Política de Seguretat de la Informació

AIGÜES DE VIC, SA i AIGÜES DE VIC ENGINYERIA I TECNOLOGIA, SL

Marc de referència de la seguretat de la informació del grup: compromís de les direccions, objectius i principis, marc normatiu, organització i responsabilitats, qualificació de la informació, gestió de riscos, tercers, incidents i règim d'aprovació i revisió, d'acord amb l'article 12 i la mesura org.1 de l'Esquema Nacional de Seguretat (Reial decret 311/2022) i la guia CCN-STIC 805.

Redactat / Revisat per:	Pol Parés Llobet	07/09/2026
Aprovat per:	Guillem Treserra Prat	24/09/2026
Versió:	2	
Estat:	Aprovat	
Classificació:	Pública	

Índex

Índex 2
Historial de canvis 3
1. Introducció 4
2. Objecte i abast 4
3. Missió de l'organització 4
4. Objectius de seguretat 5
5. Principis de seguretat 6
6. Marc normatiu 6
7. Organització de la seguretat 7
7.1. Comitè de Seguretat de la Informació 7
7.2. Rols de seguretat 7
7.3. Designació, renovació i substitució 8
7.4. Resolució de conflictes 8
8. Estructura i desenvolupament de la documentació de seguretat 9
9. Qualificació de la informació 9
10. Obligacions del personal, conscienciació i formació 10
11. Gestió de riscos 10
12. Protecció de dades de caràcter personal 10
13. Tercers: prestadors i proveïdors 10
14. Gestió d'incidents de seguretat 11
15. Aprovació, entrada en vigor i revisió 11

Historial de canvis

Versió	Canvis	Data	Autor
1	Creació del document. Signat per la Gerència el 24/09/2026	03/09/2026	Pol Parés
2	Apartat 6: retirades les dues referències al sanejament que quedaven, que no és activitat d'AIGÜES DE VIC, SA (acta del 10/09/2026)	04/11/2026	Pol Parés

1. Introducció

AIGÜES DE VIC, SA i AIGÜES DE VIC ENGINYERIA I TECNOLOGIA, SL (en endavant, AVENTEC), conjuntament el grup, depenen dels sistemes d'informació per assolir els seus objectius. Aquests sistemes s'han d'administrar amb diligència i amb les mesures adequades, en funció del risc, per protegir-los davant dels danys accidentals o deliberats que puguin afectar la confidencialitat, la integritat, la disponibilitat, l'autenticitat o la traçabilitat de la informació tractada i dels serveis prestats.

L'objectiu últim de la seguretat de la informació és garantir que l'organització pugui complir la seva missió, desenvolupar les seves funcions i prestar els seus serveis, actuant de manera preventiva, supervisant l'activitat diària i reaccionant amb prestesa davant dels incidents. Atès que les amenaces evolucionen ràpidament, la seguretat es concep com una part integral de cada etapa del cicle de vida dels sistemes, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i per les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament que se'n deriven s'identifiquen i s'inclouen en la planificació i en la contractació de serveis i productes que afecten els sistemes d'informació.

La Direcció d'AIGÜES DE VIC, SA i la Direcció d'AVENTEC es comprometen amb la protecció de la informació i dels serveis, doten el sistema de gestió dels recursos necessaris i n'impulsen la millora contínua. Aproven aquesta Política de Seguretat de la Informació, comuna a les dues societats, com a marc de referència de tota la seguretat del grup.

2. Objecte i abast

Aquesta política estableix el marc de referència de la seguretat de la informació del grup: el compromís de les direccions, els objectius i els principis de seguretat, el marc normatiu, l'organització i les responsabilitats, els criteris de qualificació de la informació, el tractament dels riscos i el règim d'aprovació i revisió. És un document únic per a les dues societats, que comparteixen un mateix sistema de gestió de la seguretat de la informació, un mateix cos documental i uns mateixos responsables.

S'aplica al sistema d'informació únic del grup, de categoria MITJANA d'acord amb l'Annex I del Reial decret 311/2022, i a tots els serveis que aquest sistema suporta, tant en entorns de tecnologies de la informació com de control industrial. La delimitació concreta dels serveis, de la informació, de les ubicacions i dels actius que formen part del sistema es determina i es manté actualitzada a la documentació del sistema de gestió. S'aplica també a totes les persones que integren les dues societats i als prestadors de serveis i proveïdors de solucions que hi intervenen. El seu compliment és obligatori per a totes elles.

3. Missió de l'organització

AIGÜES DE VIC, SA gestiona el cicle integral de l'aigua del municipi de Vic (captació, potabilització, distribució, laboratori i atenció a l'abonat) en virtut de la relació contractual que manté amb l'Ajuntament de Vic. AVENTEC desenvolupa, implanta i opera solucions de digitalització del cicle de l'aigua per a ajuntaments i entitats gestores, amb la plataforma AQUA360 (suite de programes: Smart Metering i comunicacions IoT amb Telelectura, GMAO, Oficina Virtual i Programa d'abonats),

les oficines virtuals associades i la telelectura de comptadors. Les dues societats presten serveis a entitats del sector públic per a l'exercici de les seves competències, motiu pel qual els seus sistemes d'informació queden inclosos a l'àmbit d'aplicació de l'Esquema Nacional de Seguretat, d'acord amb l'article 2.3 del Reial decret 311/2022.

La disponibilitat, la integritat, l'autenticitat, la confidencialitat i la traçabilitat de la informació i dels serveis són essencials per a la continuïtat del subministrament d'aigua, per a la facturació als abonats i per a la confiança de les entitats clients. La seguretat dels sistemes propis condiciona directament la seguretat dels sistemes que el grup gestiona per compte dels clients: un compromís de les eines d'administració, de les credencials o de les plataformes d'allotjament es pot traslladar immediatament als clients. La protecció d'aquests elements, i la dels sistemes de control industrial que suporten el cicle de l'aigua, té la consideració de prioritat de seguretat del grup.

4. Objectius de seguretat

Amb aquesta política, el grup es proposa assolir els objectius de seguretat següents:

- Garantir la confidencialitat, la integritat i l'autenticitat de la informació, i la continuïtat en la prestació dels serveis.
- Implantar mesures de seguretat en funció del risc, proporcionades i justificades.
- Formar i conscienciar les persones de l'organització, garantir la traçabilitat dels accessos, aplicar el principi de mínim privilegi i reforçar el deure de confidencialitat respecte de la informació coneguda en l'exercici de les funcions.
- Protegir físicament els actius d'informació, situant-los en àrees segures amb controls d'accés proporcionats als riscos detectats.
- Protegir la informació transmesa a través de les xarxes de comunicacions amb els mitjans adequats.
- Controlar l'adquisició, el desenvolupament i el manteniment dels sistemes al llarg de tot el seu cicle de vida, garantint la seguretat per defecte, i mantenir el control en la incorporació de nous components.
- Gestionar els incidents de seguretat per detectar-los, contenir-los, mitigar-los i resoldre'ls, i evitar que es reprodueixin.
- Protegir la informació personal amb les mesures tècniques i organitzatives adequades als riscos del tractament, d'acord amb la legislació de protecció de dades.
- Supervisar de manera contínua la seguretat, corregint les ineficiències detectades i millorant el sistema.
- Protegir la informació i els sistemes dels clients gestionats, mantenint la separació entre els entorns de cada client per evitar que un incident es propagui d'un client a un altre.
- Protegir els sistemes de control industrial que suporten el cicle de l'aigua, mantenint-los segregats de la xarxa corporativa i controlant els accessos remots, propis i de proveïdors.
- Controlar els accessos administratius i remots als sistemes propis i de clients, amb identificació individual, mínim privilegi i traçabilitat de les actuacions.
- Incorporar la seguretat al cicle de vida de les aplicacions i dels serveis desenvolupats per a clients, des del disseny fins al lliurament i el manteniment.
- Seleccionar proveïdors i components tecnològics amb garanties de seguretat proporcionades al risc, per protegir la cadena de subministrament dels serveis prestats.

5. Principis de seguretat

La presa de decisions en matèria de seguretat es regeix pels principis bàsics dels articles 5 a 11 del Reial decret 311/2022, que orienten totes les mesures i actuacions de l'organització:

- Abast estratègic: la seguretat de la informació compta amb el compromís i el suport de tots els nivells de l'organització i es coordina i s'integra de manera coherent amb la resta d'iniciatives.
- Seguretat integral: la seguretat s'entén com un procés que integra els elements tècnics, humans, materials i organitzatius, present des del disseny inicial dels sistemes i en l'operativa habitual, evitant qualsevol actuació puntual o conjuntural.
- Gestió de la seguretat basada en el risc: les mesures s'estableixen en funció dels riscos a què estan subjectes la informació i els sistemes, són proporcionals al risc que tracten i estan justificades; també es tenen en compte els riscos del tractament de dades personals.
- Prevenció, detecció, resposta i conservació: s'implanten accions preventives que minimitzen les vulnerabilitats i eviten la materialització de les amenaces i, quan es produeixen, es dona una resposta àgil per restaurar la informació i els serveis, garantint una conservació segura de la informació.
- Existència de línies de defensa: la protecció es dissenya i s'implanta en capes, de manera que la fallada d'una capa no comprometi el conjunt del sistema.
- Vigilància contínua i reavaluació periòdica: es disposa de mitjans per detectar i respondre a comportaments anòmals i per avaluar de manera continuada l'estat de seguretat, amb un procés de millora contínua que revisa i actualitza les mesures segons la seva eficàcia i l'evolució dels riscos.
- Seguretat per defecte i des del disseny: els sistemes es dissenyen i es configuren per garantir la seguretat per defecte i proporcionen la funcionalitat mínima necessària per prestar el servei.
- Diferenciació de responsabilitats: les funcions del Responsable de la Seguretat i del Responsable del Sistema estan diferenciades i recauen en persones diferents.

6. Marc normatiu

La seguretat de la informació del grup s'emmarca en les obligacions derivades de la seva naturalesa, de la normativa que li és aplicable i dels compromisos contrets amb tercers: la normativa de l'Esquema Nacional de Seguretat, la de protecció de dades personals, la sectorial d'abastament d'aigua i les obligacions contractuals amb les entitats titulars dels serveis i amb la resta de tercers. La relació de les normes que afecten aquesta política és la següent:

- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, i les seves instruccions tècniques de seguretat.
- Guies CCN-STIC del Centre Criptològic Nacional aplicables al sistema, en particular les de la sèrie 800.
- Reglament (UE) 2016/679, general de protecció de dades, i Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals.
- Reial decret 3/2023, de 10 de gener, pel qual s'estableixen els criteris tecnicosanitaris de la qualitat de l'aigua de consum, el seu control i el seu subministrament, pel que fa a les obligacions de notificació i de protecció de les instal·lacions.

- Reglament (UE) 2024/1689, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial, pel que fa als sistemes d'intel·ligència artificial que el grup desplega o utilitza.
- Text refós de la Llei de l'Estatut dels Treballadors i conveni col·lectiu d'aplicació, pel que fa als deures del personal i al règim disciplinari.
- Normativa sectorial d'abastament d'aigua, el contracte amb l'Ajuntament de Vic i les obligacions contractuals amb les entitats clients i amb la resta de tercers.

7. Organització de la seguretat

El grup adopta el model de governança de la guia CCN-STIC 801, basat en la diferenciació de responsabilitats, amb un òrgan col·legiat únic per a les dues societats i rols unipersonals amb funcions definides i un mecanisme de coordinació entre ells. Les decisions corporatives en matèria de seguretat es prenen al Comitè de Seguretat de la Informació i s'eleven a les direccions quan excedeixen les seves atribucions; la informació de seguretat es distribueix a través del Comitè i dels canals corporatius.

7.1. Comitè de Seguretat de la Informació

Es constitueix el Comitè de Seguretat de la Informació, únic per a les dues societats, integrat per la Gerència, que el presideix; el Responsable de la Seguretat, que n'exerceix la secretaria; el Responsable de la Informació i dels Serveis; i el Responsable del Sistema. S'hi poden convidar altres persones quan els assumptes ho requereixin. El Comitè es reuneix com a mínim semestralment i sempre que les circumstàncies ho requereixin, i reporta a les direccions de les dues societats.

És l'òrgan de coordinació de la seguretat i té les funcions següents: supervisar la normativa de seguretat, que aprova el Responsable de la Seguretat, i comprovar-ne la coherència amb aquesta política; fer el seguiment de l'estat de la seguretat (riscos, incidents, indicadors i auditories); fixar una valoració de referència per als tipus d'informació i serveis a fi d'harmonitzar les anàlisis de riscos; promoure la disponibilitat de recursos per atendre les necessitats de seguretat; proposar a les direccions la designació dels rols unipersonals; resoldre els conflictes de responsabilitat; revisar aquesta política; i elevar a les direccions les decisions que excedeixin les seves atribucions. La secretaria convoca les sessions, redacta les actes i custodia la documentació del Comitè. Les seves decisions queden documentades en actes.

7.2. Rols de seguretat

Es defineixen els rols unipersonals de seguretat següents, amb els deures i les responsabilitats que s'indiquen. Els rols són únics per a les dues societats i les funcions de Responsable de la Informació i de Responsable del Servei recauen en la mateixa persona, amb la denominació de Responsable de la Informació i dels Serveis.

Rol	Deures i responsabilitats
Responsable de la Informació i dels Serveis	Determina els requisits de la informació tractada i dels serveis prestats, inclosos els nivells de servei exigibles, aprova la valoració de la informació i dels serveis en les dimensions de seguretat i és el responsable de cada informació als efectes de la seva qualificació. Accepta els riscos residuals sobre la informació i els serveis.
Responsable de la Seguretat	Determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis, determina la categoria del sistema, formalitza la Declaració d'Aplicabilitat, aprova la normativa i els procediments de seguretat, supervisa la implantació de les mesures i n'informa el Comitè. Gestiona la seguretat de manera contínua, dirigeix la gestió dels incidents i actua com a interlocutor i Punt de Contacte davant de clients, proveïdors i organismes en matèria de seguretat i incidents.
Responsable del Sistema	Desenvolupa, opera i manté el sistema d'informació durant tot el seu cicle de vida, inclosos els sistemes allotjats al núvol, aplica les mesures de seguretat aprovades, custodia els registres d'operació i informa el Responsable de la Seguretat de les desviacions.
Delegat de Protecció de Dades (si n'hi ha de designat)	Assessora i supervisa en matèria de protecció de dades personals, emet el seu parer en l'anàlisi de riscos, en les avaluacions d'impacte i en la incorporació de sistemes d'intel·ligència artificial, i intervé en la gestió de les violacions de seguretat de dades personals.

Les persones designades per a cada rol consten als nomenaments signats, que es conserven amb la documentació del sistema de gestió. Quan el grup actua com a encarregat del tractament o contracta prestadors de serveis, inclosos els de núvol, el Responsable de la Seguretat, o la persona en qui delegui, exerceix de Punt de Contacte. Cap persona pot ocupar alhora els rols de Responsable de la Seguretat i de Responsable del Sistema.

7.3. Designació, renovació i substitució

Els membres del Comitè de Seguretat de la Informació i els rols de seguretat es designen i es nomenen per escrit per la Direcció de cada societat, a proposta del Comitè de Seguretat en el cas dels rols unipersonals, i les persones designades accepten les seves funcions per escrit. La constitució del Comitè, les designacions inicials i les altes i les baixes posteriors es documenten en acta. Els nomenaments es revisen cada dos anys i, en tot cas, quan el lloc queda vacant o davant d'un incompliment reiterat de les funcions, amb advertiment previ.

7.4. Resolució de conflictes

Els conflictes entre els diferents responsables els resol el Comitè de Seguretat de la Informació i, en última instància, la Direcció d'AIGÜES DE VIC, SA i la Direcció d'AVENTEC. El Responsable de la Seguretat és diferent del Responsable del Sistema i no en depèn jeràrquicament en l'exercici de les seves funcions, fet que garanteix la segregació necessària.

8. Estructura i desenvolupament de la documentació de seguretat

Aquesta política es desenvolupa mitjançant un cos documental estructurat en nivells: la normativa de seguretat, d'obligat compliment, que uniformitza l'ús dels aspectes concrets dels sistemes i les obligacions de les persones i que aprova el Responsable de la Seguretat; els procediments operatius, que detallen com s'executen les tasques i qui les fa, aprovats pel Responsable de la Seguretat amb la revisió del Responsable del Sistema; i els registres i evidències, que demostren el funcionament del sistema. Els documents porten codi, versió entera, historial de canvis i classificació, i les versions substituïdes es conserven.

La documentació de seguretat es custodia al repositori documental del sistema de gestió, amb accés segons la classificació de cada document. La normativa de seguretat està a disposició de totes les persones que la necessiten conèixer, en particular les que utilitzen, operen o administren els sistemes d'informació, a través dels canals corporatius establerts; els procediments es distribueixen al personal que els ha d'aplicar.

9. Qualificació de la informació

El Responsable de la Informació i dels Serveis és el responsable de cada informació que tracta el sistema i té en exclusiva la potestat de fixar-ne i modificar-ne el nivell de seguretat. Els criteris que determinen el nivell de seguretat requerit són els de l'article 40 i de l'Annex I del Reial decret 311/2022: per a cada tipus d'informació i per a cada servei es valora el perjudici que causaria un incident que afectés la confidencialitat, la integritat, la disponibilitat, l'autenticitat o la traçabilitat, i se li assigna el nivell BAIX, MITJÀ o ALT en cada dimensió. La valoració consta a la documentació d'abast, valoració i categorització del sistema i la revisa el Comitè de Seguretat, que en fixa la referència per harmonitzar les anàlisis de riscos.

A efectes del tractament diari per part del personal, la informació es qualifica en tres nivells, que la normativa de seguretat desenvolupa amb les regles de tractament de cadascun:

Nivell	Definició	Exemples
Pública	Informació que el Responsable de la Informació i dels Serveis ha aprovat divulgar. La seva divulgació no causa cap perjudici.	Webs corporatius, tarifes aprovades, avisos als abonats, material informatiu, aquesta política.
Ús intern	Informació d'ús exclusiu del personal del grup, la divulgació externa de la qual no està autoritzada i causaria un perjudici limitat. És el nivell per defecte de tota la informació que no es qualifica d'una altra manera.	Documentació tècnica i de procediments, comunicacions internes, actes, esquemes de xarxa, informes de gestió.
Confidencial	Informació la divulgació, alteració o pèrdua de la qual causaria un perjudici greu al grup, als abonats, als clients o a terceres persones. Correspon a la informació valorada de nivell MITJÀ o ALT en confidencialitat.	Dades personals d'abonats, de treballadors i d'usuaris dels clients, lectures i dades de facturació, dades de contracte, codi font, credencials i claus, configuracions de seguretat, informes d'auditoria i d'incidents, informació dels clients gestionats.

La informació no classificada amb restriccions que el grup rebi d'una administració pública amb la marca ÚS OFICIAL es tracta com a Confidencial. Qui crea una informació li assigna el nivell segons aquests criteris; en cas de dubte la tracta com a Confidencial i consulta el Responsable de la Informació i dels Serveis.

10. Obligacions del personal, conscienciació i formació

Totes les persones de les dues societats tenen l'obligació de conèixer i complir aquesta política i la normativa que la desenvolupa. El desconeixement de la normativa no eximeix del seu compliment. Abans de rebre credencials d'accés als sistemes, cada persona coneix i accepta per escrit aquesta política i la normativa de seguretat en els aspectes que l'afecten. El Comitè de Seguretat i l'àrea de personal disposen els mitjans perquè la informació arribi a tots els afectats.

Totes les persones reben accions de conscienciació en seguretat de la informació de manera periòdica, com a mínim anualment, amb un programa de conscienciació contínua que atén especialment les noves incorporacions. Les persones amb responsabilitat en l'ús, l'operació o l'administració dels sistemes reben la formació necessària per a un maneig segur, amb caràcter obligatori abans d'assumir la responsabilitat corresponent, tant si és la primera assignació com si es tracta d'un canvi de lloc o de funcions.

11. Gestió de riscos

La seguretat es gestiona a partir de l'anàlisi de riscos, que avalua les amenaces i els riscos a què estan exposats els sistemes amb la metodologia que aprova el Comitè de Seguretat. L'anàlisi es repeteix de manera regular, com a mínim anualment, i també quan es produeixen canvis en la informació tractada o en els serveis prestats, quan ocorre un incident greu de seguretat, quan es reporten vulnerabilitats greus o quan es modifiquen els riscos relatius a la protecció de dades.

Per harmonitzar les anàlisis, el Comitè de Seguretat estableix una valoració de referència per als tipus d'informació i els serveis. Les mesures es seleccionen segons el risc, de manera proporcionada, i el seu tractament es planifica i es prioritza en un pla de tractament que fixa responsables i terminis. Els riscos per sobre del llindar acceptable que fixa el Comitè es tracten; el risc residual l'accepta formalment el Responsable de la Informació i dels Serveis i la Gerència.

12. Protecció de dades de caràcter personal

Les dues societats tracten dades de caràcter personal, segons es descriu als seus registres d'activitats de tractament. El grup avalua els riscos relacionats amb les dades personals i estableix un pla d'actuació per corregir els que superin el llindar acceptable. Quan es detecta un tractament d'alt risc, es realitza, si escau, una avaluació d'impacte. Les mesures i la resposta a les violacions de seguretat de dades personals es coordinen amb la resta de mesures de seguretat, com també la resposta a l'exercici dels drets dels interessats.

13. Tercers: prestadors i proveïdors

Quan el grup presta serveis a altres organitzacions o tracta informació de tercers, els fa partícips d'aquesta política, respecta les obligacions de la normativa de protecció de dades quan actua com a

encarregat del tractament, estableix canals de coordinació i de comunicació d'incidents i designa el Punt de Contacte corresponent.

Quan el grup utilitza serveis de tercers, cedeix informació a tercers o adquireix solucions, inclosos els serveis de núvol, exigeix contractualment garanties de seguretat equivalents a les establertes en aquesta política, el compliment de l'Esquema Nacional de Seguretat en la mesura que el servei ho requereix i el compliment de la resta de la normativa aplicable. Els tercers queden subjectes a aquestes obligacions, poden desenvolupar els seus propis procediments per satisfer-les i han de permetre que el grup els supervisi o sol·liciti evidències del compliment, incloses auditories. Els incidents es canalitzen a través dels punts de contacte. Els tercers garanteixen que el seu personal està conscienciat en seguretat, com a mínim al nivell establert en aquesta política.

Quan algun requisit d'aquesta política no pugui ser satisfet per un tercer, el Responsable de la Seguretat emet un informe que precisa els riscos i la manera de tractar-los. L'informe l'aprova el Responsable de la Informació i dels Serveis abans de l'inici de la contractació i es trasllada a la Direcció, que autoritza continuar-ne la tramitació i assumeix formalment els riscos detectats. L'adquisició, el desenvolupament o la implantació de sistemes d'intel·ligència artificial requereix, a més del compliment de la normativa vigent en la matèria, l'informe del Responsable de la Seguretat, que consulta el Responsable de la Informació i dels Serveis i, quan cal, el Responsable del Sistema.

14. Gestió d'incidents de seguretat

El grup disposa d'un procediment per a la gestió àgil dels esdeveniments i incidents de seguretat que suposin una amenaça per a la informació i els serveis. La resposta es coordina amb les obligacions derivades de la protecció de dades, de la normativa sanitària de l'aigua de consum i d'altra normativa aplicable, i es notifica als organismes de control competents sense dilacions indegudes i, quan és necessari, a les forces i cossos de seguretat o als òrgans judicials. Tota persona té el deure de comunicar els incidents i les sospites pel canal establert.

15. Aprovació, entrada en vigor i revisió

Aquesta política és aprovada formalment per acord de la Direcció d'AIGÜES DE VIC, SA i de la Direcció d'AVENTEC, cadascuna respecte de la seva societat, d'acord amb els articles 2.3 i 12.1 del Reial decret 311/2022, i entra en vigor en la data de la seva aprovació. Resta vigent fins que sigui substituïda per una de nova i deroga qualsevol política de seguretat anterior de les dues societats. Es difon a tot el personal de les dues societats, es publica als canals corporatius i es posa a disposició dels clients, dels proveïdors i de la resta de parts interessades que la sol·licitin.

El Comitè de Seguretat de la Informació revisa la política com a mínim anualment i hi introdueix les adaptacions necessàries davant de canvis normatius, organitzatius o tècnics i de les ineficiències detectades. Quan els canvis suposen una modificació substancial dels principis o de les responsabilitats designades, el Comitè proposa els canvis, que han de ser aprovats per les direccions. La substitució de la política la insta el Comitè i la ratifiquen les direccions, i es comunica als interessats pels mateixos canals emprats per a la seva difusió.

En prova de conformitat, la direcció de les dues societats aproven i signen aquesta Política de Seguretat de la Informació.

AIGÜES DE VIC, SA - AIGÜES DE VIC ENGINYERIA I TECNOLOGIA, SL

La direcció: Guillem Treserra Prat

Vic, 04/11/2026

