

PLEC DE PRESCRIPCIONS TÈCNiques PER A LA CONTRACTACIÓ SEGONS PROCEDIMENT OBERT DE LA ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A.

DINS DEL PLA DE RECUPERACIÓ, TRANSFORMACIÓ I RESILIÈNCIA (PRTR) I FINANÇAT PER LA UNIÓ EUROPEA – NEXTGENERATIONEU

EXPEDIENT LICITADOR NÚMERO: 11632

ÍNDEx

1	GLOSSARI	3
2	INTRODUCCIÓ	4
3	ANTECEDENTS	4
4	PROTECCIÓ DE DADES	5
5	CONDICIONS GENERALS D'EXECUCIÓ DEL SERVEI	6
5.1	LLOC DE PRESTACIÓ DELS SERVEIS	6
5.2	UTILITZACIÓ D'EINES TECNOLÒGIQUES EN LA PRESTACIÓ DELS SERVEIS	6
5.3	DISPONIBILITAT DEL PERSONAL TÈCNIC D'AMSA	7
5.4	HORARI DE PRESTACIÓ DELS SERVEIS	7
5.5	ACCÉS A LES DEPENDÈNCIES D'AMSA	7
5.6	PROACTIVITAT	7
5.7	DOCUMENTACIÓ I IDIOMA	7
6	OBJECTE	8
7	ABAST DEL PROJECTE	8
8	TIPOLOGIES DELS ENTORNS DE SISTEMES	8
8.1	ENTORN DE VIRTUALITZACIÓ	8
8.2	SISTEMES OPERATIUS	8
8.3	GESTORS DE BASE DE DADES	9
8.4	SERVIDORS D'APLICACIONS I ALTRES	9
8.5	PROGRAMARI ESPECÍFIC	9
8.6	SISTEMES ON-PREMISE I CLOUD	10
8.7	VOLUMETRIES DE SISTEMES	10
9	PLA D'ACCIÓ	10
9.1	MESURES D'APLICACIÓ IMMEDIATA	10
9.2	MESURES D'APLICACIÓ HORITZÓ CURT TERMINI	11
9.3	PLA DE TREBALL	11
10	CARACTERÍSTIQUES DEL SERVEI SOL·LICITAT	12
10.1	DIMENSIONAMENT	12
10.2	SERVEIS FORA D'HORARI	12
10.3	REQUERIMENTS DE L'EQUIP CONSULTOR	13
10.4	MODEL DE RELACIÓ	13
10.5	GARANTIES	13
11	DURADA DE CONTRACTE I TERMINIS	13
11.1	TERMINI MÀXIM PER AL KICK-OFF DEL SERVEI	14



PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

11.2	TERMINI MÀXIM PER A INICI DE LA PRESTACIÓ DEL SERVEI	14
------	--	----

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

1 GLOSSARI

Terminologia abreujada que s'utilitza en el document:

AMSA	Aigües de Manresa, S.A.
ANS	Acord de Nivell de Servei (SLA)
CAU	Centre d'Atenció a l'Usuari
ENS	Esquema Nacional de Seguretat
LOPDGDD	Llei Orgànica de Protecció de Dades de Caràcter Personal i Garantia dels Drets Digitals
NBD	Next Business Day (Següent dia laborable)
NIS2	Directiva Europea de protecció de la informació
PCA	Plec de Clàusules Administratives
PPT	Plec de Prescripcions Tècniques
RDBMS	Sistema Relacional de Base de Dades
RGPD	Reglament General de Protecció de Dades
SCADA	System Control And Data Acquisition
SI	Sistemes d'Informació
SLA	Service Level Agreement (Acord de Nivell de Servei)
SO	Sistema Operatiu
TIC	Tecnologies de la Informació i Comunicació

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

2 INTRODUCCIÓ

La Societat Municipal Aigües de Manresa S.A. (en endavant Aigües de Manresa), pretén donar compliment a part de les actuacions incloses en el projecte PERTE DE DIGITALITZACIÓ DEL CICLE DE L'AIGUA, dins del Pla de Recuperació, Transformació i Resiliència - Finançat per la Unió Europea – NextGenerationEU, mitjançant serveis d'assistència tècnica especialitzada d'adequació de l'entorn de sistemes d'informació que ha estat auditat en aspectes vinculats a Ciberseguretat.

Amb Data de 23 de desembre de 2021 la Junta Consultiva de Contractació Pública va dictar instrucció (en endavant, la Instrucció) en la qual exposa els aspectes més rellevants per a la contractació pública finançada a càrrec dels fons del Pla de Recuperació, Transformació i Resiliència (PRTR) derivada de les Ordres ministerials HFP/1030/2021 i 1031/2021 de 29 de setembre. Aquestes ordres, al seu torn, van ser dictades en desenvolupament del Reial decret llei 36/2020, de 30 de desembre, pel qual s'aproven mesures urgents per a la modernització de l'Administració Pública i per a l'execució del Pla de Recuperació, Transformació i Resiliència. (RDL 36/2020).

La instrucció, conté les principals exigències tant a nivell d'actuacions dels òrgans de contractació, com aspectes que s'han d'incloure en els plecs rectors de les licitacions finançades a càrrec del PRTR, sent la mateixa a l'empara de l'article 57 RDL 36/2020 d'obligat compliment per a tots els òrgans de contractació del sector públic.

Tenint en compte l'anterior, i en vista al finançament aconseguit a càrrec del PRTR en la convocatòria d'ajuts per a millora de l'eficiència del cicle urbà de l'aigua del PERTE de digitalització del cicle de l'aigua, per a les licitacions relacionades amb el projecte PERTE DE DIGITALITZACIÓ DEL CICLE DE L'AIGUA, Aigües de Manresa precisa conèixer el grau de subjecció dels plecs rectors del referit projecte, i en cas que fos necessari, la seva adaptació a la instrucció de referència a través de clàusules a incorporar en els esmentats plecs.

3 ANTECEDENTS

AIGÜES DE MANRESA ha inclòs la prestació objecte d'aquest contracte dins del projecte denominat "PERTE DE DIGITALITZACIÓ DEL CICLE DE L'AIGUA", que ha estat inclòs com a beneficiari de finançament europeu de l'Ordre TED/934/2022 de 23 de setembre, per la qual s'aproven les bases reguladores de la concessió d'ajudes per concurrència competitiva per a l'elaboració de projectes de millora de l'eficiència del cicle urbà de l'aigua i la primera convocatòria de subvencions (2022) en concurrència competitiva de projectes de millora de l'eficiència del cicle urbà de l'aigua (PERTE digitalització del cicle de l'aigua), en el marc del Pla de Recuperació, Transformació i Resiliència, Component 5 "Preservació de l'espai litoral i els recursos hídrics", inversió 1 (C5. L1 Materialització de les actuacions de depuració, sanejament, eficiència, estalvi, reutilització i seguretat d'infraestructures (DSEAR) i Objectiu CID/OA número 76 i Inversió 3 «Transició digital en el sector de l'aigua ("Enforcement Digital Mediambiental")» del Pla de Recuperació, Transformació i Resiliència amb l'objectiu d'obtenir millores en el funcionament de les infraestructures de tractament d'aigües residuals així com millorar el compliment dels criteris d'eficiència energètica o millorar l'eficiència i reduir les pèrdues d'aigua en els sistemes de distribució d'aigua.

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

L'objectiu general és l'execució d'actuacions tècniques sobre els sistemes d'informació que permetin actualitzar la base de programari instal·lada, d'acord amb els resultats obtinguts com a conseqüència d'una auditoria de Ciberseguretat que s'ha dut a terme durant l'any 2025.

L'auditoria esmentada va identificar vulnerabilitats en diferents sistemes que operen la informació de gestió d'AMSA. L'actualització dels entorns indicats permetrà disposar d'una plataforma homogènia en versions, evitant l'ús de programaris obsolets o que puguin estar fora de suport per part de terceres parts.

4 PROTECCIÓ DE DADES

El mes d'abril de 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) (DOUE 4.5.2016).

Les parts es comprometen a complir, en tot moment, les disposicions contingudes a la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, en endavant LOPD, i a la resta de normativa vigent en matèria de dades de caràcter personal, en particular, en el Real Decret 1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament del LOPD, en endavant "RLOPD" i el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE.

Si com a conseqüència dels serveis objectes de la present contractació, l'adjudicatari tingui accés i realitzi algun tipus de tractament de dades de caràcter personal incorporats als fitxers o tractament de titularitat Aigües de Manresa, entenent com a "tractament" qualsevol acció prevista en la definició continguda a l'article 5.1.t) del RLOPD, ho farà en la condició de "Encarregat del Tractament", conforme al previst a l'article 12 de la LOPD.

En el supòsit previst en el paràgraf anterior, l'adjudicatari quedarà obligat a:

- Tractar les dades de caràcter personal a les que tingui accés amb l'exclusiva finalitat de prestar els serveis objecte del present contracte i subjecte als criteris, requisits i especificacions previstes en el mateix i/o en les successives modificacions, sense que es puguin utilitzar dites dades per a finalitat diferent.
- No comunicar a tercers les dades de caràcter personal a les que es tingui accés, ni per la seva conservació. En qualsevol cas, si durant la prestació del servei resultés necessari subcontractar una part dels mateixos a diferents subcontractats, l'adjudicatari notificarà dita situació a Aigües de Manresa, per la seva consideració i aprovació.
- Finalitzat per qualsevol causa el servei objecte del contracte, l'adjudicatari estarà obligat a retornar a Aigües de Manresa, o a destruir en cas que així ho sol·liciti per escrit Aigües de Manresa, les dades de caràcter personal a les que hagi tingut

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

accés, qualsevol còpia dels mateixos, així com a qualsevol suport, ja sigui magnètic o documental, en el que consti alguna de les dades de caràcter personal objecte del tractament, en el format i condicions en els que es trobaren en la data de dita resolució.

- Observar el secret professional respecte a les dades personals que tracti, obligació que subsistirà després de l'extinció del servei objecte d'aquest contracte per qualsevol causa.
- Col·laborar amb Aigües de Manresa per a que pugui vetllar perquè l'adjudicatari reuneixi amb les garanties per al compliment del disposat a la normativa en matèria de protecció de dades de caràcter personal.
- Si el tractament de dades es produeix a les instal·lacions i en els sistemes d'Aigües de Manresa, el personal de l'adjudicatari estarà obligat a respectar les mesures de seguretat implantades per Aigües de Manresa, incloent les mesures de caràcter tècnic i organitzatives necessàries per garantir la seguretat, confidencialitat i integritat de les dades de caràcter personal i evitar la seva alteració, pèrdua, tractament o accessos no autoritzats de conformitat amb el disposat en la RLOPD. Aigües de Manresa instruirà adequadament i per escrit a l'adjudicatari amb relació a les mesures de seguretat implementades en l'ordre d'assegurar el compliment per aquest de la present obligació.

5 CONDICIONS GENERALS D'EXECUCIÓ DEL SERVEI

5.1 LLOC DE PRESTACIÓ DELS SERVEIS

L'adjudicatari prioritzarà la realització del servei en dependències d'AMSA sempre que això no suposi demora en el pla previst o impacti en la qualitat del servei realitzat. En el cas d'accés remot, AMSA facilitarà els codis d'accés per a realitzar connexions segures (VPN) des dels equips informàtics de l'adjudicatari als sistemes servidors existents a AMSA. Per raons de seguretat no es podran realitzar altres connexions a nivell de xarxa informàtica del proveïdor contra els equips d'AMSA diferents a les VPN, excepte en aquells casos que resulti ineludible.

L'adjudicatari facilitarà la relació detallada de personal pel qual es sol·licita l'accés a les dependències. El personal de seguretat d'AMSA autoritzarà l'accés prèvia identificació en els seus registres. El personal tècnic desplaçat a dependències d'AMSA està obligat a portar l'acreditació en un lloc visible durant la seva estada a les dependències.

5.2 UTILITZACIÓ D'EINES TECNOLÒGIQUES EN LA PRESTACIÓ DELS SERVEIS

Com a criteri general, correran per compte de l'adjudicatari l'adquisició i el cost econòmic associat de l'ús de llicències de programari que es requereixi per a la realització dels serveis, proves, així com les adaptacions i configuracions necessàries per a la seva correcta operació.

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

5.3 DISPONIBILITAT DEL PERSONAL TÈCNIC D'AMSA

Per raons particulars subjectes a la distribució de la jornada laboral del personal d'AMSA, només es pot garantir la disponibilitat del mateix entre les 7:30h i les 15:00h de dilluns a divendres.

L'anterior no exclou que l'adjudicatari pugui realitzar activitats fora de l'horari indicat. En aquest sentit, s'acordarà un calendari específic per aquelles actuacions programades que requereixin suport del personal d'AMSA fora de l'horari anteriorment esmentat, sobretot pel que fa a tasques amb possible impacte en els usuaris finals o infraestructures.

5.4 HORARI DE PRESTACIÓ DELS SERVEIS

Tenint en compte que gran part del servei es correspon amb actuacions d'actualització de programari i canvis de configuració, el contractista adjudicatari ha de preveure la realització de tasques fora dels horaris habituals d'oficina (9:00h a 18:00h), sobretot per a totes aquelles actuacions que impliquin la modificació de sistemes en producció (amb interrupció del servei). Tot i això, les actuacions es coordinaran amb el departament de SI ja que, d'acord amb la durada d'interrupció que representi pel servei, es podran executar en horari de tarda (a partir de les 15:00h) i amb altres franges horàries específiques d'impacte més reduït.

Cal tenir en consideració la possibilitat de realitzar tasques de configuració i parametrització encara que no s'apliquin fins a la propera aturada o reinici del sistema afectat, a l'objecte de minimitzar les actuacions fora de l'horari d'oficina indicat.

Pel que a fa a actuacions sobre sistemes que configuren els entorns de proves, no es preveu restricció horària a l'hora d'efectuar les actualitzacions.

5.5 ACCÉS A LES DEPENDÈNCIES D'AMSA

L'adjudicatari haurà de facilitar la relació de personal assignat al servei. AMSA facilitarà, si és oportú, la targeta acreditativa que permetrà l'accés controlat a les dependències que així ho requereixin. El personal tècnic desplaçat a dependències d'AMSA està obligat a portar l'acreditació en un lloc visible durant la seva estança al centre. L'adjudicatari comunicarà qualsevol canvi en la relació de personal que està vinculada al servei.

5.6 PROACTIVITAT

L'adjudicatari haurà de vetllar per la correcta prestació del servei, així com afavorir activament aquelles actuacions en favor de la minimització del nombre d'incidències i, en general, de l'òptima prestació del servei.

5.7 DOCUMENTACIÓ I IDIOMA

Tota la documentació generada relacionada amb la prestació del servei es proporcionarà en formats editables (MS-Word, MS-power point, MS-visio, altres de programari lliure, etc).

Les referències a informació de tercers s'efectuaran en la llengua en que hagin estat creades.

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

6 OBJECTE

L'objecte del present Plec de Prescripcions Tècniques (PPT) és la definició dels serveis i condicions d'execució que regularan la prestació de l'ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT, així com les relacions entre AMSA i l'adjudicatari en tot allò referent a aspectes tècnics de la prestació del servei i seguiment del contracte.

7 ABAST DEL PROJECTE

L'abast d'aquesta contractació inclou, de manera no exhaustiva, la realització dels serveis vinculats a l'execució del Pla de Ciberseguretat que s'indiquen a continuació:

- a) Inventari de versions de programaris d'ús en els diferents sistemes.
- b) Identificació de les versions de programaris validades recomanades.
- c) Creació de la matriu d'incompatibilitats entre versions de programaris.
- d) Actualització de firmware, sistemes operatius i programari de base (RDBMS, servidors aplicacions, balancejadors, servidors web,...).
- e) Aplicació de pegats específics (segons CVE ja identificades).
- f) Establir configuracions particulars en sistemes, com ara: limitació de ports oberts, anular usuaris per defecte, etc.
- g) Les actuacions anteriors es podran realitzar en tipologies d'equips com ara:
 - Servidors físics o virtuals (VMware, ProxMox)
 - Equipament de telecomunicacions (firewalls, routers, switches...)
 - Equips Appliance específics
 - Altre equipament específic (NAS, videograbadors...)
- h) Validació de la operativitat dels entorns com a pas previ al retorn a producció.

8 TIPOLOGIES DELS ENTORNS DE SISTEMES

Els entorns de sistemes d'informació d'AMSA són diversos i per això cal que la proposta de servei contempli un equip tècnic especialitzat en múltiples entorns i programaris, capacitat per operar la varietat d'àmbits que s'indiquen en els apartats següents. Es preveu que les actualitzacions s'apliquin tant als entorns de preproducció com als productius.

8.1 ENTORN DE VIRTUALITZACIÓ

- VMware VSphere 8.0.3
- ProxMox

8.2 SISTEMES OPERATIUS

En l'entorn de sistemes s'utilitzen versions dels següents programaris:

- CentOS 4/5/6/7 (64-bit)
- Debian GNU/Linux 10 (64-bit)
- Debian GNU/Linux 6 (64-bit)

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR .
EXPEDIENT LICITADOR NÚMERO: 11632

- Microsoft Windows 10 (64-bit)
- Microsoft Windows 7 (64-bit)
- Microsoft Windows Server 2003 Standard (32-bit)
- Microsoft Windows Server 2008 (32-bit)
- Microsoft Windows Server 2008 (64-bit)
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows Server 2012 (64-bit)
- Microsoft Windows Server 2016 or later (64-bit)
- Microsoft Windows Server 2025 (64-bit)
- Oracle Linux 4/5/6/7 (64-bit)
- Other 2.4.x Linux (32-bit)
- Other 2.6.x Linux (64-bit)
- Other 3.x or later Linux (64-bit)
- Other 4.x or later Linux (64-bit)
- Rocky Linux (64-bit) 9.4
- Ubuntu Linux (32-bit)
- Ubuntu Linux (64-bit) v 18.04.06 , v20.04, v22.04, v24
- VMware Photon CRX (64-bit)

8.3 GESTORS DE BASE DE DADES

Els sistemes gestors de bases de dades estan basats en programari:

- PostgreSQL
- ORACLE
- Microsoft SQL SERVER
- MySQL

8.4 SERVIDORS D'APLICACIONS I ALTRES

- IBM WebSphere
- Apache Tomcat
- Oracle Fusion Middleware Forms
- Nginx load balancer/reverse proxy

8.5 PROGRAMARI ESPECÍFIC

En aquest apartat s'inclouen altres programaris que poden relacionar-se amb:

- a) Equips tallafocs (FORTINET).
- b) Commutadors de xarxa (FORTINET, HP Mellanox, altres.
- c) Dispositius AP (Wi-Fi) Ubiquiti.
- d) NAS i dispositius locals d'emmagatzemament.
- e) Altres de caire molt específic (appliance, enregistadors de vídeo, etc).

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

8.6 SISTEMES ON-PREMISE I CLOUD

Tot i que la major part dels sistemes són "on-premise", es disposa d'algun servei extern ubicat al núvol sobre el que es tenen "competències" per exigir l'actualització, si s'escau, dels mateixos. En aquests cassos, es preveuen els serveis d'aquesta assistència tècnica en cas de dificultats del proveïdor que suporta el sistema.

No està previst actuacions sobre entorns ofimàtics com ara MICROSOFT 365 o plataformes al núvol gestionades íntegrament per terceres parts.

En el supòsit d'intervencions de sistemes in-situ, el contractista adjudicatari ha de preveure, si fos el cas, el desplaçament de l'equip tècnic a dependències d'AMSA, principalment a la ciutat de Manresa. Això no suposarà costos econòmics de servei addicionals.

8.7 VOLUMETRIES DE SISTEMES

A títol orientatiu, s'indiquen els amidaments pel que fa a serveis TIC:

- Servidors virtuals (S.O.) sobre VMware: al voltant de 150
- Equips firewall: 6
 - FORTI 40f / 60f v 7.0.13 build 0566 (Mature)
 - FORTIGATE 100F v 7.2.11 build 1740 (Mature)
- Altres equips específics: NAS, etc.... menys de 20.

9 PLA D'ACCIÓ

Durant l'any 2025 AMSA ha dut a terme una auditoria de ciberseguretat sobre gran part dels seus sistemes d'informació i infraestructura tecnològica.

Com a resultat d'aquesta auditoria es disposa d'un pla d'acció que prioritza una sèrie d'accions de caràcter urgent i altres a realitzar en el curt termini.

9.1 MESURES D'APLICACIÓ IMMEDIATA

AMSA - PLA DE CIBERSEGURETAT: Mesures de caire URGENT/IMMEDIAT		
Id	Acció a desenvolupar	Orientat a evitar
1	Desactivar serveis (TELNET, FTP, HTTP...) obsolets i que transmeten informació en text pla on s'inclouen usuaris i contrasenyes.	Robatori de credencials, suplantació.
2	Eliminar comptes genèriques per defecte de aplicacions	Robatori de credencials, suplantació. Robatori informació i control d'aplicacions
3	En sistemes Linux/Unix controlar, revisar i revocar privilegis insegurs	Control del servidors.
4	Aplicar pegats crítics a sistemes vulnerables (Servidors de Aplicacions, SO, Aplicacions pròpies, firmware entorn OT)	Malware i Atacs

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

5	Revisió configuracions permissives de firewall	Segments de xarxa OT exposats parcialment o sense segmentació adequada.
6	Bloqueig extern de panells web crítics (GitLab, wordpress, ERP, etc.)	Robatori de credencials, suplantació. Robatori informació i control d'aplicacions

Aquestes mesures urgents s'inclouen en l'abast dels serveis a realitzar en aquest contracte d'assistència tècnica.

9.2 MESURES D'APLICACIÓ HORITZÓ CURT TERMINI

D'altra banda, en l'horitzó de sis mesos, es recomana realitzar les actuacions que s'indiquen en la taula següent:

AMSA - PLA DE CIBERSEGURETAT: Mesures horitzó 6 mesos		
Id	Acció a desenvolupar	Orientat a evitar
1	Activar MFA (2FA) en tots els accessos a RDP, SSH, AD, Firewall, correu, sharepoint.	Atac força bruta, Robatori de credencials, suplantació. Robatori informació
2	Revisió de GPOs (Arxius administratius antics o obsoletes) de AD (Control d'accés)	Robatori de credencials, execució codi maliciós
3	Activar inspecció SSL/HTTPS al Firewall	Robatori de credencials, suplantació. Control del firewall.
4	Inventari comptes de servei obsoletes i en desús per la seva eliminació	Robatori de credencials, suplantació. Robatori informació i control d'aplicacions
5	Implantació de eines més robustes antimalware i antiphishing	Implantació d'eines com XDR i Protecció proactiva contra enganys per correu, detecció de tècniques de spoofing.

Aquestes mesures a curt termini s'inclouen en l'abast dels serveis a realitzar en aquest contracte d'assistència tècnica.

9.3 PLA DE TREBALL

AMSA facilitarà l'inventari de vulnerabilitats (CVE) que, per motius obvis, no s'inclouen en aquest plec de prescripcions, així com altra informació confidencial relacionada amb l'anàlisi i resultats que s'han derivat de l'auditoria de ciberseguretat realitzada.

El contractista adjudicatari tindrà accés a aquesta informació per tal de conèixer els àmbits d'actuació sobre els que desenvoluparà el servei.

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

El pla de treball proposat s'haurà de basar en prioritzar l'actualització d'aquells entorns que representin un major factor de risc per a AMSA. Tota la documentació indicada es posarà a disposició del contractista adjudicatari.

En el cas de sistemes que estan sota manteniment compartit amb tercers, es pactaran les intervencions per tal de tenir disponibilitat d'aquells si fos precis.

Un CVE (Common Vulnerabilities and Exposures) és un identificador únic assignat a una vulnerabilitat de seguretat coneguda en programari o maquinari. Cada CVE proporciona una referència comuna perquè fabricants, administradors de sistemes i investigadors de seguretat puguin parlar de la mateixa vulnerabilitat de manera clara i estandarditzada.

La coordinació dels treballs s'efectuarà amb el Tècnic Responsable de SI, que confirmarà amb els responsables de servei d'AMSA les afectacions i horaris més adients per a dur a terme les intervencions.

Com a criteri general, no es realitzaran actualitzacions de programari, aplicació de pegats ni canvis de configuració (entorns de producció) en jornades prèvies a dies festius i/o caps de setmana. S'afavorirà la realització d'aquestes actuacions a inicis de la setmana.

A partir dels informes d'auditoria realitzats, el contractista adjudicatari haurà de preparar el pla de treball detallat, amb identificació dels sistemes afectats, la proposta d'actuació i el calendari d'actuació previst. Aquest pla de treball serà la guia per seguiment de la prestació del servei.

El pla de treball s'haurà de presentar no més tard de 20 dies naturals des de la reunió de kick-off.

Tan bon punt s'aprovi el pla de treball s'iniciarà l'activitat sobre els sistemes afectats.

10 CARACTERÍSTIQUES DEL SERVEI SOL·LICITAT

10.1 DIMENSIONAMENT

El servei d'assistència sol·licitat es dimensiona en base a hores de personal tècnic per a la prestació de servei i que es consideren suficients per portar a terme l'objecte de la contractació. L'execució dels serveis pot requerir dedicació discontinua, fruit que l'aplicació dels canvis s'hagi de realitzar en horaris especials (fora horari laboral) o altres causes per motius de disponibilitat dels serveis d'AMSA.

El dimensionament d'hores totals per a la prestació del servei és de SIS-CENTES hores.

D'altra banda, el contractista adjudicatari ha de disposar dels perfils tècnics especialitzats amb solvència contrastada per a la realització dels treballs en els entorns indicats.

S'haurà de comptabilitzar el consum d'hores realitzar segons els perfils tècnics assignats al servei i d'acord amb les actuacions realitzades (al menys per sistema).

10.2 SERVEIS FORA D'HORARI

Les activitats, prèvia validació d'AMSA, realitzades fora de l'horari d'oficina establert (9:00h a 18:00h) i/o en caps de setmana / festius, tindran una consideració de 1,5 hores de servei normal, a efectes de facturació.

PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

10.3 REQUERIMENTS DE L'EQUIP CONSULTOR

L'equip consultor proposat pel licitador haurà de tenir expertesa i capacitat provada en l'operació de sistemes per als entorns de sistemes indicats, a més dels coneixements i habilitats en la utilització d'eines de programari per a realització de les tasques encomanades.

A més a més, es valorarà positivament que l'equip de tècnics assignats al projecte tingui coneixements en aspectes com ara:

- Coneixements avançats en "hacking ètic" i l'ús d'eines associades.
- Capacitat per entendre arquitectures de sistemes complexes i les seves dependències, a nivell tècnic i funcional
- Coneixement en comunicacions TCP/IP, protocols de comunicacions IT/OT, funcions de seguretat de sistemes, etc
- Experiència en anàlisi i diagnòstic de vulnerabilitats de sistemes TIC (CVE).
- Es valorarà certificacions relacionades tant en l'àmbit de sistemes com de ciberseguretat.

10.4 MODEL DE RELACIÓ

El model de relació s'establirà a dos nivells:

- Comitè de Direcció del projecte:
 - Director TIC & Transformació Digital d'AMSA
 - Director de Projecte del contractista adjudicatari
- Comitè de Seguiment:
 - Responsable Tècnic del departament de SI d'AMSA
 - Cap de projecte del contractista adjudicatari

Donada la durada del servei es preveu que hi hagi una interacció setmanal a nivell del comitè de seguiment, a mode de supervisió del servei.

El comitè de direcció es reunirà mensualment i/o sota demanda.

10.5 GARANTIES

Les intervencions realitzades en els sistemes d'informació gaudiran d'un període de 15 dies naturals enfront incidències. En el cas d'incidències relacionades com a resultat de la intervenció realitzada, el prestador del servei les haurà d'atendre a la màxima celeritat i sense que això representi dedicació addicional en hores (inclús en festius i/o caps de setmana).

11 DURADA DE CONTRACTE I TERMINIS

La durada màxima per a la prestació del servei és de SIS (6) mesos, des de la data de signatura del contracte.



PPT - ASSISTÈNCIA TÈCNICA D'EXECUCIÓ DEL PLA DE CIBERSEGURETAT PER AL PROJECTE PRTR, PER AIGÜES DE MANRESA S.A. PERTE DIGITALITZACIÓ DEL CICLE DE L'AIGUA EN EL MARC DEL PRTR . EXPEDIENT LICITADOR NÚMERO: 11632

11.1 TERMINI MÀXIM PER AL KICK-OFF DEL SERVEI

El contractista adjudicatari disposarà d'una màxim de QUINZE (15) dies naturals, a partir de la signatura del contracte per tal de realitzar el kick-off del projecte, on entre d'altres es concretarà:

- a) Equip professional assignat al projecte i interlocutors.
- b) Intercanvi de documentació per a realització del pla de treball i resolució de dubtes.
- c) Aspectes funcionals, tècnics i replantejaments a considerar.
- d) Altres consideracions a tenir en compte d'acord amb l'oferta adjudicatària.

11.2 TERMINI MÀXIM PER A INICI DE LA PRESTACIÓ DEL SERVEI

El servei pròpiament dit s'iniciarà a partir de la validació del pla de treball, que el contractista adjudicatari presentarà no més tard de VINT (20) dies naturals des del kick-off del projecte.

Manresa, a la data de la signatura electrònica.

Abel-Joel Agelet Nonell
 Director TIC & Transformació Digital