PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA CONTRACTACIÓ DE SERVEIS DE CIBERSEGURETAT I L'ADQUISICIÓ D'UN TALLAFOCS PER A L'ORGANISME DE GESTIÓ TRIBUTÀRIA DE LA DIPUTACIÓ DE BARCELONA.

Expedient núm.: ORGT/2025/0035517

CONTINGUT

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.
Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.
Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

1. OBJECTE.

L'Organisme de Gestió Tributària de la Diputació de Barcelona (ORGT) és un organisme autònom local de la Diputació de Barcelona, dotat de personalitat jurídica pròpia, que té com a principal finalitat l'exercici de les funcions i potestats de gestió, inspecció i recaptació de tributs i altres ingressos de dret públic per delegació o encàrrec de gestió de les administracions públiques de Catalunya i dels ens públics que en depenen.

Un dels objectius de l'ORGT és l'assoliment d'un bon nivell de ciberseguretat, que maximitzi la disponibilitat dels seus serveis i l'autenticitat, confidencialitat, integritat i traçabilitat de la informació que emmagatzema, processa i transmet. Per aconseguir-ho cal millorar el nivell de ciberseguretat actual de l'ORGT ampliant la monitorització de la ciberseguretat, la detecció primerenca d'incidents, l'anàlisi de les amenaces i vulnerabilitats, i optimitzant la capacitat de detecció, contenció, erradicació i recuperació davant de qualsevol possible incident.

L'objecte d'aquesta licitació és:

- Contractar un servei de Centre d'Operacions de Seguretat (SOC, de l'anglès Security Operations Center) amb capacitats d'Equip de Resposta a Incidents (CSIRT, de l'anglès Computer Security Incident Response Team) que doni serveis de seguretat gestionada a l'ORGT.
- Actualitzar la solució actual de detecció i resposta a incidents (EDR, de l'anglès Endpoint Detection and Response), anomenada Cortex XDR cap a la solució de gestió, monitorització i automatització de processos de Ciberseguretat, anomenada Cortex XSIAM.
- Implantar un servei de tallafocs d'aplicacions web (WAF, de l'anglès Web Application Firewall), per a protegir la seu electrònica de l'ORGT.
- Implantar un servei de gestió d'accessos privilegiats (PAM, de l'anglès Privileged Acces management).
- Implantar un servei de conscienciació en ciberseguretat als empleats de l'ORGT.
- Renovar el tallafocs perimetral PA3220 a la nova versió comercial PA3410.

2. SITUACIÓ ACTUAL.

Per a dur a terme les seves funcions, l'ORGT disposa d'una infraestructura informàtica i de comunicacions redundant, allotjada en els dos centres de processament de dades (CPD) situats a la ciutat de Barcelona i que treballen en mode actiu-passiu.

L'ORGT dona servei a 1000 empleats distribuïts en una xarxa d'unes 100 oficines interconnectades amb els dos Centres de Processament de Dades (CPD) mitjançant

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

línies de comunicacions d'alta velocitat, a 4.000 usuaris dels ajuntaments (400 d'ells simultanis) que accedeixen a través d'internet a l'aplicació de gestió tributària, i als contribuents dels municipis de la província de Barcelona que accedeixen a la seu electrònica de l'ORGT.

Totes les comunicacions estan protegides per un doble tallafocs de nova generació de diferents fabricants. El tallafocs intern és un clúster de 2 nodes PA3220 (amb nom FWORGT), del fabricant Palo Alto Networks, que està allotjat en els CPDs de l'ORGT i l'extern és un clúster de 2 nodes Fortigate FG6301F del fabricant FortiNet (amb nom FWVDF), allotjat en el núvol i gestionat per l'operador de comunicacions.

L'ORGT comparteix amb la Diputació de Barcelona (DiBa) un sistema per evitar atacs de denegació de servei (antiDDoS, de l'anglès Distributed Denial of Service), que també es troba allotjat en el núvol de l'operador de comunicacions.

El tallafocs intern FWORGT interconnecta 11 xarxes mitjançant un agrupament de 2 interfícies de 10Gbps. La seva política de seguretat està formada per 600 regles de seguretat, 200 regles de traducció d'adreces i 6 túnels IPSEC.

El tallafocs FWORGT disposa de les següents subscripcions, que finalitzen la seva vigència el 28/9/26:

- Advanced URL Filtering,
- Advanced DNS Security,
- GlobalProtect,
- Advanced Threat Prevention i
- Advanced Wildfire

Els serveis de l'ORGT s'ofereixen des de 150 servidors virtualitzats amb sistema operatiu Windows Server 2012R2 o superior, que s'executen en hipervisors VmWare Vsphere ESXi 8.0 U3. Els servidors estan protegits contra programari maliciós mitjançant l'EDR Cortex XDR, del Fabricant Palo Alto Networks.

Els llocs de treball de l'ORGT són 1000 portàtils que es connecten a una de les 2000 sessions d'escriptoris virtuals (VD, de l'anglès *Virtual Desktop*) que s'executen en hipervisors VmWare Vsphere ESXi 8.0 U3. Mil sessions s'executen en el CPD actiu i les altres mil estan en repòs en el CPD passiu, esperant a donar servei en cas de contingència. Els VD són no-persistents i tenen instal·lat l'EDR Cortex XDR.

L'ORGT disposa de dues sondes de xarxa que permeten detectar activitat maliciosa en el trànsit de dades de la xarxa d'àrea local (LAN, de l'anglès Local Area Network) de servidors i a la xarxa LAN de la zona desmilitaritzada (DMZ, de l'anglès Demilitarized Zone).

L'ORGT té contractat un SOC que realitza les següents tasques:

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- Monitorització de la ciberseguretat, detecció i anàlisi d'incidents i amenaces.
- Detecció, anàlisi i gestió de vulnerabilitats.
- Administració, gestió, manteniment i monitorització de la infraestructura de ciberseguretat.
- Gestió i resposta a incidents de ciberseguretat.

El SOC actual es recolza en un SIEM (de l'anglès, Security Information and Event Management) del model QRadar del fabricant IBM, que correla els esdeveniments de vàries fonts d'informació, com són el tallafocs, les sondes de xarxa, alguns servidors i els EDR, que permet la detecció de possibles activitats malicioses.

La gestió de la infraestructura al núvol (FWVDF i sistema antiDDoS) la duu a terme l'operador de comunicacions.

3. ABAST I DESCRIPCIÓ DEL SERVEI.

L'abast del servei és la contractació d'un Centre d'Operacions de Seguretat (SOC, de l'anglès Security Operations Center) amb capacitats d'Equip de Resposta a Incidents (CSIRT, de l'anglès Computer Security Incident Response Team) que doni serveis de seguretat gestionada a l'ORGT.

Els serveis que el SOC durà a terme són els següents:

- Monitorització de la ciberseguretat, detecció i anàlisi d'incidents i amenaces.
- Detecció, anàlisi i gestió de vulnerabilitats.
- Administració, gestió, manteniment i monitorització de la infraestructura de ciberseguretat.
- Gestió i resposta a incidents de ciberseguretat.

El SOC haurà d'estar fonamentat en l'ús de la solució Cortex xSIAM, que és una solució de gestió, monitorització i automatització de processos de ciberseguretat, especificada en l'apartat 4.2.

El SOC sol·licitat té la particularitat que un dels seus integrants, al que anomenem Referent Tècnic, estarà dedicat de manera exclusiva a l'ORGT. Amb aquesta mesura, el SOC disposarà d'un millor coneixement de la infraestructura i necessitats de l'ORGT i així podrà aportar un millor i més àgil servei. El detall de les tasques que durà a terme el Referent Tècnic es troben recollides a l'apartat 5.6 del present Plec.

A més del servei de SOC, l'ORGT vol millorar les mesures preventives de ciberseguretat que té implantades. Per això renovarà el tallafocs perimetral, aparell que realitza el filtrat de les comunicacions d'entrada i sortida a l'ORGT, implantarà un

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

servei de tallafocs d'aplicacions web, WAF (de l'anglès Web Application Firewall.) i implantarà una solució de gestió d'accessos privilegiats (PAM, de l'anglès Privileged Access management). Aquestes millores estan detallades als apartats 6, 7 i 8 respectivament.

L'element més important de la cadena de seguretat i que pot evitar més incidents és l'usuari final, per això el contractista haurà d'implantar un servei de conscienciació en ciberseguretat pels empleats de l'ORGT, detallat a l'apartat 9.

4. SERVEI DE CENTRE D'OPERACIONS DE SEGURETAT (SOC).

4.1. PRINCIPIS DEL SERVEI.

El contractista es fa responsable de la ciberseguretat de l'ORGT, per tant caldrà que aporti proactivitat i proposi de manera continua millores en la ciberseguretat dels sistemes d'informació i serveis de l'ORGT.

Els sistemes d'informació de l'ORGT estan categoritzats com de categoria mitja en l'Esquema Nacional de Seguretat (ENS).

El contractista durà a terme el servei de SOC seguint les normes, instruccions, guies i procediments elaborats pel CCN-CERT (Centro Criptológico Nacional – Computer Emergency Response Team).

Els desplaçaments, dietes i qualsevol altra despesa associada estarà inclosa en el servei i no suposarà major cost per a l'ORGT.

Els tècnics de la DSI tindran accés a les consoles de gestió dels serveis subministrats en el present contracte.

4.2. SOLUCIÓ DE GESTIÓ, MONITORITZACIÓ I AUTOMATITZACIÓ DE PROCESSOS DE CIBERSEGURETAT.

L'ORGT actualitzarà la solució EDR anomenada Cortex XDR i el servei de SIEM ofert en una plataforma Qradar, a l'evolució comercial anomenada CORTEX xSIAM (codi PAN-XSIAM-BASE-ENT-PLUS) i que és una solució de gestió, monitorització i automatització de processos de ciberseguretat.

El Cortex xSIAM emmagatzemarà els esdeveniments rebuts de les fonts d'informació que la DSI consideri oportuns, fins un màxim de 100 Gigabytes d'ingesta diària (codi PAN-XSIAM-BASE-GB), i cercarà patrons de possibles ciberatacs. A l'inici del servei les fonts d'informació que enviaran esdeveniments al magatzem del Cortex xSIAM seran les següents:

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- 1250 agents de Cortex xSIAM, instal·lats als escriptoris virtuals i servidors.
- Tallafocs intern (FWORGT), detallat a l'apartat 6.
- Tallafocs extern (FWVDF).
- Tallafocs d'aplicacions web (WAF) de l'apartat 7
- Dos balancejadors de càrrega Citrix Netscaler.
- Tres controladors de domini (DC, de l'anglès Domain Controller) Microsoft Windows de l'ORGT.
- Dos servidors de DNS (de l'anglès, Domain Name System).
- Vuit servidors de la DMZ (de l'anglès, DeMilitarized Zone).
- Dues sondes de xarxa.

El contractista aportarà servei de suport del fabricant de la solució de gestió, monitorització i automatització de processos de ciberseguretat (codi PAN-XSIAM-PREM-SUCCESS).

Els licitadors proposaran el preu d'ampliació per protegir 1 agent de CORTEX xSIAM addicional.

4.3. SERVEI REGULAR.

4.3.1. MONITORITZACIÓ DE LA CIBERSEGURETAT, DETECCIÓ I ANÀLISI D'INCIDENTS I AMENACES.

El servei de monitorització de seguretat es durà a terme en modalitat 24x7 i té com a objectiu la detecció de qualsevol amenaça potencial o efectiva en la ciberseguretat de l'ORGT que pugui ser detectada en base a l'anàlisi continu dels esdeveniments o alertes de seguretat reportats pels sistemes d'ORGT. Aquest servei es fonamenta en l'ús de la solució de gestió, monitorització i automatització de processos de ciberseguretat que ha estat detallada a l'apartat 4.2.

Aquest servei, ha de realitzar:

- Monitorització continua dels esdeveniments i alertes en temps real generats per les fonts d'informació que envien els seus esdeveniments de seguretat a la solució gestió, monitorització i automatització de processos de ciberseguretat.
- Detecció, identificació i classificació dels possibles incidents de seguretat i recol·lecció d'evidències necessàries per l'anàlisi posterior.
- Priorització de la resolució dels incidents en funció de la seva perillositat real i el seu impacte.
- Notificació al SOC i al Referent Tècnic (5.6), amb descripció de l'incident detectat i la seva categorització.
- Anàlisi complert dels incidents tenint en compte totes les possibles fonts d'informació (evidències, anàlisi de vulnerabilitats, altres incidents,

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Indicadors de compromís, etc.), per a obtenir l'impacte de l'incident, actius afectats, nivell de compromís del servei i qualsevol informació que permeti optimitzar la contenció, mitigació i erradicació de l'incident.

- Proposar un pla de contenció, mitigació i recuperació de l'incident detectat en base a procediments establerts i amb l'objectiu de resoldre l'incident el més aviat possible i amb totals garanties.
- Elaborar anàlisi preliminar dels incidents.
- Gestió de l'escalat dels incidents de nivell de perillositat molt alt (L4) (5.7) o els que la DSI consideri oportú, a l'equip especialitzat de resposta a incidents (CSIRT) amb tots els recursos necessaris.
- Coordinar l'execució dels plans de contenció, mitigació i recuperació fins que es doni per tancat l'incident, amb tot l'equip involucrat al mateix, sota la supervisió de la DSI.

4.3.2. DETECCIÓ, ANÀLISI I GESTIÓ DE VULNERABILITATS.

L'objectiu del servei és tenir un mecanisme per detectar i contrarestar les vulnerabilitats que puguin haver als sistemes d'ORGT, així com poder fer un seguiment del cicle de vida de les vulnerabilitats detectades (detecció, correcció i verificació).

Aquest servei durà a terme:

- La supervisió de les noves vulnerabilitats descobertes a nivell mundial i comprovació si afecten als actius d'ORGT.
- La detecció i identificació de vulnerabilitats mitjançant eines especialitzades.
- La notificació a la DSI de les vulnerabilitats detectades.
- La proposta de correcció o mitigació de les vulnerabilitats.
- El seguiment de la correcció de les vulnerabilitats amb un procés de gestió del cicle de vida de la vulnerabilitat en el que es verificarà si s'han fet les correccions adients i si aquestes han solucionat les vulnerabilitats detectades.

Les vulnerabilitats detectades hauran de ser classificades i documentades d'acord als organismes especialitzats i bases de dades de coneixement com son CVE (Common Vulnerabilities and Exposures) i CWE (Common Weakness Enumeration) i fent servir el mètode de càlcul CVSS (Common Vulnerability Scoring System) per a classificar la seva criticitat. S'haurà de facilitar la lectura i la comprensió de les debilitats trobades mitjançant aquest servei.

Com consideracions generals de les anàlisis de vulnerabilitats s'haurà de tenir en compte que:

- No es realitzaran atacs o proves de denegació de servei.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- S'hauran de preveure possibles impactes en el servei deguts a les accions portades a terme durant les anàlisis. S'hauran de notificar a la DSI abans de dur-les a terme, per programar-les i acordar les condicions de les execucions, per no afectar els serveis.
- Es farà èmfasi en les recomanacions de les vulnerabilitats i errors de seguretat detectats prèviament però que encara no han estat corregits.
- En tota intervenció serà requerit que hi hagi un responsable de la DSI al corrent de les activitats realitzades, durant tot el temps de vida de l'anàlisi.
- Les proves realitzades, la descripció de vulnerabilitats trobades amb les evidencies i l'estudi de l'impacte en termes de confidencialitat, integritat i disponibilitat, i les recomanacions de seguretat per a resoldre o evitar les vulnerabilitats s'inclouran en l'informe de Gestió de les Vulnerabilitats (5.13)

4.3.2.1. Gestió de vulnerabilitats dels sistemes de base dels servidors.

El contractista realitzarà un anàlisi de vulnerabilitats setmanal dels servidors de l'ORGT, inicialment seran 250 servidors, mitjançant eines especialitzades de gestió integral, detecció i resposta a vulnerabilitats que permetin realitzar tan anàlisis dels actius directament des de la xarxa com anàlisis exhaustius mitjançant un agent i un usuari autenticat. El resultat d'aquestes anàlisis s'inclouran en l'informe de gestió de les vulnerabilitats (5.13).

Els servidors a analitzar disposen d'un dels següents sistemes operatius: Windows Server 2012R2 o superior, VmWare Vsphere ESXi 8.0 U3, Oracle Linux 5.15 i altres variants de Linux.

Si es detecten vulnerabilitats crítiques, el contractista ho comunicarà abans de 24 hores a la DSI, proposant mesures correctores.

La DSI pot demanar l'anàlisi de vulnerabilitats d'un servidor sota demanda, el contractista l'haurà de dur a terme abans d'una setmana i el corresponent informe es lliurarà abans de dues setmanes.

4.3.2.2. Gestió de vulnerabilitats de la xarxa LAN.

El contractista instal·larà dos escàners de xarxa (NIPS, de l'anglès Network Intrusion Prevention System) que realitzaran una prevenció en temps real d'atacs de ciberseguretat gràcies a l'anàlisi del trànsit de xarxa. Un dels escàners s'instal·larà a la xarxa de servidors públics, en la que hi ha la seu electrònica, el portal Citrix i altres servidors (10 servidors) i l'altra s'instal·larà a la xarxa de servidors interns en la que hi ha els controladors de domini, els servidors DHCP i altres servidors (20 servidors).

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

El resultat d'aquestes anàlisis del trànsit de xarxa s'inclouran en l'informe de gestió de les vulnerabilitats (5.13).

Si es detecten vulnerabilitats molt crítiques, el contractista ho comunicarà abans de 24 hores a la DSI, proposant mesures correctores.

4.3.2.3. Gestió de vulnerabilitats dels llocs web.

El contractista realitzarà proves d'intrusió (Pentesting, de l'anglès Penetration Testing) a llocs web de l'ORGT publicats a internet, en les que simularà de manera controlada un ciberatac. L'objectiu d'aquestes proves d'intrusió és la detecció de vulnerabilitats reals, comprendre el seu impacte potencial i proposar mesures de correcció abans que l'ORGT sigui víctima d'un atac real.

Les metodologies a seguir per realitzar les proves d'intrusió estaran alineades amb PTES (De l'anglès, Penetration Testing Execution Standard) i OSSTMM (de l'anglès, Open Source Security Testing Methodology Manual.

Les proves d'intrusió es realitzaran anualment a dos llocs web que decidirà la DSI durant el primer trimestre de l'any, seguint l'escenari de caixa gris, en el que es simula un atacant amb alguns coneixements de l'organització, i permet fer un anàlisi de la seguretat dels serveis web més profund que en el cas de l'escenari de caixa negra, en el que es simula un atacant sense cap coneixement de l'organització.

Les activitats a realitzar en les proves d'intrusió seran:

- Definició de l'abast i objectius.
- Recollida d'informació.
- Enumeració i anàlisi de vulnerabilitats.
- Explotació de les vulnerabilitats trobades.
- Activitats de post-explotació.

El contractista inclourà el resultat de les proves d'intrusió en l'informe de gestió de les vulnerabilitats (5.13). L'informe haurà de contenir els següents apartats

- Descripció detallada de les vulnerabilitats trobades.
- Proves de concepte realitzades.
- Valoració de l'impacte i risc.
- Recomanacions tècniques de correcció de les vulnerabilitats.
- Conclusions executives per a l'equip directiu.

4.3.2.4. Simulacre de ciberatac a l'organització.

El contractista realitzarà simulacres de ciberatac dissenyats per posar a prova la seguretat de l'organització, tot imitant les tàctiques, tècniques i procediments d'un adversari real. L'objectiu principal no és només identificar vulnerabilitats tècniques a un

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

servidor específic, com és el cas d'una prova d'intrusió, sinó també avaluar la capacitat de detecció, resposta i resiliència de l'organització davant d'amenaces persistents avançades (APT, de l'anglès Advanced Persistent Threat).

Es realitzaran dos simulacres de ciberatac: un en el transcurs del segon trimestre del segon any de contracte i l'altre durant el segon trimestre del quart any de contracte.

En aquests exercicis de seguretat ofensiva, també anomenats exercicis de Red Team, hi intervenen els següents actors:

- Red Team: Actua com un atacant, està format per especialistes en seguretat ofensiva, que intenta comprometre sistemes, robar dades o accedir a informació crítica sense ser detectat.
- Blue Team: És l'equip defensiu que protegeix, detecta i respon als incidents de seguretat de l'organització.
- White Team: Supervisa l'exercici, gestiona la coordinació i controla l'impacte per evitar conseqüències negatives reals durant la realització de l'exercici.

Els objectius de la realització d'un exercici de Red Team són:

- Comprovar si un atacant podria obtenir accés a informació sensible.
- Avaluar el temps de detecció i resposta del Blue Team.
- Detectar mancances en processos, eines de seguretat i entrenament del personal.
- Millorar la postura de ciberseguretat general.

El contractista inclourà el resultat de l'exercici de Red Team en l'informe de gestió de les vulnerabilitats (5.13). L'informe haurà de contenir els següents apartats:

- Resum Executiu.
- Abast i objectius.
- Metodologia usada.
- Cronologia de l'exercici.
- Vectors d'entrada i accés inicial.
- Moviment lateral i escalada de privilegis.
- Impacte aconseguit.
- Detecció i resposta: Avaluació del Blue Team.
- Recomanacions i millores.

4.3.3. ADMINISTRACIÓ, GESTIÓ, MANTENIMENT I MONITORITZACIÓ DE LA INFRAESTRUCTURA DE CIBERSEGURETAT.

El contractista haurà de donar servei d'administració, gestió, manteniment i monitorització a tota la infraestructura de ciberseguretat interna adquirida en el present contracte. El contractista es responsabilitzarà del seu correcte funcionament sempre sota la supervisió i aprovació de la DSI.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Aquest servei de manera general ha de cobrir, per la infraestructura de ciberseguretat interna:

- Manteniment dels equips: gestionar el contracte de manteniment i garanties amb els fabricants de l'equipament. Gestionar casos amb el fabricant, com per exemple la substitució de peces o de l'equipament complet. Accés a la base de dades de coneixement del fabricant.
- Supervisió de salut dels equips: Monitoritzar de forma permanent (24*7), l'estat de les variables de funcionament idònies per a cada dispositiu administrat. Aquestes variables de funcionament han de ser les necessàries per garantir el correcte funcionament dels equips (ús de CPU, ús de la RAM, espai de disc, espai dels sistemes de fitxers, taula de connexions, numero de sessions, etc.) i notificar si hi ha algun problema.
- Resolució de consultes: Resoldre qualsevol dubte que els tècnics de la DSI puguin plantejar referent a ciberseguretat, tan de sistemes administrats en el present contracte, com d'altres sistemes relacionats amb la ciberseguretat.
- Resolució de peticions de servei: realitzar les peticions de servei sobre els equips administrats així com la realització de tasques d'operació sol·licitades per la DSI.
- Realització de còpies de seguretat: Fer còpies de seguretat de la configuració de l'equipament gestionat per l'empresa contractista. Verificar la validesa de les còpies de seguretat.
- Actualitzacions del software dels dispositius: Realitzar les actualitzacions dels equips administrats, recomanades pel fabricant de l'equip. Es farà un seguiment de les versions dels equips i s'alertarà de les noves recomanacions d'actualització.
- Registre i control d'actuacions: Inventariar i enregistrar totes les actuacions realitzades als equips administrats i les motivacions que les han provocat.
- Revisió mensual de la infraestructura de ciberseguretat i elaborar informe que permeti conèixer l'estat actual de seguretat dels equipaments administrats, així com el número, el detall i l'estat de les peticions i els incidents, i la disponibilitat dels equips.

Pel que fa a la infraestructura de ciberseguretat al núvol (tallafocs FWVDF i equipament antiDDoS) , el SOC del contractista realitzarà les següents tasques:

- Interlocució amb el SOC de l'operador de comunicacions, per a dur a terme noves peticions.
- Seguiment dels incidents.
- Seguiment del servei ofert pel SOC de l'operador de comunicacions.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

4.3.4. GESTIÓ I RESPOSTA A INCIDENTS DE SEGURETAT.

L'ORGT pren totes les mesures preventives que estan al seu abast, tan a nivell tècnic, procedimental i personal, per assolir un alt nivell de ciberseguretat, però tot i així és susceptible que pateixi incidents de seguretat.

L'ORGT requereix, en cas de patir un incident de ciberseguretat de nivell de perillositat molt alt (L4) i els de nivell de perillositat inferior que la DSI consideri oportú, que aquest sigui atès per un equip de resposta a incidents (CSIRT, de l'anglès Computer Security Incident Response Team). (Nota: Els nivells de perillositat dels incidents es troben documentats a l'apart 5.7.)

El CSIRT haurà de proporcionar el suport i l'experiència necessaris per a dur a terme les tasques d'anàlisi, contenció, erradicació i recuperació de l'incident per minimitzar el seu impacte.

L'empresa contractista haurà de ser membre del fòrum FIRST (de l'anglès Forum of Incident Response and Security Teams) i de la Xarxa Nacional de SOCS en nivell plata. Ambdues entitats garanteixen que els seus membres disposen de les eines i coneixements necessaris per millorar les seves capacitats de prevenció, protecció, detecció i resposta a incidents.

Totes les tasques que el contractista hagi de realitzar per a analitzar, contenir, erradicar i recuperar d'un ciberincident de nivell de perillositat molt alt (L4) i els de nivell de perillositat inferior que la DSI consideri oportú, es consideraran que són serveis de resposta a incidents de molt alta perillositat (apartat 4.5).

4.3.5. CUSTÒDIA D'EVIDÈNCIES DIGITALS.

El contractista custodiarà durant 2 anys i usant els seus sistemes d'informació, totes les alertes e incidències de la solució de gestió, monitorització i automatització de processos de ciberseguretat. Aquestes alertes e incidències es guardaran seguint les recomanacions del CCN-CERT, per a que siguin vàlides com a evidències digitals en possibles investigacions judicials. En el Protocol d'Actuació (clàusula 5.2) es detallarà el procediment a seguir per a que el contractista entregui les evidències digitals d'un dia concret a l'ORGT amb un temps de resposta de dos dies.

4.4. SERVEIS ADDICIONALS.

La ciberseguretat és un entorn en constant canvi i per això és difícil preveure totes les necessitats que tindrem en els propers anys. Per a donar resposta als possibles imprevistos, la DSI considera necessari contractar una bossa d'hores de tècnic per executar tasques relacionades amb la ciberseguretat que no estiguin previstes en el servei regular (4.3). A aquestes tasques les anomenem serveis addicionals.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Els serveis addicionals es duran a terme sota demanda i seguint les directrius de l'apartat 5.9

4.5. SERVEIS DE RESPOSTA A INCIDENTS DE MOLT ALTA PERILLOSITAT.

Per a donar resposta als possibles incidents de nivell de perillositat molt alt (L4) i els de nivell de perillositat inferior que la DSI consideri oportú, l'ORGT considera necessari contractar una bossa d'hores d'equip de resposta a incidents (CSIRT) per executar tasques relacionades amb l'anàlisi, contenció, erradicació i recuperació de incidents.

El següent és un llistat orientatiu de possibles serveis de resposta a incidents de molt alta perillositat que pot ser necessari dur a terme, en resposta a un incident, durant la vigència del contracte:

- Tasques de contenció per minimitzar l'impacte de l'incident.
- Tasques de mitigació i erradicació de l'incident.
- Tasques de recuperació dels serveis afectats per l'incident.
- Suport a les tasques que realitzarà la DSI com a resposta a l'incident.
- Coordinació durant l'incident amb la DSI i totes les parts que puguin estar involucrades, com per exemple: Diputació de Barcelona, operador de telecomunicacions i organismes oficials als que calgui reportar.
- Anàlisi de codi maliciós per identificar les seves capacitats (vectors d'entrada, tècniques d'ofuscació, mètodes de propagació, tècniques d'exfiltració, etc.), obtenir els indicadors de compromís (IOC, de l'anglès Indicator of Compromise).
- Assistència tècnica jurídica en la comunicació de l'incident als organismes oficials que calgui (CCN-CERT, AEPD, etc...) i als afectats per un incident.

Quan es produeixi un incident de nivell de perillositat molt alt (L4) i els de nivell de perillositat inferior que la DSI consideri oportú, el contractista haurà de realitzar una anàlisi de l'incident i elaborarà Pla Preliminar de Resposta a l'Incident que contindrà les mesures per a contenir, mitigar i erradicar l'incident, i per a recuperar els sistemes afectats per l'incident. També contindrà la dedicació necessària del contractista per a dur a terme aquestes tasques.

El Pla Preliminar de Resposta a l'Incident es presentarà a la DSI en els terminis establerts a l'apartat 5.7.

Els serveis de resposta a incidents de molt alta perillositat detallats en el Pla Preliminar de Resposta a l'incident es consideraran finalitzats quan hagin estat validats per la DSI. El contractista els facturarà trimestralment en funció de la seva realització efectiva.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

5. PRESTACIÓ DEL SERVEI.

5.1. IMPLANTACIÓ DEL SERVEI

La implantació dels serveis de ciberseguretat del present contracte es duran a terme seguint les següents fases:

- **Fase 1.** A partir de la signatura del contracte i fins l'inici efectiu del mateix previst pel 1 d'agost de 2026, s'hauran de dur a terme les següents tasques:
  - Assignar responsable del servei i referent tècnic del servei des del primer dia de contracte.
  - Configurar la infraestructura de comunicació entre ORGT i el contractista (apartat 5.3).
  - Informar a la DSI dels canals de comunicació (apartat 5.4) que caldrà usar en el servei.
  - Elaborar el Pla d'Implantació, validat i acceptat per la DSI, que inclourà els mecanismes necessaris per executar la implantació del servei:
    - Reunions de coordinació i informació,
    - connectivitat a l'entorn,
    - planificació de la renovació del nou tallafocs,
    - planificació de la implantació del gestor de vulnerabilitats,
    - planificació de la implantació de les sondes de xarxa,
    - planificació de la implantació del servei WAF,
    - planificació de la implantació de la solució de gestió d'accessos privilegiats,
    - planificació de la implantació del servei de conscienciació.
  - Implantar la solució de gestió, monitorització i automatització de processos de ciberseguretat (apartat 4.2).
  - Elaborar el protocol d'actuació (apartat 5.2).
  - Renovar les subscripcions de llicències actuals del tallafocs FWORGT, detallades a l'apartat 2.
  - Instal·lar eina que permet consolidar els logs dels dos nodes del tallafocs.

- La **fase 2.** Dotze mesos de durada des de l'inici del contracte. En aquesta fase el contractista durà a terme:
  - Renovació tecnològica del tallafocs (apartat 6).
  - Implantació del gestor de vulnerabilitats (apartat 4.3.2.1),
  - Implantació de les sondes de xarxa (apartat 4.3.2.2),
  - Implantació del Servei de WAF (apartat 7).
  - Implantació de la solució de gestió d'accessos privilegiats (apartat 8.1)
  - Implantació del servei de conscienciació en ciberseguretat dels empleats de l'ORGT (apartat 9.1).

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

5.2. PROTOCOL D'ACTUACIÓ.

El contractista elaborarà, de manera consensuada amb la DSI, el Protocol d'Actuació. Aquest document és un recull dels procediments a seguir entre ORGT i el contractista per a dur a bon terme el servei de SOC.

El Protocol d'Actuació, com a mínim ha de detallar els següents aspectes:

- Descripció del servei i recursos humans dedicats al mateix.
- Contacte del Responsable del servei i del Referent Tècnic.
- Relació de tècnics de la DSI autoritzats a comunicar peticions i incidents.
- Classificació nivell de perillositat dels incidents de seguretat.
- Procediment de comunicació, tractament i notificació dels incidents.
- Procediment d'escalat dels incidents.
- Procediment de comunicació de peticions i consultes.
- Procediment de petició de serveis addicionals.
- Procediment de petició de serveis de resposta a incidents de molt alta perillositat.
- Tasques realitzarà el SOC.
- Tasques a realitzar en l'anàlisi de vulnerabilitats trimestral.
- Tasques que es realitzaran a les revisions periòdiques mensuals.
- Contingut de l'informe de seguiment del servei.
- Contingut de l'informe de gestió de les vulnerabilitats
- Acords de servei a assolir.

5.3. INFRAESTRUCTURA DE COMUNICACIÓ ENTRE CONTRACTISTA I ORGT.

L'accés remot a l'equipament objecte d'aquest contracte no pot dependre de la infraestructura de comunicacions de l'ORGT. Per tant, el contractista establirà una connexió remota entre el seu centre de gestió i cadascun dels dos CPDs de l'ORGT. Aquesta connexió inclou la provisió de línia, router i establiment d'un túnel xifrat extrem a extrem. Aquest router es connectarà directament a la consola del tallafocs.

El cost de les línies de comunicacions i llicències necessàries per a dur a terme la connexió remota van a càrrec del contractista.

És responsabilitat del contractista configurar adequadament els llocs de treball dels seus tècnics i la seva infraestructura de xarxa, per a poder connectar-se de manera segura a la infraestructura de l'ORGT.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

5.4. CANALS DE COMUNICACIÓ.

El contractista disposarà d'una aplicació web en la que es puguin donar d'alta les peticions i incidències, consultar la seva evolució i accedir als informes del servei. L'ORGT també podrà comunicar les peticions i incidències mitjançant correu electrònic o telèfon.

El tècnic referent disposarà d'accés a l'aplicació interna de gestió d'incidències de l'ORGT, anomenada U33.

5.5. RESPONSABLE DEL SERVEI.

L'empresa contractista nomenarà un Responsable del servei que respondrà davant l'ORGT de la qualitat del servei, vetllarà pel compliment dels compromisos adquirits i impulsarà el servei per millorar la ciberseguretat d'ORGT.

El Responsable del servei realitzarà com a mínim, les següents tasques:

- Convocar les reunions de seguiment del servei (5.12).
- Fer acta de les reunions de seguiment del servei (5.12).
- Vetllar per l'assoliment dels acords de servei.

5.6. REFERENT TÈCNIC DEL SERVEI.

L'empresa contractista designarà un Referent Tècnic del servei, assignat en dedicació exclusiva a l'ORGT durant tota la durada del contracte.

El referent tècnic durà a terme la seva activitat de manera presencial des de les dependències de l'ORGT, un mínim de dos dies setmanals, consensuats amb la DSI.

De manera no limitativa les tasques que haurà de realitzar el Referent Tècnic són les següents:

- Ser interlocutor principal davant d'ORGT per la gestió, l'escalat i la coordinació de les necessitats o incidents que puguin sorgir.
- Realitzar el primer nivell d'atenció de les incidències, peticions i consultes relacionades amb la ciberseguretat.
- Afegir fonts d'informació a la solució de gestió, monitorització i automatització de processos de ciberseguretat.
- Configurar casos d'ús a la solució de gestió, monitorització i automatització de processos de ciberseguretat.
- Traspassar les incidències, peticions i consultes que no estigui capacitat per resoldre o quan estigui massa ocupat, a la resta d'integrants del SOC.
- Realitzar qualsevol tasca del servei regular (apartat 4.3).

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- Gestionar les tasques del servei regular (apartat 4.3), els serveis addicionals (apartat 4.4) i els serveis de resposta a incidents de molt alta perillositat (apartat 4.5) sol·licitats al SOC, controlant els escalats i optimitzant les gestions internes del contractista per tal d'agilitzar la seva resolució.
- Supervisar totes les tasques que realitzi el contractista, fins i tot les que es portin a terme en horari nocturn o dies festius.
- Coordinar els tècnics de l'empresa contractista que intervinguin en qualsevol activitat del servei.
- Interlocució amb l'operador de comunicacions per realitzar canvis en la política de seguretat de la infraestructura de seguretat de l'ORGT al núvol.
- Interlocució amb la Direcció de Serveis de Tecnologies i Sistemes Corporatius de la Diputació de Barcelona per realitzar canvis necessaris per ORGT, en la política de seguretat de DiBa.
- Interlocució amb qualsevol proveïdor de l'ORGT, de temes relacionats amb la Ciberseguretat.
- Dur a terme activitats mitigadores i correctives de vulnerabilitats detectades en les anàlisis de vulnerabilitats.
- Proposar, gestionar i dur a terme millores del servei.
- Elaborar protocols tècnics i operatius de resposta a incidents.
- Elaborar els informes de seguiment del servei.

El Referent Tècnic haurà de disposar de telèfon mòbil i estar disponible a atendre trucades de les 8h a les 18h, els dies laborables a la ciutat de Barcelona. També rebrà, a qualsevol hora, les notificacions d'avís d'incident de molt alta perillositat (L4).

Esporàdicament es duran a terme activitats que caldrà realitzar en horari de mínima afectació als serveis que ofereix l'ORGT, en horari nocturn o festiu. El Referent Tècnic haurà de realitzar o supervisar aquestes tasques.

L'empresa contractista no caldrà que substitueixi al Referent Tècnic quan estigui de vacances o afectat per una incapacitat temporal inferior a dues setmanes. Les seves funcions les assumirà el SOC durant la seva absència.

5.7. GESTIÓ D'INCIDENTS.

El contractista seguirà la metodologia del CCN-CERT pel que fa a la gestió i resposta a incidents de ciberseguretat, detallada en les guies CCN-STIC-403 "Gestión Incidentes de Seguridad Informáticos" i CCN-STIC-817 "Esquema Nacional de Seguridad. Gestión de Ciberincidentes".

Tenint en compte el document CCN-STIC-817 els possibles incidents soferts per l'ORGT són classificats amb els següents nivells de perillositat real:

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- Nivell baix (L1).
- Nivell mig (L2).
- Nivell alt (L3).
- Nivell molt alt (L4).

Els únics incidents considerats de molt alta perillositat (L4) que pot patir l'ORGT, són les amenaces persistents avançades (APT, de l'anglès Advanced Persistent Threat). Per aquests incidents i els que la DSI consideri oportú, el SOC activarà l'equip de resposta a incidents de ciberseguretat (CSIRT) i s'aplicaran els acords de servei per a incidents de molt alta perillositat (L4).

La DSI comunicarà al SOC els incidents que detecti classificats en un dels 4 nivells de perillositat. Els incidents detectats pel servei regular del SOC (4.3.1) seran categoritzats de la mateixa manera per l'empresa contractista.

Per mesurar els acords de nivell de servei, tindrem en compte les següents definicions:

- Temps de notificació de l'incident: És el temps transcorregut entre la detecció de l'incident pel sistema de monitoratge fins que el contractista ho notifica a la DSI.
- Temps d'anàlisi preliminar: És el temps transcorregut entre la detecció de l'incident pel sistema de monitoratge o la comunicació de l'incident al contractista fins que l'empresa contractista entrega informe amb l'anàlisi preliminar de l'incident i presenta pla preliminar de resposta a l'incident.
- Horari de servei: És l'interval horari on es comptabilitzaran els acords de nivells de servei.

Els acords de nivell de servei establerts en la gestió dels incidents, depenent de la seva perillositat són:

- Incidents de perillositat baixa (L1) i incidents de perillositat mitja (L2). El temps de notificació de l'incident és d'un dia i el temps de l'anàlisi preliminar és de 2 dies tenint en compte que l'horari de servei és de 8h a 18h els dies laborables a la ciutat de Barcelona.
- Incidents de perillositat alta (L3). El temps de notificació de l'incident és de quatre hores i el temps de l'anàlisi preliminar és de vuit hores tenint en compte que l'horari de servei és de 8h a 18h els dies laborables a la ciutat de Barcelona.
- Incidents de perillositat molt alta (L4). El temps de notificació de l'incident és d'una hora i el temps de l'anàlisi preliminar és de quatre hores tenint en compte que l'horari de servei és 24x7.

Una incidència estarà resolta si està plenament documentada i té el vistiplau funcional i tècnic de la DSI.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Pels incidents de perillositat molt alta (L4) i els que la DSI consideri oportú es durà a terme un informe d'anàlisi de l'incident, que com a mínim contindrà:

- Data i hora de detecció
- Data i hora de notificació.
- Data i hora de resolució i tancament.
- Nivell de perillositat de l'incident.
- Causa de l'incident.
- Resum de les accions recomanades per mitigar, contenir i erradicar l'incident, i per recuperar els sistemes d'informació.
- Impacte de l'incident: Equips afectats, valoració en la imatge, afectació en la confidencialitat i integritat de la informació i afectació en la disponibilitat dels serveis.

5.8. GESTIÓ DE PETICIONS .

Els tècnics de la DSI autoritzats donaran d'alta peticions de canvi en la política de seguretat, mitjançant els canals de comunicació establerts (5.4) i el SOC serà responsable de proposar i implementar la solució més adient i segura, sota la supervisió de la DSI.

Tot i que es preveu un volum inferior a 400 peticions anuals, el contractista haurà d'atendre totes les peticions sol·licitades per la DSI.

Una relació no exhaustiva de possibles peticions és la següent:

- Canvi de paraula de pas d'accés als equips.
- Afegir o modificar una política del tallafocs.
- Afegir o modificar una política de traducció d'adreces (NAT, de l'anglès Network Address Translation) en el tallafocs.
- Crear un túnel IPSEC amb una empresa col·laboradora.
- Crear un túnel SSL-VPN amb una empresa col·laboradora.
- Afegir o modificar un cas d'ús a la solució de gestió, monitorització i automatització de processos de ciberseguretat.
- Configurar respostes automàtiques a esdeveniments a la solució de gestió, monitorització i automatització de processos de ciberseguretat.
- Forçar l'actualització de les signatures de malware en el tallafocs.
- Modificar l'abast de l'anàlisi de vulnerabilitats.
- Modificar la configuració del tallafocs d'aplicació web (WAF, de l'anglès Web Application Firewall).
- Modificar la configuració del gestor d'accessos privilegiats (PAM, de l'anglès Privileged Acces Management).
- Modificar la configuració del Servei de conscienciació en Ciberseguretat.

A criteri dels tècnics de l'ORGT, les peticions es classificaran en dos nivells de prioritat: normal i urgent.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Una petició estarà tancada si està plenament documentada i té el vistiplau funcional i tècnic de la DSI.

Els acords de nivell de servei establerts en la gestió de les peticions, depenent de la seva prioritat, serà:

- Peticions ordinàries. El temps de resolució d'aquestes peticions és de 8 hores tenint en compte que l'horari de servei és de 8h a 18h els dies laborables a la ciutat de Barcelona.
- Peticions urgents. El temps de resolució d'aquestes peticions és de 4 hores tenint en compte que l'horari de servei és de 24x7.

5.9. GESTIÓ DE SERVEIS ADDICIONALS.

Quan l'ORGT necessiti dur a terme alguna de les intervencions enumerades en l'apartat Serveis Addicionals 4.4, o qualsevol altra tasca que estigui relacionada amb la ciberseguretat i que no estigui inclosa en el servei regular (4.3), se li sol·licitarà al Referent Tècnic i aquest elaborarà una proposta de valoració que contindrà com a mínim:

- Descripció de la tasca a realitzar.
- Documentació a entregar en finalitzar la tasca.
- Perfil i dedicació del tècnic per a dur a terme la tasca.
- Planificació de dates en que es realitzarà la tasca.

El contractista lliurarà la proposta de valoració a la DSI en el termini de dues setmanes des de la data de la petició. Un cop rebuda la proposta de valoració, la DSI decidirà l'aprovació del servei addicional. Si s'aprova, es durà a terme d'acord amb el calendari presentat. Si no s'aprova, es desestimarà la seva implementació, es tancarà la petició i no suposarà cap cost per a l'ORGT.

Es considera que l'horari ordinari de realització dels serveis addicionals es de 8:00 a 18:00, (de dilluns a divendres, no festius), si bé esporàdicament es duran a terme activitats que caldrà realitzar en horari de mínima afectació als serveis que ofereix l'ORGT, en horari nocturn o festiu.

L'estimació de serveis addicionals a dur a terme en horari de mínima afectació és de 4 tasques anuals amb una dedicació aproximada de 40 hores. Aquest nombre és purament orientatiu i s'hauran de dur a terme totes les tasques addicionals en horari de mínima afectació sol·licitades.

Els serveis addicionals es consideraran finalitzats quan estiguin en producció, documentats i hagin estat validats per la DSI. El contractista els facturarà trimestralment en funció de la seva realització efectiva.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

5.10. REVISIONS PERIÒDIQUES.

Mensualment es realitzaran les següents comprovacions en l'equipament de Ciberseguretat:

- Anàlisi de les noves versions de programari de l'equipament i de la necessitat d'aplicar-les.
- Anàlisi d'actualitzacions de seguretat de l'equipament i de la necessitat d'aplicar-los.
- Anàlisi del rendiment dels dispositius a fi de detectar necessitats d'escalat de l'equipament.
- Anàlisi de la política de seguretat dels tallafocs.
- Anàlisi de la configuració del WAF.
- Anàlisi de la configuració de la solució de gestió, monitorització i automatització de processos de ciberseguretat.
- Anàlisi de les amenaces i incidents de seguretat publicats pels CERT (Equips de resposta a Incidents) com p.e. INTECO-CERT, CCN-CERT o CESICAT-CERT. Comprovar si l'ORGT està afectat per aquestes amenaces i si és necessari, proposar les mesures preventives adequades.

El resultat d'aquestes tasques s'inclouran en l'informe mensual de seguiment del servei.

5.11. INFORME DE SEGUIMENT DEL SERVEI.

El referent tècnic del servei elaborarà un informe mensual on figurarà l'evolució de tots els serveis prestats en el present contracte i el presentarà a la DSI abans del dia 20 del següent mes. En l'informe com a mínim hi haurà de constar:

- Detall de totes les peticions obertes durant el mes, en que s'informarà:
    - Descripció.
    - Prioritat (urgent o ordinària).
    - Estat de la petició.
    - Data/hora en que s'ha comunicat la petició.
    - Data/hora en que un tècnic assumeix la resolució.
    - Data/hora en que ha quedat resolta.
    - Indicador (Sí/No) d'assoliment de l'ANS (Acord de nivell de servei).
    - Nombre d'hores de desviació de l'ANS. (Només cal informar-lo en les peticions que no assoleixen l'ANS).

- Detall de totes les incidències obertes durant el mes, en que s'informarà:
    - Descripció.
    - Grau de Perillositat de la incidència (L1, L2, L3 o L4).
    - Estat de la incidència.
    - Tasques realitzades per a resoldre-la.
    - Data/hora en que s'ha comunicat la incidència.
    - Data/hora en que un tècnic inicia l'anàlisi preliminar.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- Data/hora en que es finalitza l'anàlisi preliminar.
- Indicador (Sí/No) d'assoliment de l'ANS.
- Nombre d'hores de desviació de l'ANS. (Només cal informar-lo en les incidències que no assoleixen l'ANS).

- Detall dels serveis addicionals sol·licitats durant el mes i els pendents de finalització, en què s'informarà:
  - Descripció del servei addicional.
  - Data de sol·licitud del servei.
  - Data lliurament de la proposta de valoració.
  - Estat de realització del servei addicional.
  - Planificació. Data en que estarà en producció el servei.

- Enumeració de dies en que no hi ha hagut referent tècnic assignat al servei.

L'informe de seguiment del servei també contindrà els resultats de la revisió periòdica (5.10) i de la revisió de la infraestructura (4.3.3).

El contingut d'aquest informe es consensuarà amb la DSI i es detallarà en el Protocol d'Actuació.

5.12. REUNIONS DE SEGUIMENT.

El Responsable del servei convocarà mensualment una reunió de seguiment del servei en la que es tractaran, com a mínim, els següents temes:

- Incidències més habituals.
- Revisió dels serveis addicionals i dels serveis de resposta a incidents de molt alta perillositat portats a terme.
- Seguiment de la qualitat del servei.
- Millores possibles en el servei.
- Millores possibles a la infraestructura de ciberseguretat de l'ORGT.

El Referent Tècnic del servei assistirà a la reunió de seguiment i el Responsable del servei n'elaborarà una acta.

5.13. INFORME DE GESTIÓ DE LES VULNERABILITATS.

El referent tècnic elaborarà trimestralment un informe de gestió de les vulnerabilitats per poder avaluar l'estat de seguretat de la infraestructura de l'ORGT i el presentarà a la DSI durant el primer mes del següent trimestre,.

Aquest informe contindrà:

- Detall de l'anàlisi de vulnerabilitats dels sistemes de base dels servidors (4.3.2.1).

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- Detall de l'anàlisi del trànsit de xarxa (4.3.2.2).
- Detall de les proves d'intrusió dels llocs web (4.3.2.3).
- Detall del simulacre de ciberatac (4.3.2.4).

El contingut d'aquest informe es consensuarà amb la DSI i es detallarà en el Protocol d'Actuació.

5.14. DEVOLUCIÓ DEL SERVEI.

El penúltim trimestre de vigència del contracte, l'empresa contractista elaborarà el Pla de Devolució del Servei que inclogui els mecanismes necessaris per tal de traspassar competències, coneixement, documentació i les evidències digitals custodiades (4.3.5) a ORGT, a la finalització del contracte. Aquest pla haurà de ser aprovat per la DSI i contindrà com a mínim la següent informació:

- Configuració del tallafocs perimetral.
- Configuració i casos d'ús de la solució de gestió, monitorització i automatització de processos de ciberseguretat.
- Configuració del servei de WAF.
- Configuració de la solució de gestió d'accessos privilegiats.
- Configuració del servei de conscienciació en ciberseguretat.
- Evidències digitals dels últims 2 anys.

El cost d'elaboració del Pla de Devolució del Servei i tots els recursos necessaris per a dur-lo a terme, està inclòs dins el preu del servei.

6. RENOVACIÓ TALLAFOCS.

El contractista es farà càrrec del manteniment, la gestió i la subscripció de les llicències enumerades a l'apartat 2, del tallafocs perimetral actual, des de l'inici del contracte. A continuació es descriuen les característiques del nou tallafocs.

6.1. ESPECIFICACIONS DE MAQUINARI

L'ORGT necessita renovar el tallafocs intern FWORGT, que consisteix en un clúster de dos nodes del model PA3220 del fabricant Palo Alto Networks pel model actualitzat PA3410 del mateix fabricant i que està inclòs en el *Catálogo de Productos y Servicios de Seguridad de las Tecnologias de la Información y la Comunicación (CPSSTIC) elaborat pel Centro Criptológico Nacional (CCN)*.

El nou tallafocs disposa de 10 interfícies òptiques SFP+ de 10 Gbps, de 4 interfícies òptiques SFP28 de 25G i un rendiment en mode prevenció d'amenaces superior a 10Gbps.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

El contractista subministrarà els 2 nodes PA3410 (codi PAN-PA-3410), 4 transceptors SFP+ tipus 10GBase-SR (codi PAN-SFP-PLUS-SR) del fabricant Palo Alto Networks i 4 transceptors SFP+ tipus 10GBase-SR (codi RTXM228-551-C98) del fabricant Cisco Systems i compatibles amb els commutadors del CPD que són del model Cisco Nexus 9360, i les 4 fibres òptiques necessàries per interconnectar el nou tallafocs a la infraestructura de xarxa de l'ORGT.

6.2. SUBSCRIPCIÓ DE LLICÈNCIES.

El nou tallafocs PA3410 requereix les mateixes subscripcions que disposa el tallafocs actual, i aquestes són:

- Advanced URL Filtering (codi PAN-PA-3410-BND-CORESEC-5YR),
- Advanced DNS Security (codi PAN-PA-3410-BND-CORESEC-5YR),
- GlobalProtect (codi PAN-PA-3410-GP-5YR-HA2),
- Advanced Threat Prevention (codi PAN-PA-3410-BND-CORESEC-5YR) i
- Advanced Wildfire (codi PAN-PA-3410-BND-CORESEC-5YR).

També es requereix llicència del producte Panorama (codi PAN-PRA-25) per aconseguir que els logs dels dos nodes es consolidin en un únic entorn per així facilitar l'anàlisi forense dels incidents i l'elaboració d'informes.

6.3. IMPLANTACIÓ.

La renovació del nou tallafocs comportarà que el contractista haurà de dur a terme les següents tasques:

- Subministrament del maquinari.
- Subministrament de tot el cablejat necessari per realitzar la instal·lació (xarxa elèctrica i xarxa de dades.)
- Contractació de les subscripcions de llicències necessàries.
- Instal·lació de cada node del tallafocs en el corresponent CPD.
- Connexió dels nodes del tallafocs a la xarxa elèctrica i a la xarxa de dades.
- Migració de la configuració actual al nou tallafocs.
- Posar en producció el nou tallafocs durant un cap de setmana, amb un tall de servei menor a dues hores.
- Documentar les tasques realitzades.
- Formació dels tècnics de la DSI.
- Esborrat de dades dels nodes del tallafocs FWORGT.
- Trasllat dels nodes del tallafocs FWORGT a les dependències de l'ORGT.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

6.4. SERVEI DE GARANTIA

El contractista contractarà el servei de garantia del fabricant per tot el maquinari adquirit (codi PAN-SVC-BKLN-3410-5yr), a partir de la data de lliurament dels equips (6.3) i fins la finalització del contracte.

La garantia del fabricant permetrà:

- Accedir a les actualitzacions i pegats de seguretat de programari dels equips.
- Accedir a la base de dades de coneixement.
- Aportar peces de recanvi noves per a substituir les peces avariades.
- Aportar transceptors nous per a substituir els transceptors avariats.
- Gaudir d'un servei d'atenció i resolució de casos.

6.5. SERVEI DE MANTENIMENT

El servei de manteniment té per objectiu esmenar i reparar les incidències o avaries que sorgeixen en els equips físics i en la correcció de problemes derivats del funcionament incorrecte dels programes associats a l'equipament. El contractista durà a terme el servei de manteniment del tallafocs i per tant realitzarà les següents accions:

- Registrar les incidències,
- Seguiment de les incidències,
- Gestionar la garantia amb el fabricant.
- Diagnosticar i primer intent de resolució de la incidència,
- Configurar el nou maquinari.
- En el cas d'avaries hardware, s'enviarà un tècnic de camp a substituir les peces avariades, per les aportades pel fabricant.
- Aportar fibres de connexió entre l'equipament i la infraestructura de xarxa de dades.
- Aportar cables de connexió entre l'equipament i la xarxa elèctrica.
- La substitució dels transceptors i de les fibres que uneixen l'equipament a la infraestructura de xarxa.

El servei de manteniment tindrà les següents característiques:

- La comunicació dels incidents es realitzarà usant els canals de comunicació previstos a l'apartat 5.4.
- Servei d'assistència en modalitat 24 x 7.
- La mà d'obra, els desplaçaments, els recanvis, els costos derivats de la diagnosi, el desmuntatge de l'equip avariat, la configuració i la posada en marxa estan inclosos en el servei.
- Els recanvis usats seran els originals del fabricant.
- Nombre il·limitat d'incidents.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Pel que fa al nivell de servei que haurà de complir el servei de manteniment del tallafocs, es considera que haurà d'atendre dos tipus d'avaries:

- Normals. Avaries que afecten a un element de maquinari redundat del tallafocs actiu, o bé el tallafocs passiu pot assolir el servei del tallafocs actiu.
- Crítiques. Avaries que provoquen el tall del servei, com per exemple el tallafocs actiu pateix un problema i el passiu no entra en funcionament.

Per a les avaries normals s'haurà de complir:

- Temps de notificació de l'incident de 4 hores.
- Temps de substitució d'un node avariat de 8 hores.

Per a les avaries crítiques s'haurà de complir:

- Temps de notificació de l'incident d'una hora.
- Temps de resposta presencial, si es requereix, de 2 hores.

7. SERVEI DE TALLAFOCS D'APLICACIÓ WEB (WAF).

L'ORGT necessita protegir la seva seu electrònica i altres serveis web de possibles atacs maliciosos duts a terme mitjançant trànsit HTTP i HTTPS. Per aconseguir-ho cal implantar un tallafocs d'aplicacions web (WAF, de l'anglès Web Application Firewall) que funciona com una capa intermediària entre els usuaris i els serveis web, i protegeix dels següents ciberatacs:

- SQL Injection. Intents d'injectar codi SQL maliciós per llegir, modificar o eliminar dades de la base de dades.
- Cross-Site Scripting (XSS). Inserció de scripts maliciosos dins de pàgines web per robar cookies, tokens de sessió,
- Cross-Site Request Forgery (CSRF). Fa que un usuari autenticat realitzi accions no desitjades en una aplicació on està autenticat.
- Command Injection. Inserció de comandes del sistema operatiu a través de camps d'entrada vulnerables.
- Path Traversal. Permet accedir a fitxers o directoris fora de l'arrel de l'aplicació.
- Session Hijacking. Captura i usa els tokens de sessió per suplantar usuaris legítims.
- HTTP Request Smuggling / Splitting. Manipulació de la manera en què els servidors interpreten les capçaleres HTTP per evadir controls de seguretat.
- Bots maliciosos. Xarxes d'ordinadors que recullen excessiva informació i extreuen dades.
- Brute-force i credential stuffing. Atac que realitza intents massius d'obrir sessió. Intenta provocar una denegació de servei.
- Altres atacs a serveis web que sorgeixin durant la vigència del contracte.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Les característiques del servei de tallafocs d'aplicació web a implantar són les següents:

- Servei ofert en mode SaaS (De l'anglès Software as a Service).
- Protegir 10 llocs web.
- Ampla de banda a protegir de 100Mbps.
- Bloquejar futures tècniques d'atac a llocs web.
- Integració amb la solució de gestió, monitorització i automatització de processos de ciberseguretat, detallat a l'apartat 4.2.

7.1. IMPLANTACIÓ.

La implantació del servei tallafocs d'aplicació web comportarà que el contractista haurà de dur a terme les següents tasques:

- Configurar en el WAF les aplicacions protegides.
- Redirecció del trànsit destinat als llocs web de l'ORGT cap al WAF.
- Aplicar polítiques de seguretat en el WAF.
- Posar en producció el WAF amb un tall de servei menor a dues hores.
- Documentar les tasques realitzades.
- Formació dels tècnics de la DSI.

L'administració, suport i monitorització del servei es duran a terme com a tasques incloses en el servei regular (4.3.3)

8. GESTOR D'ACCESSOS PRIVILEGIATS (PAM).

L'ORGT necessita protegir els usuaris amb rols crítics (administradors de sistemes, administradors de bases de dades, enginyers de xarxa, etc.) i per això vol implantar una solució de gestió d'accessos privilegiats (PAM, de l'anglès Privileged Access Management).

El PAM ha d'aportar les següents funcionalitats:

- Control d'accés privilegiat. Limita qui pot accedir a quines màquines, aplicacions i sota quines condicions.
- Gestió de credencials. Emmagatzema i gestiona contrasenyes privilegiades en una caixa forta virtual, amb rotació automàtica de contrasenyes.
- Sessió auditada i monitoratge en temps real. Registra les sessions d'accés privilegiat per detectar i respondre a accions sospitoses o no autoritzades.
- Elevació i delegació de privilegis. Permet concedir accés temporal o limitat segons la necessitat, sense compartir contrasenyes.
- Gravació de les sessions. Permet enregistrar les sessions.
- Descobriment de comptes d'usuari privilegiats.
- Importació de secrets emmagatzemats en un Keepass.
- Mesures de seguretat disponibles:

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

- Autenticació mitjançant multifactor.
- Còpia de seguretat xifrada i periòdica dels secrets.
- Generació d'un fitxer de recuperació per la restauració de l'entorn.
- Possibilitat de disposar d'una instància secundària preconfigurada en el CPD passiu.
- Mode emergència per accedir a les credencials en cas de desastre.

Les característiques de la solució PAM a implantar a l'ORGT són les següents:

- Solució instal·lada en alta disponibilitat als hipervisors VmWare Vsphere ESXi 8.0 U3 dels dos CPD de l'ORGT.
- Protegirà a 75 usuaris privilegiats: 40 interns i 35 externs.
- Protegirà l'accés a 200 servidors amb sistemes operatius Windows Server 2012R2 o superior, Oracle Linux 5.15 i VmWare Vsphere ESXi 8.0 U3.
- Protegirà l'accés a servidors de la DMZ.
- Integració amb el Directori Actiu.
- Integració amb la solució de gestió, monitorització i automatització de processos de ciberseguretat detallada a l'apartat 4.2.

8.1. IMPLANTACIÓ.

La implantació del gestor d'accessos privilegiats comportarà que el contractista haurà de dur a terme les següents tasques:

- Contractació de les subscripcions de llicències necessàries.
- Instal·lar el gestor d'accessos privilegiats a servidors virtuals de l'ORGT.
- Configurar el gestor d'accessos privilegiats:
  - Protegir l'accés dels administradors de sistemes i els tècnics de les empreses externes col·laboradores als servidors de l'ORGT.
  - Activar la rotació automàtica de contrasenyes.
  - Activar l'accés temporal amb aprovació.
  - Configurar totes les mesures de seguretat disponibles.
- Crear instància secundària preconfigurada en el CPD passiu.
- Documentar les tasques realitzades.
- Formació dels tècnics de la DSI.

L'administració, suport i monitorització del PAM es duran a terme com a tasques incloses en el servei regular (4.3.3)

9. CONSCIENCIACIÓ EN CIBERSEGURETAT.

El contractista portarà a terme un servei de conscienciació en ciberseguretat pels empleats de l'ORGT que disposi de les següents funcionalitats:

- Formació estructurada per nivells: Habilitats pràctiques agrupades en mòduls temàtics com contrasenyes, navegació web, correu electrònic, xarxes socials,

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

dispositius mòbils, dades confidencials, GDPR, entre d'altres. Cada tema s'ha de presentar en diversos nivells de dificultat adaptant-se al perfil de risc de cada empleat.

- Cursos principals i exprés: El curs principal proporciona una formació exhaustiva amb lliçons interactives, reforços, tests i simulacions de phishing. El curs exprés, en canvi, és una formació breu en format audiovisual, ideal per a refrescar coneixements o per a sessions ràpides.
- Aprenentatge progressiu i adaptat als coneixements assolits per l'empleat.
- Recordatoris periòdics per consolidar els coneixements.
- Simulacions de phishing: Es portaran a terme campanyes de phishing simulades amb plantilles personalitzables, permetent avaluar i millorar la capacitat dels empleats per detectar correus electrònics maliciosos.
- Tipologies de phishing: Les campanyes de phishing simularan atacs de les següents tipologies:
    - Phishing de clic en un enllaç
    - Phishing de descàrrega d'un document maliciós.
    - Phishing de captura de credencials.
    - Phishing d'escaneig de QR.
- Automatització completa: El servei de conscienciació estarà completament automatitzat, des de la programació de cursos fins a l'enviament de recordatoris i informes, reduint la càrrega administrativa.
- Visibilitat de l'evolució de la conscienciació en ciberseguretat:
    - Disponibilitat de quadres de comandament per disposar d'una visió en temps real.
    - Informes d'evolució de les campanyes de phishing.
    - Informes de la maduresa en ciberseguretat dels empleats, nivell de risc de l'empleat.
- La interfície d'usuari final i els continguts dels cursos han d'estar disponibles en català.

Les característiques del servei de conscienciació en ciberseguretat a implantar a l'ORGT són les següents:

- Dimensionar per 1100 empleats.
- Suport a l'idioma català. Totes els comunicacions amb els alumnes s'han de poder realitzar en català.
- Integrable amb el Directori Actiu.
- Integrable amb la solució de gestió, monitorització i automatització de processos de ciberseguretat detallada a l'apartat 4.2.
- El servei de conscienciació en ciberseguretat es pot recolzar en una solució a les instal·lacions pròpies o al núvol, però en ambdós casos ha de prendre les mesures de seguretat oportunes.
- El contractista aportarà totes les llicències necessàries.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

9.1. IMPLANTACIÓ

La implantació del servei de conscienciació en ciberseguretat comportarà que el contractista haurà de dur a terme les següents tasques:

- Instal·lació en els servidors virtuals de l'ORGT.
- Integrar amb el directori actiu.
- Segmentar els empleats segons el seu rol (administratius, tècnics i directius) i decidir la seva ruta de formació.
- Configurar el servei de conscienciació en ciberseguretat.
- Programar campanyes de phishing
- Configurar informes de seguiment.
- Documentar les tasques realitzades.
- Formació dels tècnics de la DSI.

L'administració, suport i monitorització de la solució de conscienciació en ciberseguretat es duran a terme com a tasques incloses en el servei regular (4.3.3)

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 27795df79cf27e4c089c Adreça de validació: https://seuelectronica.diba.cat

Metadades del document

Núm. expedient	ORGT/2025/0035517
Tipus documental	Plec de clàusules o condicions
Títol	Plec de prescripcions tècniques per la contractació de serveis de ciberseguretat i l'adquisició d'un tallafocs per a l'Organisme de Gestió Tributària de la Diputació de Barcelona

Signatures

Signatari		Acte	Data acte
Jordi Valls Moya (SIG)	Cap del Servei d'Explotació i Sistemes	Signa	03/12/2025 16:10

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
27795df79cf27e4c089c	https://seuelectronica.diba.cat	