució, perquè l'organització client conegui les dependències dels elements que són crítics per als serveis suportats per la solució.	L'organització ATL disposarà d'una anàlisi d'impacte (BIA) que inclogui la solució aportada pel proveïdor.	
op.cont.2 Pla de continuïtat	B	M	A	10%	90%	Si el proveïdor disposa d'un pla de continuïtat que estigui relacionat, directament, amb la solució aportada, haurà d'informar el client.	Per a categoria alta, el Pla de Continuitat haurà d'assegurar la solució, sempre que s'hagi determinat la seva conveniència en el BIA.	
op.cont.3 Proves periòdiques	B	M	A	10%	90%	El proveïdor informarà l'organització client de les proves realitzades respecte al seu Pla de continuïtat, i en quina data les ha realitzat, amb relació al suport i manteniment correctiu de la solució aportada.	L'organització client haurà de realitzar proves del seu Pla de Continuitat, en relació a la solució implantada.	
op.mon.1 Detecció d'intrusió	B	M	A	10%	90%	<u>Inicialment no aplica.</u> No obstant això, el proveïdor disposarà en la seva pròpia xarxa de desenvolupament.	L'organització client disposarà d'eines específiques de detecció i prevenció d'intrusió (IDS/IPS) o aprofitarà	

1.7 Directrius de Seguretat

op.mon.2 Sistema de mètriques	B	M	A	10%	90%	Per a categoria mitjana el proveïdor disposa de mesuraments relacionats amb els incidents que gestiona, que hagin estat oberts per l'organització client, incloent-hi els temps de resolució.	L'organització client calcularà les mètriques de categoria mitjana, referides a la gestió d'incidents, harmonitzant-les si és necessari amb els mesuraments facilitats pel proveïdor de la solució respecte als incidents que li han estat escalats.	
mp.if.1 Àrees separades amb control d'accés	TOTES			10%	90%	<u>Inicialment no aplica.</u> No obstant això, el proveïdor disposarà d'àrees separades i protegides on s'ubicarà el repositori de codi font i la resta de la infraestructura TIC necessària per poder prestar els serveis de suport, manteniment i desenvolupament.	La infraestructura TIC que suporta la solució implantada, incloent-hi els elements maquinari específics que pugui incorporar, s'instal·larà en àrees separades protegides amb control d'accés.	
mp.if.2 Identificació de les persones	TOTES			20%	80%	<u>Inicialment no aplica.</u> No obstant això, el proveïdor disposarà d'un sistema d'identificació de les persones amb accés a la sala on es troba el repositori de codi font. Únicament personal autoritzat i identificat hauria d'accedir a la parametrització de la solució en el procés d'implantació en les dependències de l'organització client, sota la supervisió del Responsable de Seguretat del mateix.	S'identificarà totes les persones que accedeixin als locals on es troben els equips que suporten la solució i únicament es permetrà treballar en els equips a personal qualificat que estigui degudament autoritzat.	
mp.if.3 Condicionament o dels locals	TOTES			10%	90%	<u>Inicialment no aplica.</u> No obstant això, el proveïdor disposarà de les seves dependències condicionades per poder prestar els serveis associats a la solució implantada (manteniment i suport).	S'ha de disposar d'unes instal·lacions auxiliars adequades per garantir l'eficaç compliment de la infraestructura TIC en la qual es recolza la solució implantada, protegint-la dels riscos identificats.	
mp.if.4 Energia elèctrica	B	M	A	20%	80%	<u>Inicialment no aplica.</u> No obstant això, els elements TIC necessaris per prestar serveis de suport i atenció al client tindran garantit el subministrament elèctric durant els temps acordats en els SLA subscrits amb l'organització client.	S'ha de garantir l'energia elèctrica en els equips que suporten la solució implantada i, en cas de fallada de subministrament, garantir-ne el funcionament mitjançant SAIS i, si és possible, generadors elèctrics.	
mp.if.5 Protecció davant incendis	TOTES			20%	80%	<u>Inicialment no aplica.</u> No obstant això, els elements TIC necessaris per prestar serveis de suport i atenció al client tindran garantida la protecció enfront d'incendis.	S'han de protegir davant incendis els equips que suporten la solució implantada, ja siguin aquests fortuits o deliberats, aplicant almenys la normativa industrial pertinent.	
mp.if.6 protecció enfront d'inundacions	B	M	A	20%	80%	<u>Inicialment no aplica.</u> No obstant això, els elements TIC necessaris per prestar serveis de suport i atenció al client tindran garantida la protecció enfront d'inundacions.	S'han de protegir davant incidents causats per l'aigua, ja siguin fortuits o deliberats, els equips que suporten la solució implantada.	

1.7 Directrius de Seguretat

mp.if.7 Registre d'entrada i sortida d'equipament	TOTES			10%	90%	No aplica. No obstant això, el proveïdor ha de registrar l'entrada i sortida d'equipament a l'àrea segura on es troba la infraestructura TIC del proveïdor de la solució emprada per poder donar servei de manteniment i suport, inclòs el repositori de codi font.	A l'àrea segura on s'ubica la infraestructura que suporta la solució implantada, existirà un registre detallat de tota entrada i sortida d'equipament, incloent-hi la identificació de la persona que autoritza de moviment.	
mp.if.9 Instal·lacions alternatives	B	M	A	0%	100%	No aplica. No obstant això, per a categoria alta, es disposarà d'instal·lacions alternatives que alberguin la infraestructura TIC necessària per prestar serveis de manteniment i suport.	Per a sistemes de categoria alta, es garantirà l'existència i disponibilitat d'instal·lacions alternatives que suportin la solució implantada, per poder seguir operant en el cas que les instal·lacions habituals no estiguin disponibles. Les instal·lacions alternatives gaudiran de les mateixes garanties de seguretat que les instal·lacions habituals.	
mp.per.1 Caracterització del lloc de treball	B	M	A	50%	50%	El personal de desenvolupament, manteniment i suport del proveïdor tindran identificades les seves implicacions respecte a la seguretat. De la mateixa manera, el personal del proveïdor assignat per implantar la solució en el client, complirà els requeriments de seguretat establerts pel propi client, a més dels del proveïdor.	Es definiran els requisits que han de satisfer les persones que hagin d'ocupar el lloc de treball, en particular, en termes de confidencialitat. Per al Sector Públic, a més dels que consten en la RLT es definiran els llocs subjectes a subcontractació, incidint en implicacions de seguretat.	Es definiran perfils i grups d'usuaris en la solució, d'acord amb els requisits de seguretat.
mp.per.2 Deures i obligacions	TOTES			50%	50%	En funció de la funcionalitat de la solució implantada, es disposarà d'elements que permetin a l'usuari conèixer els drets i obligacions respecte a l'ús de la mateixa. En el seu defecte, es detallaran en el manual d'usuari. El proveïdor de la solució, especialment el seu personal de suport a clients, subscriu clàusules de confidencialitat.	S'informarà cada persona que treballi en la solució implantada, dels deures i responsabilitats del seu lloc de treball en matèria de seguretat, ja sigui personal intern o subcontractat.	Se subscriuran acords de confidencialitat amb els treballadors. Se subscriurà un acord de confidencialitat amb el proveïdor de la solució.
mp.per.3 Conscienciació	TOTES			50%	50%	Tot el personal del proveïdor de la solució, especialment el de suport directe al client, estarà conscienciat respecte a la confidencialitat i altres dimensions de la seguretat.	S'han de realitzar les accions necessàries per conscienciar regularment el personal.	
mp.per.4 Formació	TOTES			50%	50%	El proveïdor de la solució pot desenvolupar accions formatives relacionades amb aquesta, de manera que pugui conèixer-se pels usuaris les funcionalitats i accions permeses en l'eina, així com el seu ús segur.	Es formarà regularment el personal per a l'adequat compliment de les seves funcions operant la solució, sobre la configuració de la mateixa a personal administrador, sobre la detecció i reacció davant incidents als usuaris i al CAU i respecte a la correcta gestió de la informació tractada per la plataforma als usuaris.	

1.7 Directrius de Seguretat

mp.per.9 Personal alternatiu	B	M	A	50%	50%	Es garantirà l' existència i disponibilitat, en el proveïdor de la solució, de diverses persones que es puguin fer càrrec de les funcions de suport i manteniment correctiu en cas d' indisponibilitat del personal habitual.	Per a categoria alta, es garantirà l' existència i disponibilitat d' altres persones, en l' organització client, que es puguin fer càrrec de les funcions d' administració de la solució en cas d' indisponibilitat del personal habitual.	El personal alternatiu haurà d' estar sotmès a les mateixes garanties de seguretat que el personal habitual.
mp.eq.1 Lloc de treball net	B	M	A	*No	Sí	<u>No aplica.</u>	S' exigirà que els llocs de treball romanguin malmesos, sense més material damunt la taula que el requerit per a l' activitat que s' està realitzant en cada moment. Per a categoria mitjana es guardaran sota clau en abandonar el lloc.	
mp.eq.2 Bloqueig de lloc de treball	B	M	A	30%	70%	L' aplicació pot disposar d' un temps d' inactivitat de sessió, havent de validar-se de nou un cop assolit. Si l'organització client estableix la cancel·lació de les sessions obertes, habitualment en accessos remots a la solució, el proveïdor haurà realitzat el desenvolupament preveient que aquesta casuística no alteri o danyi la integritat de la base de dades.	En l' organització client on s' hagi implantat la solució, es disposarà de polítiques a l' efecte. Mitjançant directives de domini s' establiran els temps d' inactivitat de l' usuari abans de bloqueig del lloc, requerint-se una nova autenticació. Per a categoria alta, les polítiques de cancel·lació de sessions inactives es poden establir a nivell de directives de domini.	
mp.ep.3 Protecció d' equips portàtils	B	M	A	0%	100%	<u>No aplica.</u> No obstant això, si els desenvolupadors o personal de manteniment i suport del proveïdor de la solució treballen en remot sobre equips portàtils, es disposarà de polítiques i mesures de seguretat adequades, que incloguin l' ús de VPN i tal vegada xifrat del disc.	Els portàtils evitaran connectar-se remotament a la solució des de xarxes no segures. S'evitarà que l'equip contingui memoritzades claus d'accés remot a l'organització i/o a la solució. Es disposarà en l' organització client d' una política de treball remot que es desenvoluparà amb les mesures de seguretat oportunes.	
mp.eq.9 Mitjans alternatius	B	M	A	50%	50%	El proveïdor de la solució mantindrà el suport acordat i no es consideraran, llevat de limitacions en els nivells de servei, fallades en l' atenció per no disposar de mitjans alternatius.	L' organització ATL disposarà de mitjans alternatius de tractament per suportar la solució, conforme als temps establerts en l' anàlisi d' impacte.	
mp.com.1 Perímetre segur	B	M	A	40%	60%	Quan per motiu de l'operativa i funcionalitat de la solució implantada pugui afectar-se a aquest control del client obrint determinats ports i/o creant regles específiques en el tallafocs (FW), s'informa clarament en la Guia d'instal·lació de la solució implantada de tots els punts necessaris perquè l'organització client pugui realitzar en la configuració del FW, balancejadors, etc., els canvis necessaris per mantenir l' eficàcia i compatibilitat de les funcions de seguretat del perímetre.	L' organització client haurà de disposar d' un sistema tallafocs que separi la xarxa interna de l' exterior. Per a categoria alta disposarà de doble corona de <i>clusters</i> de FW, de diferents fabricants. S' han d' estudiar amb deteniment les implicacions de requerir crear noves regles en el FW per a la seguretat global del perímetre. Únicament personal especialitzat i autoritzat ha de crear regles en el FW.	

1.7 Directrius de Seguretat

mp.com.2 Protecció de la confidencialitat	B	M	A	50%	50%	Quan el proveïdor de la solució requereixi prestar suport remot, s'establiran VPN per garantir una connexió segura a les instal·lacions d'ATL.	S'utilitzaran VPN per a accessos des de l'exterior del perímetre. Per a categoria alta, es verificarà el xifrat de les dades tractades per l'aplicació i, si s'escau, es xifrarà la base de dades en què es recolzi o s'albergarà en una cabina de discos que cifre per maquinari.
mp.com.3 Protecció de l'autenticitat i la integritat	B	M	A	50%	50%	La solució implantada disposarà de prevencions davant accions d'alteració de la informació, atacs d'injecció de codi, o segrestos de sessió, especialment si és accedida des d'Internet. L'aplicació només permetrà com a mitjans d'autenticació els descrits en els controls d'accés. Els perfils d'usuari i els seus drets, si són gestionats per la pròpia solució, s'emmagatzemaran xifrats amb la robustesa adequada.	L'accés es realitzarà mitjançant VPN. Es realitzarà periòdicament algun test d'intrusió, especialment quan s'introdueixin modificacions significatives en la solució.
mp.com.4 Segregació de xarxes	B	M	A	0%	100%	<u>No aplica.</u> No obstant això, el proveïdor de la solució proporciona en la Guia d'instal·lació informació sobre l'arquitectura de la solució, al costat de possibilitats i consideracions davant possibles segregacions.	Per a categoria alta, se segregará la solució implantada d'altres xarxes la coexistència de les quals pugui comportar risc per a la seguretat global de l'organització client.
mp.com.9 Mitjans alternatius	B	M	A	0%	100%	<u>No aplica.</u> Llevat dels mitjans de comunicació emprats pel proveïdor per donar suport sobre la solució implantada, si aquesta és de categoria alta.	Per a categoria alta, es garantiran mitjans alternatius de comunicacions per mantenir l'accés a la solució, quan aquest es requereixi des de l'exterior del perímetre de l'organització client.

mp.si.1 Etiquetatge	TOTES			0 %	100 %	<u>No aplica.</u>	Si s'empren suports, hi ha d'haver una política d'etiquetatge en l'organització client, que inclogui els empleats per realitzar <i>backups</i> de la solució implantada.
mp.si.2 Criptografia	B	M	A	10 %	90 %	<u>No aplica.</u> No obstant això, es recomanarà al client, ja sigui en accions de suport, o en la Guia d'instal·lació i la resta de documentació de la solució, que quan es realitzin còpies en elements extraïbles s'avalui configurar el seu xifrat emprant algorismes acreditats.	Ha d'existir una política de xifrat per a mitjans removibles, inclosos aquells en què poguessin externalitzar-se còpies de seguretat, incloses les de la solució implantada, que consideri el risc i la qualificació de la informació emmagatzemada.
mp.si.3 Custòdia	TOTES			0 %	100 %	<u>No aplica.</u>	Es custodiaran degudament els suports emprats, especialment els que continguin les còpies de seguretat de la solució implantada.. Les còpies de seguretat es conservaran en una ubicació diferent de la que conté la base de dades copiada. s còpies de seguretat es conservaran en una

1.7 Directrius de Seguretat

					ubicació diferent de la que conté la base de dades copiada.	
mp.si.4 Transport	TOT ES	0 %	10 0 %	<u>No aplica.</u>	S'ha de garantir que els dispositius portàtils i mòbils al costat dels suports, com poden ser els que contenen les còpies de seguretat, romanguin sota el control de l'organització client i que satisfan els seus requisits de seguretat mentre estan sent desplaçats.	
mp.si.5 Esborrat i destrucció	B M A	50 %	50 %	S'utilitzaran dades específiques de prova. No obstant això, quan el personal de proveïdor hagi de realitzar accions amb dades del client, procurarà anonimitzar-los prèviament. Si no fos possible, s'han d'emprar les mateixes mesures de seguretat que en producció i en acabar s'han d'emprar mètodes d'esborrat segur, d'acord amb productes certificats. Quan s'hagin de desinstal·lar versions, o es procedeixi a retirar màquines incloses en la solució, es procedirà a un esborrat segur i en el seu cas destrucció certificada amb indicació individual del número de sèrie dels suports destruïts.	L'organització client disposarà d'una política d'esborrat i destrucció conforme a estàndards acreditats. El responsable de seguretat de l'organització client procedirà a confirmar el procés i el producte emprat per esborrar o destruir els actius inclosos en la solució implantada, o que la suporten, abans de la seva retirada.	Es conservaran registres evidències de l'esborrat i destrucció segurs.
mp.sw.1 Desenvolupament	B M A	10 0 %	0 %	El proveïdor de la solució empra una metodologia de desenvolupament que té en compte la seguretat. No obstant això, en desenvolupaments a mida es podrà emprar la metodologia de l'organització client. Es disposa d'evidències de control del desenvolupament i de la qualitat d'aquest, així com de les dades de prova emprades i quines d'aquestes proves són respecte a la seguretat. S'estarà en condicions d'evidenciar la seguretat del procés mitjançant diagrames o altres elements en la Guia d'instal·lació o la resta de documentació de la solució. La solució final implantada inclou requisits de seguretat i, en concret, elements d'identificació i autenticació, així com de protecció de la informació que tracti. La solució implantada inclou registre de pistes d'auditoria.	Si l'organització client disposa d'una metodologia de desenvolupament que tingui en compte la seguretat, es pot exigir al proveïdor de la solució que els desenvolupaments a mida s'hi adaptin. L'organització client requerirà als proveïdors de la solució, habitualment si és aquesta a mida, el compliment d'un procés de desenvolupament en entorn separat al de producció.	

1.7 Directius de Seguretat

mp.sw.2 Acceptació i posada en servei	B	M	A	70 %	30 %	<p>El proveïdor de la solució realitza anàlisis de vulnerabilitats i proves de penetració de la mateixa periòdicament, especialment si s'ha modificat la versió de la solució de forma rellevant.</p> <p>Tot desenvolupament per a la solució, incloses les seves successives versions, evolucions o pegats, hauran d'haver estat comprovats abans del seu llançament respecte als requeriments de seguretat en un entorn aïllat i sense dades reals.</p> <p>El proveïdor de la solució donarà suport a l'organització client, si és requerit, pel que fa a les proves de preproducció per evitar el deteriorament de la seguretat.</p>	<p>L'organització client requerirà al proveïdor de la solució evidències de la realització d'anàlisis de vulnerabilitats.</p> <p>Per a categoria mitjana, l'organització client realitzarà proves de penetració abans de la posada en producció de la solució implantada. Per a categoria alta es realitzarà una anàlisi de coherència en la integració de la solució implantada amb els sistemes existents.</p>	
mp.info.1	TOTES					<p>El proveïdor compleix amb la legislació aplicable en matèria de protecció de dades.</p> <p>El proveïdor col·laborarà amb el Delegat de Protecció de Dades (DPD) de l'organització client, per evidenciar el nivell de compliment de la solució a la normativa.</p> <p>El procés de desenvolupament de la solució considerarà la privacitat per defecte (PbD).</p>	<p>L'organització client inclourà requeriments de protecció de dades en els seus sistemes i per a les solucions externes que es contractin.</p> <p>Disposarà d'un DPD que supervisarà l'impacte o el risc que té la solució en l'àmbit de la privacitat. Si ho estima necessari demanarà la realització d'una EIPD.</p> <p>Contemplarà la gestió del risc, incloent-hi la privacitat, en l'organització.</p>	
mp.info.2 Qualificació de la informació	B	M	A	0 %	100 %	<p>El proveïdor de la solució mantindrà la seva pròpia política de qualificació. La certificació del sistema de desenvolupament, manteniment i suport de la solució respecte a l'ENS, per part del proveïdor, determina el nivell dels serveis i dades a tractar per la solució un cop implantada en l'organització client.</p>	<p>S'aurà de disposar en l'organització client d'una política de qualificació de la informació.</p> <p>Els actius d'informació hauran d'estar inventariats.</p>	
mp.info.3 Xifrat	B	M	A	0 %	100 %	<p><u>No aplica.</u> No obstant això, el proveïdor podria incorporar mecanismes de xifrat a la solució implantada.</p>	<p>Per a categoria alta, la informació amb un nivell alt en confidencialitat es xifrarà tant durant el seu emmagatzematge com durant la seva transmissió. S'empraran sistemes de xifrat en les cabines de discos si la solució implantada no incorpora mecanismes de xifrat per programari.</p>	
mp.info.4 Signatura electrònica	B	M	A	10 %	90 %	<p>La solució implantada, si és necessari, permetrà l'ocupació o la integració amb altres serveis susceptibles d'emprar signatures electròniques ja sigui per a autenticació o per assegurar la integritat de la informació gestionada.</p>	<p>Existirà una política de signatura electrònica.</p> <p>Per a categoria mitjana, es verificarà que la solució implantada empi sistemes de signatura electrònica avançada, basats en certificats qualificats.</p> <p>Es gestionaran els certificats, incloent-hi el proveïdor, les dates de caducitat i les adreces per al correu electrònic d'avís de renovació, si és possible de forma centralitzada.</p>	<p>La signatura electrònica és un servei extern a qualsevol sistema <i>on-premise</i>, per la qual cosa la màxima responsabilitat recau sobre el client. El proveïdor únicament haurà de garantir la integració.</p>

1.7 Directrius de Seguretat

mp.info.5 Segells de temps	B	M	A	10%	90%	Per a categoria alta, si és necessari per aplicar aquest control, la solució implantada es basa en segells de temps electrònics qualificats.	Si és d' aplicació, i tindran en compte els segells de temps en la política de signatura electrònica. Per a categoria alta, si és necessari, la solució implantada es basarà en segells de temps electrònics qualificats. Es gestionaran els segells de temps.	El segellament de temps, per les seves pròpies característiques, és una funció externa a qualsevol sistema <i>on-premise</i> , per la qual cosa la màxima responsabilitat recau sobre el client. El proveïdor únicament haurà de garantir la integració.
mp.info.6 Neteja de documents	TOTES			10%	90%	Aquest control pot ser cobert per procediments i eines del client. No obstant això, podria dotar-se a la solució de mecanismes de control i esborrat de determinades metadades en els documents generats i/o emmagatzemats.	Es disposarà de normativa referida a l'esborrat de metadades. Es poden implantar solucions internes, automàtiques, o procediments manuals, que complementin les prestacions de la solució implantada. Cal recordar que, en base a l' ENI, certes metadades són requerides a efectes d' interoperabilitat, per la qual cosa no sempre és aconsellable una eliminació indiscriminada.	Les dades tractades són del client, per la qual cosa la màxima responsabilitat recau sobre ell.
mp.info.9 Còpies de seguretat	TOTES			10%	90%	El proveïdor de la solució realitzarà recomanacions respecte a les còpies de seguretat de la solució a la Guia d'instal·lació.	L' organització client disposarà d' un procediment de còpies en el qual es configuraran les còpies conforme als RPO declarats en el BIA i seguint les recomanacions del proveïdor de la solució.	
mp.s.1 Protecció del correu electrònic	TODAS			50%	50%	<p>Cuando una de las funcionalidades de la solución implantada sea el envío de notificaciones mediante correo electrónico, se dispondrá de un registro de actividades completo que incluya los correos electrónicos enviados.</p> <p>Se valorará la posibilidad de incluir funcionalidades antispam en relación al envío de correos electrónicos automáticos desde la solución, en base a permitir configurar:</p> <ul style="list-style-type: none"> Número de correos enviados por minuto. Número de destinatarios que se pueden asignar en un solo correo. Tamaño máximo del contenido del correo. Establecer las posibles acciones a realizar si se intenta sobrepasar los parámetros definidos, como cancelar el envío y enviar una notificación al usuario y/o al administrador. 	<p>Debe existir en la organización cliente una política de correo electrónico y procedimientos de seguridad que incluyan los principales problemas de seguridad que suele tener asociados: cifrado de adjuntos sensibles, limitaciones de uso, etc., así como mecanismos de seguridad: antivirus en relación a correos entrantes y salientes y antispam. También se articulará la concienciación del usuario.</p> <p>Si la solución implantada no dispone de un servidor de correo electrónico propio, sino que se integra con el servidor de correo corporativo de la organización cliente a través del protocolo SMTP, será este servidor el que se encargue de realizar la gestión requerida y deberá supervisarse.</p>	

1.7 Directrius de Seguretat

mp.s.2 Protecció de serveis i aplicacions Web	B	M	A	50%	50%	A nivell del desenvolupament de la solució, el proveïdor ha tingut en compte la prevenció de manipulació d'URL, prevenció d'atacs d'injecció de codi, prevenció d'intents d'escalat de privilegis, d'atacs "Cross site scripting", d'atacs de manipulació de programes o dispositius o de sistemes d'emmagatzematge, ja sigui a nivell de les diferents fases de desenvolupament o bé en el propi cicle de vida del producte una vegada en producció.	L'organització client ha de gestionar la seguretat en els serveis publicats mitjançant la solució implantada, incloent anàlisi de seguretat o hacking ètic almenys un cop any. S'externalitzen tercers per aconseguir una separació entre qui gestiona i qui realitza les proves de penetració.	
mp.s.8 Protecció davant la denegació de servei	B	M	A	0%	100%	L'aplicació no té accés des del exterior. No cal aplicar mesures de protecció davant la denegació de servei.	Es dimensionarà el sistema amb folgança, respecte a les taules de dimensionament que proporciona el proveïdor a la Guia d'instal·lació. Per a categoria alta s'establiran procediments de reacció als atacs, que incloguin comunicació amb el proveïdor de comunicacions.	
mp.s.9 Mitjans alternatius	B	M	A	0%	100%	<u>No aplica.</u>	Per a categoria alta es garantirà l'existència i disponibilitat de mitjans alternatius per prestar els serveis que presta la solució implantada, en el cas que fallin els mitjans habituals. Aquests mitjans alternatius estaran subjectes a les mateixes garanties de protecció que els mitjans habituals.	