PLEC DE PRESCRIPCIONS TÈCNIQUES QUE HA DE REGIR EL PROCEDIMENT PER A LA CONTRACTACIÓ DEL SERVEI D'IMPLEMENTACIÓ DEL CENTRE D'OPERACIONS DE CIBERSEGURETAT DE L'AJUNTAMENT D'ESPLUGUES DE LLOBREGAT (EXPT: 2023/12079/1408).

1 INTRODUCCIÓ

En la determinació de les prescripcions, s'han tingut en compte els art. 124 a 128 de la LCSP sobre definicions i regles per establir les prescripcions tècniques.

L'abast del servei és la implantació d'un servei d'operacions de ciberseguretat que millori les capacitats actuals de la seguretat informàtica de l'Ajuntament d'Esplugues de Llobregat a tots els nivells (proactiu, preventiu i reactiu) i en les disciplines més rellevants en l'àmbit de la ciberseguretat.

L'explotació del servei ha de permetre mantenir un equilibri entre la detecció d'alertes de seguretat i l'esforç necessari per solucionar-los i documentar-los.

2 OBJECTE DEL CONTRACTE

L'objecte d'aquesta licitació és la implantació d'un Centre d'Operacions de Seguretat, per donar resposta a les necessitats actuals de l'Ajuntament d'Esplugues de Llobregat en matèria de ciberseguretat, el manteniment dels sistemes d'informació existents i el desenvolupament dels plans estratègics en matèria TIC d'acord amb les prescripcions que es recullen al plec de prescripcions tècniques.

3 OBJECTIUS

L'objectiu de crear el SOC permet adoptar les mesures oportunes per gestionar els riscos de seguretat i notificar els incidents que tindrien un efecte pertorbador significatiu. Per aquest motiu, el SOC es realitzarà incorporant-se al LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces) que és una eina que millorarà la coordinació entre el CERT Governamental Nacional i l'Ajuntament.

Altres dels principals objectius d'aquest projecte és millorar les capacitats de prevenció, protecció, detecció i resposta davant d'incidents de ciberseguretat. Per això, l'Ajuntament treballa perquè els requisits de gestió dels incidents siguin acords a les seves capacitats. Perquè un desequilibri entre tots dos compromet la qualitat i/o la seguretat de la informació.

La millora en capacitats no és estanca i ha de tenir en compte que la informació i les activitats digitals incumbeixen a totes les àrees de l'Ajuntament. Per això es

treballarà per simplificar i minimitzar els actius necessaris. L'últim objectiu principal és mantenir les persones i els seus drets al centre de les actuacions en ciberseguretat. Les dades personals són un dels actius més valuosos de l'Ajuntament. I el projecte també es concentra a garantir-ne la protecció.

Desafortunadament, l'accés a les eines que comporten amenaces per a la informació estan a l'abast dels delinqüents cibernètics des de fa molt de temps i la protecció de les dades no pot ser una mera declaració sinó que s'han d'acompanyar de les inversions del projecte en mesures de seguretat. Atès que els tractaments es fan des d'equips informàtics, s'emmagatzemen en suports i es distribueixen per xarxes de dades, la protecció de tots els components del sistema d'informació són un objectiu primordial de l'Ajuntament. Precisament aquests components es veuen sota risc constant i apareixen constantment noves amenaces, tant des de dins de l'entitat com des de l'exterior.

4 ABAST

Els serveis principals que es formen part de l'abast d'aquest servei són:

- Desplegament efectiu del SIEM (Security Information and Event Management), actualment implantat a l'Ajuntament, a la totalitat del parc.
- Desplegament/integració de LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces). LUCIA és una eina desenvolupada pel CCN-CERT per a la Gestió de Ciberincidents a les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat. Amb ella es pretén millorar la coordinació entre el CERT Governamental Nacional i els diferents organismes i organitzacions amb què col·labora. La integració amb Lucia serà procedimental.
- Serveis d'anàlisi i resposta d'incidents de ciberseguretat, desastres, recuperació de les operacions després d'un incident de ciberseguretat, suport a les investigacions i els requeriments, el registre i el seguiment d'activitats.
- Recollir, analitzar i presentar informació de dispositius de xarxa i seguretat.
- Facilitats d'identificació d'accessos (logs).
- Detecció de vulnerabilitats i comprovació de compliment de polítiques de seguretat. Les vulnerabilitats seran a nivell de sistema operatiu i a nivell d'anàlisi de trànsit de xarxa per a un informe objectiu.
- Possibilitat d'incloure el context de l'activitat de la xarxa, el context dels

usuaris/actius, els registres d'aplicacions i la reducció d'incidents en alertes reals.

- Traçabilitat d'informació de la infraestructura objecte d'abast.
- Serveis de prevenció i contramesures, anàlisi continuada i tractament de les vulnerabilitats, recomanacions i suport.
- Serveis de monitorització contínua de logs i esdeveniments de seguretat, capacitats de detecció primerenca d'incidents i amenaces i vigilància digital.
- Serveis de suport a la gestió i operació del SOC.
- Cal configurar diferents panells d'informació, quadres de comandament, casos d'ús personalitzats i models d'informes en formats explotables externament.
- Informes periòdics de mètriques i indicadors, i tot allò que ajudi a millorar la governança de la ciberseguretat.
- Informes d'incidents de seguretat, l'adjudicatari haurà de lliurar un informe relatiu a l'incident en què inclourà les traces de detecció del mateix i les mesures que s'han pres per contenir o mitigar. El termini màxim per al lliurament de l'informe serà de 7 dies.

Descriure que l'entorn és Windows en clients i servidors, virtualització sobre vmware i synology d'emmagatzematge. Aquest és l'entorn a protegir, especialment pel que fa a Windows. Detallar els accessos externs a través de la intranet, correus electrònics, teamviewer, RDP i les debilitats actuals referents a què els usuaris són i seran administradors dels seus propis PCs, mentre duri aquest projecte. Concretament:

- Entorn d'usuaris: 300 PCs a 8 xarxes
- Entorn de servidors: 120 servidors a 12 xarxes, dels quals 110 són windows server, la resta linux
- Virtualització: VMWare ESXi 7 amb 8 host i VSAN
- Emmagatzematge secundari: 4 cabines Synology
- Principals vies d'accés remot: navegació per internet, recepció de correus electrònics, connexions remotes per TeamViewer i Anydesk, serveis http publicats pels servidors, i tots els serveis que dona l'ajuntament al ciutadà

Actualment l'ajuntament té sota suport i manteniment les llicències següents, necessàries per dur a terme els serveis aquí descrits. S'indica la data de

finalització del dit suport i manteniment de manera que serà responsabilitat de l'adjudicatari renovar-ne el manteniment i suport fins a la data de finalització del contracte adjudicat, incloent-hi les pròrrogues en cas de ser executades.

Producte.- SIEM SPLUNK

Instància Splunk Cloud SAAS dedicada a l'Ajuntament d'Esplugues amb el número d'entitlement (o contracte/o identificador) E-0028770

Capacitat de fins a 25Gb d'ingesta diària

Manteniment a incorporar des del primer dia de contracte.

********** **********

Producte.- ArcServer

Número de llicencia: 9080025

Codi Fabricant: MUPR0600MRWTB2E12C

Arcserve UDP Premium Edition - Managed Capacity per TB between 2 - 5 TB - One Year Enterprise Maintenance Renewal.

Quantitat: 2

Manteniment fins a 15/06/2025

********** **********

Producte: FortiAnalyzer-VM FortiCare Premium Support

1 Year FortiCare Premium Support (for 1-6 GB/Day of Logs)

Product Serial Number: FAZ-VM0000028463

Cobertura de suport de producte

Support Type Support Level Expiration Date

- Firmware & General Updates. Tipus de Suport: Web/Online. Finalitza el 31 de desembre del 2024
- Enhanced Support. Tipus de Suport: Premium. Finalitza el 31 de desembre del 2024
- Telephone Support. Tipus de Suport: Premium. Finalitza el 31 de desembre del 2024

********** **********

Producte: FortiGate-200F

1 Year Unified Threat Protection (UTP)

(IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)

Quantitat: 2

FG200FT920900267 fins a 14/01/2025

FG200FT920900264 fins a 13/01/2025

********** **********

5 DESCRIPCIÓ DETALLADA DELS SERVICIS DEL CENTRE D'OPERACIONS DE SEGURETAT (SOC)

Aquest servei se centra en l'execució d'activitats relacionades amb serveis SOC (Centre d'Operacions de Seguretat). El SOC s'activarà tan aviat com sigui necessari per assegurar que no hi ha minvament en el servei actual, i gestionarà i administrarà les vulnerabilitats i amenaces d'una forma proactiva i reactiva, mitjançant la monitorització de les xarxes de comunicació i equips que allotgen els sistemes informàtics , així com l'accés a les dades de l'Ajuntament. Igualment oferirà assessoria i plantejarà opcions innovadores per portar un control de les comunicacions i detecció de vulnerabilitats, amb l'objectiu que no es vegi afectat el servei als sistemes d'informació, tant des de l'interior de la xarxa de l'Ajuntament com des de l'exterior.

Les operacions de Ciberseguretat del Centre d'Operacions de Seguretat tindran els objectius següents:

- Garantir la prestació dels serveis i/o prestacions, d'acord amb la demanda esperada i d'acord amb els nivells acordats, garantint la planificació i els objectius de qualitat establerts.
- Documentar la informació necessària per al coneixement precís de l'inventari i l'estat de l'equip i les instal·lacions objecte d'aquest contracte, així com les actuacions que es duen a terme, per facilitar tant l'anàlisi del funcionament dels serveis com la presa de decisions destinades a corregir les desviacions sobre els objectius previstos.
- Servei de resposta a incidents (CSIRT) que proporcioni serveis i suport per prevenir, gestionar i respondre a incidents de seguretat de la

informació/ciberseguretat.

5.1 ACTIVITATS REQUERIDES

A continuació, es descriuen les activitats que conformen el conjunt del Servei de Seguretat Gestionada SOC 24x7 i que l'adjudicatari haurà de realitzar, sense que la relació que apareix a continuació pretengui descriure de manera exhaustiva les característiques del servei contractat, sinó les línies generals requerides per Ajuntament. Els requisits referits s'han d'entendre com a requisits mínims i de compliment obligat, i els licitadors poden millorar-los en les seves propostes. En qualsevol cas, les propostes han d'oferir informació detallada sobre les característiques particulars del servei projectat, incloent-hi l'equipament HW/SW requerit per a la prestació del servei, que ha d'estar explícitament descrit a la Proposta Tècnica.

L'adjudicatari haurà de desenvolupar i aportar els coneixements, les metodologies, els recursos humans i els tècnics necessaris per assegurar la prestació òptima del servei, així com mantenir un Quadre de Comandaments òptim per a la qualitat del Servei de Seguretat Gestionada.

L'adjudicatari s'obliga a guardar secret i a fer-lo guardar al personal que empri per a l'execució del contracte, respecte a tota la informació de l'Ajuntament, que amb motiu del desenvolupament dels treballs i serveis arribi al seu coneixement, no podent utilitzar-la per a si o per a una altra persona, entitat o signatura.

5.2 Detecció i prevenció

S'hauran d'establir els mecanismes de detecció i prevenció que el licitador consideri necessaris per a una prestació correcta del servei.

La solució proposada haurà d'incloure tots els elements HW i/o SW de detecció o prevenció que l'adjudicatari estimi necessaris per a la prestació del servei a part dels ja esmentats anteriorment (Firewall, SIEM, XDR i Seguretat Correu Electrònic, etc.).

No obstant això, els elements de seguretat actualment disponibles a l'Ajuntament, (Firewall, SIEM, XDR i Seguretat Correu Electrònic, etc.), hauran de ser emprats com a part de la solució tècnica proposada pel licitador, de cara a una eficient prestació d'aquest servei ampliant les funcionalitats que considerin oportunes dins del contracte i sempre que no entrin a Fi de Vida Útil (EOL) durant el contracte, cas en què hauran de ser substituïts arribat aquest moment, per part de l'Ajuntament. La configuració i actualització d'aquests elements anirà a càrrec de l' adjudicatari i haurà de respectar la funcionalitat actual dels mateixos.

Les activitats de detecció i prevenció cobriran almenys els aspectes següents:

- Analitzar, detectar i bloquejar atacs a aplicacions web però preferentment atacs interns i protocols de Windows: SMB, NETBIOS, NTLM, Kerberos, etc. La solució proposada haurà de ser capaç de mantenir la traçabilitat de les sessions web i les consultes a les bases de dades generades per aquestes, detectar comportaments anòmals i bloquejar possibles atacs.
- Proporcionar mecanismes de detecció i prevenció davant d'intrusions perimetrals, atacs de virus, ransomware i la llista inclosa per CVE (numeració internacional de les vulnerabilitats públiques https://www.cve.org). I s'hi pot buscar totes les vulnerabilitats de windows, de notes, de vmware,etc. La gran majoria es fan pegats pels fabricants, però les urgents (dia zero ja en explotació) o les que encara no ha sortit el pegat cal prendre mesures concretes per minimitzar-ne l'explotació.
- Establir mecanismes de protecció davant d'atacs de dia 0, atacs dirigits o APT's o el sabotatge per part d'un administrador, a través de mecanismes de sandboxing, anàlisi de trànsit o similars.
- Establir mecanismes de protecció davant d'atacs de denegació de serveis. Actualment l'Ajuntament no té mecanismes de protecció implantats.

5.3 Monitorització

Aquesta activitat consistirà en la supervisió de l'estat dels actius, la supervisió de l'sniffer de xarxa i la generació de les alertes corresponents en cas d'esdeveniments que puguin afectar la seguretat de la informació mitjançant les actuacions següents:

- Detectar i recol·lectar evidències de les incidències que es produeixin a la infraestructura de l'Ajuntament i que puguin posar en perill la seguretat de la informació.
- Discernir entre falsos positius o negatius analitzant les diferents alertes detectades.
- Processar i correlacionar els esdeveniments recol·lectats en temps real per detectar esdeveniments rellevants a la infraestructura gestionada que puguin ser indicatives d'un atac i emetre les alertes oportunes.
- Correlacionar els esdeveniments recol·lectats amb altres fonts d'informació com ara BBDD reputacionals, informació d'altres atacs detectats a altres xarxes, etc.

- Integrar fonts d'informació procedents de múltiples dispositius i fabricants.
- Monitoritzar informació sobre l'estat dels dispositius, sistemes, aplicacions i serveis des del punt de vista de disponibilitat i rendiment.
- Monitoritzar contingut de la xarxa mitjançant un sniffer cercant símptomes d'atacs i incompliments de polítiques
- Emmagatzemar i custodiar els esdeveniments recol·lectats durant un ampli rang de temps per, en cas de necessitat, fer una anàlisi forense i obtenir dades relatives a l'origen, destinació i traça dels incidents de seguretat. Custodiar fora de l'abast d'un atac al programari
- Utilitzar canals de comunicació segurs amb xifratge de dades i verificació d'origen i destí.
- Mantenir la disponibilitat dels serveis protegits davant d'eventuals errors en els elements de seguretat instal·lats per l'adjudicatari. En cap cas la decisió d'un dels elements no ha de ser motiu d'indisponiblitat dels serveis que protegeix.
- Monitoritzar l'estat operatiu dels elements instal·lats per l'adjudicatari.
- Monitorització del compliment de les polítiques de seguretat
- Per comprovar que realment s'estan aplicant les polítiques de seguretat relacionades amb evitar atacs de l'home al mig o l'ús de NTLM, es monitoritzarà el contingut de les xarxes i es generaran les alertes oportunes de seguretat o d'incompliment de les mesures aplicades.

  La llista de deteccions com a mínim ha d'incloure:

- Detecció de contrasenyes en text obert
- Detecció de comunicacions no encriptades
- Detecció d'accés SAMBA sense xifrar o signar
- Detecció d'ús de NTLM o, si no, protocols obsolets de seguretat
- Detecció d'ús de tiquets kerbers inadequats encriptats per RC4 o qualsevol anomalia indici d'un PassTheHash o PassTheTicket

La monitorització s'haurà de dur a terme a través d'un Log Manager que permeti la col·lecció, agregació, emmagatzematge i retenció, anàlisi i cerca de Log's, amb el SIEM actualment implantat a l'Ajuntament, de manera que es pugui filtrar el volum de dades passades al SIEM, exigint-se un volum de dades correlades pel SIEM de l'Ajuntament.

5.4 Gestió d' Incidents

El propòsit d'aquesta activitat és reaccionar davant de les alertes generades pel monitoratge i realitzar totes les accions necessàries per a la contenció o neutralització dels possibles atacs i la restauració a la situació prèvia, així com les gestions de notificacions pertinents:

- Classificar i prioritzar les diferents alertes generades pel procés de monitorització.
- Contenir o neutralitzar els atacs detectats d'acord amb els procediments establerts juntament amb l'Ajuntament. En aquest sentit, l'adjudicatari liderarà, juntament amb el personal tècnic de l'Ajuntament, el desenvolupament d'un Pla de Gestió i Resposta a Incidents. I haurà de comptar a més amb el servei SOC contractat amb aquesta finalitat.
- Notificar mitjançant els canals establerts als interlocutors que formin part del procés d'escalat i presa de decisions que l'Ajuntament estableixi al llançament del servei.
- Utilitzar canals de comunicació segurs per a l'intercanvi d'informació que garanteixin la confidencialitat, integritat i origen legítim de les notificacions.
- Després de cada incident, fer-ne una anàlisi forense i elaborar un informe en què es descriguin que és el que ha passat, com ha passat i quines mesures de millora s'han d'adoptar.

Després de cada incident, seguir els procediments de coordinació i notificació de ciberincidents (bé sigui la comunicació de caràcter obligatòria o potestativa) amb el CCN-CERT, que la normativa vigent durant el contracte estableixi i d'acord amb les indicacions de la Guia Nacional de Notificació i Gestió de Ciberincidents (aprovada pel Consell Nacional de Ciberseguretat el 21 de febrer del 2020 o posteriors).

5.5 Gestió de vulnerabilitats

La gestió de vulnerabilitats ha de proporcionar un nivell d'alerta primerenca davant d'amenaces emergents, encara que encara no s'hagin materialitzat en atacs als actius:

- Alertar amb caràcter periòdic de vulnerabilitats que puguin afectar la seguretat dels actius
- Proposar plans d'actuació per minimitzar el risc d'un atac aprofitant una vulnerabilitat emergent.

- Implementar els canvis necessaris als actius protegits per minimitzar el risc d'un atac que aprofiti una vulnerabilitat emergent.
- Alertar de riscos emergents (per exemple, vulnerabilitats de dia 0, atacs a gran escala, etc.) que puguin afectar la seguretat de l'Ajuntament.

La gestió de vulnerabilitats és un procés continu de TI consistent en la identificació, l'avaluació i la correcció de vulnerabilitats en els sistemes d'informació i les aplicacions d'una organització.

5.6 Operacions de Ciberseguretat

L'empresa adjudicatària ha de comptar amb la certificació d'acord amb l'ENS de categoria mitjana i ha d'estar formalment certificada com a CSIRT.es. A més, els seus serveis han d'estar certificats a ISO 20000-1, ISO 27001, ISO 22301. D'altra banda, cal registrar-se com a proveïdor de serveis de ciberseguretat (Institut Nacional de Ciberseguretat) tots aquests de gran valor per a l'Ajuntament.

El SOC formarà part de la Xarxa Nacional de Centres d'Operacions de Ciberseguretat que es coordinarà mitjançant la Plataforma Nacional de Notificació i Seguiment de Ciberincidents, prevista a l'article 11 del Reial Decret 43/2021, de 26 de gener, pel qual es desenvolupa el Reial decret llei 12/2018, del 7 de setembre, de seguretat de les xarxes i sistemes d'informació.

El SOC haurà de complir amb les següents obligacions:

- Intercanvi fluid de ciberincidents amb la Plataforma Nacional de Notificació i Seguiment de Ciberincidents mitjançant la implantació i l'operació de l'eina de gestió d'incidents LUCIA del CCN-CERT.
- Implantació de les tecnologies necessàries que permetin la vigilància del perímetre i de la xarxa interna

Així mateix, funcionarà com a CSIRT (Computer Security Incidence Response Team) amb els serveis següents:

- Resposta a Incidents com a CSIRT.
- Sensibilització CSIRT.
- Revisions de seguretat i auditories de serveis com CSIRT, fent anàlisis. vulnerabilitats amb una freqüència trimestral mínima.
- Desenvolupament de serveis de seguretat CSIRT.

- Alertes CSIRT

5.7 Administració i Operació

Aquest servei assumeix l'administració operació i actualització (en aquells elements susceptibles de ser-ho), de la infraestructura de seguretat a l'Ajuntament (Firewalls, SIEM, XDR, Seguretat Correu Electrònic, el SOAR en el supòsit.) com a mínim amb les gestions i requeriments següents :

- Gestionar la política de seguretat dels dispositius.
- Gestionar les versions de programari dels dispositius.
- Aplicar pegats.
- Gestionar configuracions.
- Atendre els requeriments de l'Ajuntament quant a sol·licitud de canvis sobre la infraestructura HW i SW de seguretat gestionada.
- Optimitzar configuracions per a la millora del rendiment.
- Disponibilitat del servei en 24x7

5.8 UN ALTRE SERVEIS A VALORAR

Seran valorats altres serveis de valor afegit al servei SOC entre ells cal destacar el de Serveis de Pentesting i Serveis BAS i qualsevol altre que l'adjudicatari proposi.

5.9 Serveis de Pentesting

Els serveis de Pentesting, o conjunt d'atacs simulats dirigits al sistema informàtic de l'Ajuntament, i només amb una única finalitat:

Detectar possibles debilitats o vulnerabilitats perquè siguin corregides i no puguin ser explotades. Aquestes auditories comencen amb la recollida, en fonts d'accés obert, d'informació sobre l'empresa, els empleats, usuaris, sistemes i equipaments. Continua amb una anàlisi de vulnerabilitats que s'intentaran explotar, fins i tot amb tècniques d'enginyeria social, atacant els sistemes fins assolir els seus objectius. Finalment, es realitza un informe que indica si els atacs tingueren èxit, i en cas afirmatiu perquè i quina informació o accés tindrien, és a dir, se simulen atacs tal com els portaria a terme un ciberdelinqüent que volgués

fer-se amb el control del sistema o amb la informació continguda. D'aquesta manera, es pot determinar:

- si el sistema informàtic és vulnerable o no,
- avaluar si les defenses amb què compta són suficients i eficaces, i
- valorar la repercussió de les fallades de seguretat que es detectin.

En la preparació del pentesting es realitza un pla amb un conjunt d'atacs dirigits, segons la tecnologia que s'utilitzi a l'Organització i les seves necessitats de seguretat. Per això, els auditors han de comptar amb metodologies —algunes específiques segons la tecnologia o estàndards de seguretat, i altres de més generals—, que els ajuden a realitzar-les de forma sistemàtica. Haurem d'escollir quines proves volem que facin i sobre quines aplicacions o serveis, previ consentiment de l'Ajuntament.

Altres tipus de proves de penetració segons la informació inicial de què disposa l'adjudicatari poden ser:

- Caixa blanca: si disposen de tota la informació sobre els sistemes, aplicacions i infraestructura, poden simular que l'atac es realitza per algú que coneix l'empresa i els seus sistemes;
- Caixa grisa: si disposeu d'una mica d'informació, però no de tota;
- Caixa negra: si no teniu informació sobre els nostres sistemes; en aquest cas, se simula el que faria un ciberdelinqüent aliè.

Això no obstant, quan s'executi un servei de pentesting, a més d'acordar-ne la finalitat, l'objecte de l'anàlisi i quin tipus de prova que volem que es realitzi a més i com es tracta d'un atac «permès» hem de tenir en compte les qüestions legals que afectin l'Ajuntament i que hauran de ser consensuades prèviament (a delimitar tant l'Ajuntament com l'adjudicatari).

5.10 Servei plataforma de simulació de bretxes i atacs (BAS)

L'adjudicatari pot proporcionar una plataforma de simulació de bretxes i atacs (BAS), que permeti a l'Ajuntament simulacions de ciberatacs multi vectorials contra si mateix, per exposar vulnerabilitats immediates i que proveeixi de processos de mitigació per mitigar cada bretxa.

Els principals vectors de l'eina, com a mínim, seran:

- Alertes d'amenaces immediates
- Avaluació de correu electrònic

- Avaluació de navegadors
- Avaluació de tallafocs per a aplicacions web
- Moviments laterals a xarxes amb dominis Windows
- Avaluació de solucions end-point
- Avaluació per a filtració de dades
- Avaluació de consciència sobre phising o ransomware
- Avaluació de SIEM/SOC
- El servei ha d'incloure un tauler o Dashboard on monitoritzar la situació de totes les eines de seguretat i la seva correlació.

Serveis de consultoria sobre arquitectura en seguretat

L'adjudicatari auditarà i assessorarà l'Ajuntament pel que fa a **l'arquitectura** de comunicacions, serveis i dispositius per avaluar la situació actual i proposar arquitectures que ajudin a millorar la seguretat objecte d'aquest projecte. Entre elles, es tractaran solucions de microsegmentació, ZTNA, la utilització massiva de factors de doble autenticació, l'estructura de les xarxes, VLANs i ús del tallafoc. Aquestes arquitectures estaran dissenyades tenint en compte que els pitjors atacs venen des de dins de la pròpia xarxa.

6 PLANIFICACIÓ I POSADA EN MARXA DEL SERVEI

Per a una completa prestació dels serveis que integren aquest projecte, distingim tres fases:

- Fase 1: Implantació, parametrització i formació de l'eina SIEM, Lucia.
- Fase 2: Prestació dels serveis avançats de gestió d'incidents de seguretat.
- Fase 3: Serveis a demanda

Fase 1: Serveis d'implantació

L'objectiu central és implementar un Centre d'Operacions de Seguretat (SOC). El SOC formarà part de la Xarxa Nacional de Centres d'Operacions de

Ciberseguretat que es coordinarà mitjançant la Plataforma Nacional de Notificació i Seguiment de Ciberincidents, prevista a l'article 11 del Reial Decret 43/2021, de 26 de gener, pel qual es desenvolupa el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.

El SOC haurà de complir amb les següents obligacions:

- Intercanvi automàtic i fluid de ciberincidents amb la Plataforma Nacional de Notificació i Seguiment de Ciberincidents mitjançant la implantació i l'operació de l'eina de gestió d'incidents LUCIA del CCN-CERT.
- Implantació de les tecnologies necessàries que permetin la vigilància del perímetre i de la xarxa interna

Fase 1.1.- Implantació, parametrització i formació de l'eina SIEM, Lucia.

L´Ajuntament ja disposa d´un SIEM implantat: SPLUNK Cloud. Cal ampliar-ne la implantació. Per això, l'adjudicatari proveirà la infraestructura necessària per suportar l'eina SIEM i tots els requeriments necessaris per al desplegament total efectiu.

Actualment es disposa d'Instància Splunk Cloud SAAS dedicada amb el número d'entitlement (o contracte/o identificador) E-0028770. Capacitat fins a 25Gb d'ingesta diària, de la qual es farà càrrec l'adjudicatari.

En aquesta fase del servei s'emmarquen les activitats següents per part de l'adjudicatari, excepte en els casos en què s'indiqui expressament que seran realitzades per l'Ajuntament d'Esplugues de Llobregat:

- Tots els logs de servidors i firewall s'han de centralitzar al SIEM de l'Ajuntament: SPLUNK Cloud, ja disponible.
- Desplegar el SIEM a la totalitat del parc de servidors i altres elements que es consideri.
    - Revisar el disseny de l'arquitectura de l'eina SIEM, incloent-hi requisits de maquinari sobre la base de logs monitoritzats.
    - Revisar canvis dels requeriments tècnics que puguin sorgir del desplegament del SIEM.
    - Preparació, documentació i desplegament de l'eina.
- Desplegament del sistema d'alertes primerenques
- Integració procedimental amb Llúcia

- Integració de les fonts acordades a l'arrencada del projecte. El nombre de fonts a integrar al sistema de recol·lecció de logs i correlat serà de mínim 9 fonts. Aquestes fonts són les següents:

Fonts	Fabricant
Directori Actiu	Windows
Servidor DNS	Windows
Servidor DHCP	Windows
Antispam	Fortimail
XDR	Sophos
Firewall	Fortinet
Antivirus	Sophos
Controladora Wifi	Aruba
Switches Core	Cisco
MDM	Vodafone

L'emmagatzematge i el manteniment de logs ha de ser de mínim de 6 mesos.

- Definició de quadre de comandament de les fonts d'informació integrades.
- Aplicació d'intel·ligència mitjançant casos d'ús, personalització i desenvolupament de casos nous d'ús.
- En finalitzar la fase d'instal·lació i d'implantació, s'haurà de proporcionar al personal de l'equip tècnic de l'Ajuntament d'accés a la consola de gestió de l'eina i la formació necessària sobre les eines de treball.

Aquesta fase haurà de ser implantada en un termini màxim de dos mesos, si es produeix una desviació d'implantació haurà de ser notificada amb 15 dies d'antelació al responsable de l'Ajuntament d'Esplugues de Llobregat, qui validarà si la desviació és correcta evitant així les possibles penalitzacions definides al plec administratiu.

Fase 1.2 Documentació a lliurar

La documentació lliurada per l'adjudicatari i validada per l'Ajuntament servirà com a punt de partida per a la fase d'implantació i haurà d'incloure:

- Plànol detallat de posada en marxa i configuració, incloent-hi estimació de temps per a cadascuna de les tasques. Procés d'instal·lació, que inclogui tots els elements necessaris per disposar de l'equipament i eines totalment operatives.
- Identificació de parts involucrades en el desplegament i les dependències

entre elles: necessitats d'infraestructura maquinari, connectivitat de xarxa, adreçament IP necessari, etc.

- Pla de configuració del sistema.
- Proposta d'integració amb sistemes externs.
- Proposta de polítiques generals de configuració.
- Proposta de definició d'alertes i incidents.
- Arquitectura del sistema desplegat. Diagrames físics i lògics.

Fase 2: Prestació dels serveis avançats de gestió d'incidents de seguretat.

Aquest servei vindrà suportat pel personal adscrit al SOC de l'adjudicatari. Els serveis de gestió de la seguretat desenvolupat pel SOC inclouran les funcions següents:

- Monitorització de seguretat, detecció primerenca d'incidents i amenaces
- Detecció, anàlisi i gestió de vulnerabilitats
- Manteniment, revisió, administració i reporting de la infraestructura
- Gestió i resposta a incidents de seguretat de la informació (CSIRT)
- Interlocutor únic del proveïdor responsable de servei

Fase 2.1.- Monitorització de seguretat, detecció primerenca d'incidents i amenaces

El servei de monitorització de seguretat té com a objectiu la detecció de qualsevol violació o amenaça imminent de la seguretat que pugui ser detectada en base a l'anàlisi continuada dels esdeveniments o alertes de seguretat reportats per les fonts d'integració definides, gràcies a la seva correlació i anàlisi esdeveniments.

Aquest servei ha de garantir la detecció i resposta en la modalitat 24x7, per aconseguir aquest objectiu ha de complir les condicions següents:

- Monitorització dels esdeveniments de seguretat mitjançant el SIEM proporcionat per l'adjudicatari
- Detecció, identificació, classificació i categorització de possibles incidents de seguretat i recol·lecció d'evidències necessàries per a anàlisis posteriors.

- Alertar o notificar als responsables de l'Ajuntament d'Esplugues de Llobregat (correu electrònic, sms o trucada) i oferir informació breu que s'ha detectat i la categorització que s'ha donat. El nivell de notificació estarà definit per la criticitat/impacte de l'incident.
- Integració procedimental amb LUCIA ferramenta del CCN-CERT per a la notificació d'incidents.
- Correlació i anàlisi d'esdeveniments.
- Anàlisi d'incidents tenint en compte totes les fonts d'informació i qualsevol informació que permeti la contenció, remediació i recuperació dels actius afectats i afectació als serveis compromesos i derivats per poder fer una valoració d'impacte.
- Proposta de protocols en resposta als incidents, plans de mitigació i remediació.
- Execució automàtica davant d'incidents amb accions ràpides de bloqueig, contenció i resposta, prèviament definits i creat amb l'Ajuntament per a certes alertes.
- Orquestració d'accions de remediació automàtica (SOAR) sobre les principals tecnologies de seguretat.
- Servei de detecció i resposta gestionada (MDR), realitzant les tasques següents:
    - Monitorització (Threat intelligence): Validació d'alertes, neteja de falsos positius, anàlisi, normalització i contextualització de tots els registres.
    - Investigació (Threat hunting): procés de cerca proactiva a través de les xarxes per detectar i aïllar amenaces avançades capaces d'evadir les solucions de seguretat. La recerca de recerca d'activitat sospitosa, més basada en el comportament i nebulosa, no basada en alertes o esdeveniment desfermat, mirar a través de l'entorn i buscar proactivament patrons d'atac i crear regles.
    - Resposta (24/7): presa de mesures automàtiques de forma proactiva com a remediació d'un atac, infecció, accés no autoritzat.
- Incorporació de fonts d'indicadors de compromís (IOC), privats, públics i propis de l'adjudicatari.
- Coordinar l'execució dels plans de mitigació i remediació iniciats fins que

es doni per tancat l'incident amb l'equip involucrat en l'incident, en cas que fos necessari el desplaçament d'algun membre de l'equip anirà a càrrec de l'adjudicatari.

Fase 2.2.- Detecció, anàlisi i gestió de vulnerabilitats

Per poder tenir un seguiment del cicle de vida de les vulnerabilitats detectades, corregides i verificades cal tenir un sistema de detecció i contra mesura d'amenaces que puguin existir als sistemes de l'Ajuntament.

L'objectiu d'aquest mecanisme és el següent:

- Alerta i identificació de vulnerabilitats potencials i confirmades de tots els sistemes de l'organització, aquesta detecció es realitzarà mitjançant eines especialitzades proporcionades per l'adjudicatari.
- Filtratge de falsos positius per evitar-ne el tractament.
- Creació de protocols (correctius o preventius) per mitigar o corregir les vulnerabilitats detectades.
- Verificació de la implantació dels protocols correctius i preventius per garantir la correcció de les vulnerabilitats detectades.

Fase 2.3.- Manteniment, revisió, administració i reporting de la infraestructura

L'adjudicatari es responsabilitzarà del funcionament correcte dels elements implantats, configurats i gestionats objecte de la licitació. La configuració de seguretat sempre serà validada i aprovada pel cap de projecte assignat per l'Ajuntament d'Esplugues de Llobregat.

El proveïdor podrà operar els equips de seguretat en cas necessari únicament sota la supervisió i l'aprovació pel cap de projecte assignat per l'Ajuntament. En cas que l'actuació estigui fora de les competències objecte d'aquesta licitació l'adjudicatari haurà de donar suport a les consultes i peticions relacionades amb canvis i millores de configuració, actualitzacions dels dispositius i instal·lacions o activacions de nous serveis/característiques sobre la infraestructura de seguretat que pugui rebre.

Totes les implantacions, configuracions i gestions que realitzi l'adjudicatari mínim hauran de complir amb les recomanacions establertes d'accés segur realitzades pel CCN.

L'objectiu d'aquesta fase és:

- Monitorització permanent (24/7) de l'estat dels equips objecte de la licitació i de les fonts integrades, per tal de poder garantir el bon funcionament del servei.
- Donar solució a incidents o caigudes de serveis crítics a conseqüència de qualsevol atac o vulnerabilitat de seguretat
- Suport a la revisió de la configuració i esdeveniments dels equips gestionat o no per l'adjudicatari.
- Resolució d'incidents, manteniments i tasques sol·licitades pel cap de projecte assignat per l'Ajuntament sobre els equips i els serveis administrats per l'adjudicatari.
- Manteniment, planificació i execució de canvis necessaris segons la recomanació del fabricant sobre el servei proporcionat per l'adjudicatari.
- Correcció de vulnerabilitats identificades al servei i equipaments proporcionats, notificació de vulnerabilitat dels equips no gestionats per l'adjudicatari.
- Totes les actuacions (canvis, configuracions o actualitzacions) han de ser notificades prèviament, motivades i programades en una finestra acordada amb el cap de projecte assignat per l'Ajuntament.
- El servei de manteniment, revisió i administració haurà de gestionar els incidents, peticions i consultes davant de la necessitat d'informació, degradació o comportament no esperat sobre els equipaments o del mateix servei administrat.
- L'adjudicatari haurà de proporcionar els terminis d'acord de servei (SLA) per a l'atenció i la resolució d'incidents i peticions en els diferents nivells de severitat:
    - CRITIC: Incidències greus per tall del servei.
    - ALT: Incidències en què hi ha degradació del servei.
    - MEDI-BAIX: Incidències amb algun impacte al servei.

Aquests terminis hauran de ser acordats i validats pel cap de projecte assignat per l'Ajuntament i mai no podran superar els temps establerts a la taula següent.

	Resposta	Resolució	Consultes
CRÍTIC	30 min	4h	2d

ALT	30 min	8h	3d
MITJÀ-BAIX	30 min	48h	3d

Fase 2.4.- Gestió i resposta a incidents de seguretat de la informació (CSIRT)

En cas de patir un incident greu de seguretat l'Ajuntament d'Esplugues de Llobregat requereix un equip de resposta a incidents especialitzat que proporcioni el suport i l'experiència necessària per analitzar, contenir i remediar els atacs dirigits contra l'organització i minimitzar-ne l'impacte.

Aquest servei es caracteritza per:

- Investigació i anàlisi forense
    - Avaluació, validació, obtenció d'evidències i contextualització de l'incident
    - Identificació de vectors dentrada, tècniques d'ofuscació, mètodes de propagació, tècniques d'exfiltració, etc.
    - Obtenir indicadors de compromís (IOC).
    - Coneixement de contramesures de mitigació.
    - Contextualització de l'amenaça mitjançant la fase forense i les fonts d'intel·ligència del proveïdor.
    - Identificació de l'abast de l'incident (actius compromesos, moviments laterals, escalada de privilegis, etc.).
- Resposta i remediació
    - Davant incident de coordinació de totes les parts involucrades i el responsable del projecte per part de l'Ajuntament.
    - Guia i suport per minimitzar l'impacte de l'incident en curs.
    - Suport a l'erradicació, recuperació i tornada al servei,
    - Monitorització i control post incident.
- Actuacions davant d'incident
    - Identificació del codi maliciós (malware) o atac.
    - Identificació de l'objectiu de l'atac.

- Identificar tots els possibles IOC.
- Identificació de vectors d'entrada, tècniques d'ofuscació, mètodes de propagació, tècniques de filtració, etc.
- Identificació de dominis, IPs, URLs, etc. Susceptibles a bloqueig.

La metodologia per a la gestió i resposta als incidents de seguretat haurà de ser en compliment del CCN-CERT, d'acord amb l'Esquema Nacional de Seguretat (ENS) i que està referenciada a les guies CCN-STIC-403 i CCN-STIC-817 .

El servei és responsable de les actuacions en incidents amb criticitat mitjana o baixa amb la cobertura dels serveis objecte d'aquesta licitació. Si l'incident és d'alta criticitat, el CSIRT prendrà la responsabilitat per defecte, també es pot sol·licitar l'actuació del CSIRT sota demanda de l'Ajuntament o des dels primers nivells del SOC.

Matriu de classificació d'incidents:

		IMPACTE		
		Baix	MediAlt	
AFECTACIÓ	Baixa	Molt baixa	Baixa	Mitjana
	Mitjana	Baixa	Mitjana	Alta
	Alta	Mitjana	Alta	Molt alta

- MOLT ALTA/ALTA: Incidents d'alt impacte amb alta afectació i degradació o pèrdua de servei vitals.
- MITJANA: Incidents d'un impacte important, però sense afectació a serveis vitals.
- BAIXA: Incidents de seguretat sense cap impacte crític.

Fase 2.5.- Interlocutor únic del proveïdor responsable de servei

L´Ajuntament d´Esplugues de Llobregat requereix un interlocutor únic (security manager) i amb disponibilitat garantida, responsable de tots els serveis de seguretat objecte d´aquesta licitació per part del proveïdor adjudicatari.

Aquest interlocutor serà el responsable de garantir la qualitat de tots els serveis oferts per l'adjudicatari. A banda d'impulsar l'evolució de la millora dels serveis durant tota la durada de la licitació.

Fase 2.6.- Documentació a lliurar

- Protocols d'actuació davant alertes de seguretat: Del funcionament habitual del sistema de gestió centralitzada de la seguretat se n'extrauran informacions conseqüència de la monitorització i de la correlació d'esdeveniments. A partir de l'experiència aportada per l'adjudicatari, es definirà una classificació del nivell de gravetat per a les alertes de seguretat, així com els protocols d'actuació associats per a cadascuna.
- Informe d'incident: L'adjudicatari es compromet a lliurar en un termini inferior a 48 hores posterior a un incident greu un informe on inclogui la descripció de l'incident, afectació (objecte o servei afectat, temps total, temps d'inici i fi d'incidència), antecedents, causa arrel de l'incident, la solució i les accions realitzades. Després del tancament de l'incident i en un termini màxim de 7 dies, cal lliurar l'informe detallat de l'incident.
- Informe de les vulnerabilitats: L'adjudicatari lliurarà informe setmanal de les vulnerabilitats detectades i corregides, amb evidències i estudi d'impacte en temes de confidencialitat, integritat i disponibilitat. En cas de detectades i no corregides l'informe haurà de reflectir recomanacions per a corregir-les.
- Informe periòdic que permeti conèixer l'estat actual de seguretat dels equipaments administrats, així com el número, el detall i l'estat de les peticions, alertes i incidents de cada equip i la seva disponibilitat.
- Informe mensual d'incidents: L'adjudicatari lliurarà informes incloent el resum mensual d'incidents.

Fase 3: Serveis a demanda

L'Ajuntament estima una borsa de jornades destinada als serveis que no estan previstos i que puguin sorgir. Aquestes tasques aniran destinades tant a la

prevenció, gestió i resposta davant d'incidents de seguretat de la informació, com a altres necessitats de seguretat.

Aquestes jornades inclouran:

- Un mínim de 25 jornades anuals a raó de 8h/jornada de tècnics especialitzats en resposta a incidents (CSIRT) donaran suport a incidents greus de seguretat que ho requereixi l'Ajuntament. La primera resposta d'incidents serà donada pel personal del SOC, aquestes jornades estaran supeditades a les necessitats del SOC de forma excepcional i prèviament autoritzades pel responsable de l'Ajuntament i la gravetat de l'incident o sota demanda de l'Ajuntament.
- Un mínim de 50 jornades anuals per provisió segons les necessitats de seguretat de l'Ajuntament. En aquestes 50 jornades s'hi inclou el desplaçament a les dependències en cas estrictament necessari i sol·licitat pel responsable de l'Ajuntament.

7 MÈTODE DE GESTIÓ I DESCRIPCIÓ D'EQUIP TÈCNIC

4.

5.

5.1 Model de gestió

Per prestar els serveis descrits en aquesta proposta d'una manera eficaç i eficients s'aplicaran models de gestió internacionals de prestigi reconegut: ISO 20000-1, ISO 27701, ISO 9000, ISO 14001 i ENS (nivell Mitjà).

5.2 Equip de treball

El equip de treball que portarà a cap el projecte estarà compost per perfils multidisciplinaris, *Enginyers en Telecomunicacions i/o Informàtica o estudis anàlegs (CFGM o FPII Informàtica o electrònica)* , sent el detall de cada perfil:

- Coordinador del projecte: El Coordinador del projecte serà el punt d'interlocució habitual amb els Equips de Treball. Serà un consultor amb almenys deu anys de experiència en seguretat i capacitació adequada a les necessitats particulars d'aquest projecte.
- Enginyers de Seguretat: Seran els membres del equip tècnic encarregat de definir l'arquitectura i la configuració de les plataformes a desplegar. S'encarregaran també de portar a terme la formació del equip del SOC i configurar a les eines, les tècniques, mètodes de penetració i contramesures per a entorns Windows.

Tindran experiència de dos anys almenys en el disseny, desplegament i configuració de totes les eines a desplegar.

- Analistes de Seguretat: L'equip d'analistes donarà suport a la definició de fonts a integrar, casos d'ús i regles de correlació. S'encarregaran també de fer la formació del equip del SOC.

  Els analistes de seguretat tindran dos anys de experiència a el desplegament, configuració i operació de les eines a desplegar.

  Certificació específica del personal adscrit al projecte
  - CISA – ISACA
  - CISM – ISACA
  - Lead Auditor ISO 27001
  - Lead Auditor ISO 22301
  - CEH - Certified Ethical Hacker
  - Màster en Ciberseguretat, TOGAF, CSX.

5..3 Sistema de seguiment i control

El model de seguiment i control del projecte es basarà en un model a tres nivells per tal de garantir la comunicació i la interlocució amb les diferents parts i assegurar un seguiment adequat del projecte.

Es crearà un comitè per a cada nivell, establint-se un Comitè de Direcció, un Comitè de Seguiment i un Comitè Operatiu. Aquests comitès es reuniran amb la periodicitat que es determini durant l'establiment del contracte i en la fase inicial del projecte d'implantació del servei. A més, es duran a terme tantes reunions addicionals com es consideri oportú per garantir la gestió adequada del servei.

- Comitè de Direcció. L'objecte del Comitè de Direcció serà la definició d'aspectes estratègics del servei. La freqüència de les reunions es proposarà inicialment de manera semestral. Els seus documents de treball principals seran els informes executius de progrés del projecte, així com les agendes i actes de reunió.

- Comitè de Seguiment. Aquest comitè estarà conformat pel cap de projecte i els coordinadors del projecte. Per a aquest comitè es proposa una reunió mensual per revisar els informes de control, revisar incompliments, riscos i accions correctores, així com verificar el progrés i la millora contínua del projecte, el registre de risc i els informes de control i seguiment. El Comitè de Seguiment serà el principal responsable del control del projecte, utilitzant per a això:

  - La definició del calendari i fites del projecte

- Informes mensuals de l'estat del projecte en què:
  - Es mesuren els indicadors per verificar la correcta execució
  - Es mostri el progrés i el grau de compliment de les fites programades
- Les eines que es posin a disposició de l'Ajuntament per part del proveïdor per al seguiment del projecte.

- Comitè Operatiu. Amb una funció eminentment tècnica i pràctica, assumirà la coordinació i la gestió diària del projecte. Estarà constituït pels diferents responsables i tècnics involucrats al projecte. Es reuniran de manera setmanal, o sempre que el servei ho requereixi, per assegurar la resolució de conflictes, revisar les solucions implantades i avaluar riscos i propostes de millora.

8 CONDICIONS ESPECIALS D'EXECUCIÓ

L'execució d'aquest projecte s'haurà de fer de manera presencial.

Acta d'inici de la prestació del servei

Un cop formalitzat el contracte en document administratiu, s'ha d'estendre l'acta d'inici de prestació del servei, per exemplar triplicat, que serà signada pel representant legal de l'empresa i el responsable del contracte.

Lliurament dels treballs i/o realització dels serveis

El contractista haurà de lliurar els treballs realitzats dins del termini estipulat al contracte; el responsable del contracte efectuarà l'examen de la documentació presentada i, si estimés complertes les prescripcions tècniques i restants condicions contractuals, proposarà que se'n dugui a terme la recepció. En cas que estimés incomplertes les prescripcions tècniques del contracte, donarà per escrit al contractista les instruccions precises i detallades per tal d'esmenar les faltes o defectes observats, fent constar en aquest escrit el termini per efectuar les esmenes i les observacions que consideri oportunes . En cas de reclamació per part del contractista respecte de les observacions formulades, el responsable del contracte us elevarà, amb el seu informe, a l'òrgan de contractació per a la seva resolució. Si el contractista no reclamés per escrit respecte a les observacions del responsable del contracte, se n'entendrà la conformitat i quedarà obligat a corregir o esmenar els defectes detectats. En serveis de

prestació contínua, el plec de clàusules administratives podrà establir altres maneres de constatar la correcta execució dels serveis prestats.

Recepció dels treballs i serveis

Quan la prestació s'ajusti a les condicions del contracte serà procedent la recepció i s'aixecarà l'acta corresponent que serà signada pel responsable del contracte i el representant legal del contractista. Si la prestació no és ajustada a les condicions necessàries per a la recepció, es donaran per escrit les instruccions oportunes al contractista per tal que esmeni els defectes observats i compleixi les seves obligacions en el termini que per això es fixi; no és procedent la recepció fins que les instruccions hagin estat emplenades, aleshores s'estén l'acta corresponent. En serveis de prestació contínua, el plec de clàusules administratives podrà preveure altres maneres de recepció. L'acta de recepció serà estesa per triplicat exemplar, un dels quals serà incorporat a l'expedient de contractació.

Obligacions en matèria de prevenció de riscos laborals

- El contractista estarà obligat al compliment de la Llei 31/1995, de 8 de novembre, de prevenció de riscos laborals i restant legislació general i sectorial aplicable en aquesta matèria respecte dels treballadors adscrits a la contracta.
- En cas de concurrència de treballadors del contractista amb altres treballadors en un centre de treball municipal, l'Ajuntament vetllarà pel compliment de la normativa de prevenció de riscos laborals per part de les empreses que presten serveis corresponents a la pròpia activitat en els termes establerts pel RD 171/2004, del 30 de gener, pel qual es desenvolupa l'art. 24 de Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals, en matèria de coordinació d'activitats empresarials L'Ajuntament facilitarà a l'empresa que resulti adjudicatària del contracte els documents i la informació a què fa referència l'art. 7 del Reial decret 171/2004, de 30 de gener, relatiu a: Avaluació de riscos del centre de treball, mesures de prevenció, pla d'emergència i qualsevol altre que correspongui. El contractista està obligat a presentar, abans de formalitzar-se l'acta d'inici de prestació del servei, els documents que seguidament s'indiquen en compliment del que disposa l'art. 10.2 del Reial Decret 171/2004:
    - Avaluació de riscos i planificació de l'activitat preventiva.

- Compliment de les obligacions en matèria d'informació i formació respecte dels treballadors que hagin de prestar serveis al centre de treball.

- Qualsevol altre que l'Ajuntament consideri convenient o necessari. 3. El contractista tindrà accés a la documentació municipal a través de la plataforma informàtica autoritzada per l'Ajuntament en la forma que li serà indicada pel responsable del contracte i haurà de presentar els documents a través de la mateixa plataforma.

Reforç de la conscienciació i potenciació de les capacitats dels empleats i col·laboradors externs en matèria de seguretat de la informació i ciberseguretat.

Suport a les activitats de divulgació i conscienciació en matèria de seguretat de la informació, realitzant almenys les tasques següents:

- Elaboració de propostes formatives (Mòduls formatius, Newsletters, Guies, píndoles, etc.).
- Generació de continguts divulgatius relacionats amb la prevenció i la resposta a incidents de seguretat.
- Proves de Phising per avaluar situació de conscienciació abans i després de la formació
- Formació in situ a tot el personal sobre enginyeria social i prevenció.

9 ALTRES SERVEIS A VALORAR A L'ALCANDE DEL CONTRACTE

Els serveis que es descriuen a continuació seran de valoració al plec en el cas que el licitador els incloïa dins l'abast de la seva proposta.

6.

7.

7.1 DETECTAR ATACS, ORDINADORS INFECTATS I INCOMPLIMENTS DE POLÍTIQUES DE SEGURIDA

Monitoritzar el comportament de tots els ordinadors (PCs, servidors i cimbells) i cercar forats de seguretat en ells, a més de monitoritzar el contingut de la xarxa interna i l'accés des de i cap a Internet.

RESUM

L'equip de monitorització és responsable de detectar els ordinadors amb evidències d'estar infectats o d'estar realitzant accions potencialment perjudicials, o que incompleixen les polítiques de seguretat de l'Ajuntament, ja sigui intencionadament o per errors en la configuració de les mesures de seguretat.

Tant els PC com els servidors s'han de monitoritzar a nivell de comportament i d'accés des de i cap a internet, usant un antivirus, el tallafoc, i un sniffer i cercar comportaments anòmals o perillosos.

Especialment, es monitoritzaran els controladors de domini, servidors DNS, DHCP i els servidors de fitxers.

Addicionalment, es realitzaran proves de penetració i de cerques de vulnerabilitats a tots els actius, per prevenir aquestes situacions.

També s'analitzarà el contingut de la xarxa interna usant un sniffer per donar suport al compliment de l'objectiu.

Es crearan cimbells, ordinadors específicament febles i especialment monitoritzats, perquè siguin els principals objectius en cas d'atac.

DETALL

L'equip de monitorització és responsable de detectar els ordinadors amb evidències d'estar infectats o d'estar realitzant accions potencialment perjudicials, o que incompleixen les polítiques de seguretat de l'Ajuntament, ja sigui intencionadament o per errors en la configuració de les mesures de seguretat.

Aquesta detecció es farà per les alertes del mateix antivirus, o pel comportament

anòmal de les esmentades màquines, sobretot pel que fa a accessos a Internet i els protocols usats.

Es monitoritzarà el comportament dels ordinadors a nivell de processos, ia nivell d'accés des de i cap a internet, a més del registre del syslog del tallafocs central.

També es monitoritzaran les configuracions de tots els ordinadors, segons la llista d'especificacions indicades als annexos, com ara detectar la desactivació del tallafoc local o de l'antivirus, tenir habilitat la compartició de fitxers, tenir carpetes compartides, tenir determinats serveis habilitats com el del FAX, o permetre les connexions RDP des d'IPs no autoritzades. En especial, es comprovarà la configuració del Windows Defender per veure que no hi hagi excepcions a les carpetes a analitzar.

Algunes d'aquestes configuracions no només s'han de comprovar a la configuració (veure si està aplicada certa GPO o no), sinó que s'haurà de comprovar explícitament si funciona. Per exemple, encara que s'hagi aplicat la restricció d'accés a l'RDP només des de certes IPs, cal intentar connectar el port 3389 per comprovar que està bloquejat. Aquestes mesures són necessàries perquè hi podria haver configuracions contradictòries que interfereixin en les mesures de seguretat, com podria ser una regla incorrecta al tallafoc local, o que estigui deshabilitat.

Part d'aquesta monitorització consisteix en la comprovació sistemàtica de forats de seguretat: es llançaran proves de penetració automàtica a tots els sistemes, tant en horaris planificats com de forma aleatòria quan el personal de l'Ajuntament ho consideri necessari. Aquesta comprovació ha d'incloure detecció de programari amb vulnerabilitats o no actualitzats.

Tots els logs de servidors i firewall s'han de centralitzar al SIEM de l'Ajuntament: SPLUNK Cloud, ja disponible.

Els ordinadors per monitoritzar són els PCs dels usuaris, els servidors en domini, els servidors fora de domini, i en concret els servidors de còpies de seguretat.

Les vulnerabilitats s'han de buscar tant en aquests equips, com a les cabines Synology, els servidors físics VMWare i el vCenter.

La monitorització de la xarxa es divideix en 3 blocs: la xarxa interna dels usuaris, les xarxes DMZ que segmenten els servidors i l'accés des d'Internet.

La monitorització de l'accés des d'Internet la controla el tallafoc, igual que les mesures de seguretat, per tant, s'han de monitoritzar aquestes alertes per si hi ha alguna cosa greu a destacar. El tallafoc ja conté regles específiques per a accions prohibides (com utilitzar navegadors Tor), i llançar els oportuns esdeveniments, que són els que s'han de monitoritzar.

A més, cal monitoritzar el contingut de la xarxa interna i de les DMZ, de forma puntual però repetitiva ia voluntat, cercant contingut no desitjat o paquets que no haurien d'estar, com a mínim el que s'indica als annexos, però podent adaptar-se a la necessitat que es tingui a cada moment.

Per realitzar aquestes funcions, l'equip de monitorització definirà els recursos que necessita a cada xarxa, i l'Ajuntament els ho proporcionarà. Entre ells, es definiran ordinadors PC estàndard, a la xarxa d'usuaris, des del qual s'intentarà realitzar moviments horitzontals a la resta d'ordinadors, i també es realitzaran parts de les funcions ja definides que són més efectives des de dins de la pròpia xarxa que a través del tallafoc, o fer de sniffer.

De la mateixa manera, es crearan servidors virtuals a cadascuna de les xarxes per realitzar aquestes mateixes tasques.

En el cas concret dels honeypots (màquines pensades perquè siguin les principals víctimes d'un atac i millorar-ne així una detecció primerenca), l'equip de monitorització proporcionarà la solució del mercat que consideri més oportuna, o en defecte d'això sol·licitarà a l'Ajuntament els ordinadors que consideri necessaris (sent la seva responsabilitat les llicències), formant part del servei deixar-los instal·lats, configurats, i dur a terme la seva administració. S'han de detectar rangs d'IPs no definides per l'Ajuntament, peticions DNS a servidors no autoritzats, peticions DNS l' IP d'origen de les quals no és a la xarxa des d'on s'envia, contrasenyes en clar, paquets NT/NTLM, paquets SAMBAv1, identificació de usuari com Anonymous, etc.

Un cas especial és la monitorització dels controladors de domini i els servidors de fitxers. S'haurà de fer especial èmfasi tant en la seva monitorització com en els informes que es facin, i en supervisar les alertes que es generin pel Microsoft ATA, quan estigui instal·lat. També es monitoritzarà el canvi als fitxers que defineixen el NETLOGON com la GPO de windows, per alertar quan es produeixin canvis sospitosos (fora d'horari laboral, nocturn, o no esperat)

S'aplicaran les mesures oportunes per detectar els atacs més perillosos, com ara Golden/Silver Ticket, o qualsevol MIM.

Les deteccions automàtiques, que es configurin, han de llançar alertes a l'equip de sistemes perquè prenguin les mesures oportunes.

L'equip de monitorització col·laborarà amb sistemes per validar que s'estan complint les mesures de seguretat que es vagin prenent. Aquestes mesures són dinàmiques, i s'aniran ampliant amb el pas del temps, per la qual cosa el monitoratge s'haurà de poder adaptar a les futures deteccions que es vagin necessitant.

L'equip de monitorització també aportarà el vostre coneixement i experiència per millorar les accions necessàries per aconseguir l'objectiu. De manera proactiva ha d'aportar les iniciatives necessàries per aconseguir l'objectiu principal, incloent regles que considera que el tallafocs hauria de tenir per aconseguir generar les alertes necessàries, sempre des del punt de vista de monitorització.

Les amenaces a monitoritzar s'hauran d'ampliar segons es produeixin les principals alertes públiques, com ara les publicades per INCIBE, CCN-CERT o de MITRE, que ens afectin. O també:

- www.exploit-db.com: Offensive Security Exploit Database Archive.
- www.securityfocus.com: SecurityFocus.
- www.helpnetsecurity.com: Help Net Security.
- www.symantec.com: Vulnerabilities - Symantec Corp.

En cas que s'hagi de fer una recuperació total del sistema per part de l'Ajuntament, l'equip de monitorització participarà en el control de quins dispositius s'estan activant a mesura que es recuperen, per contrastar que les úniques màquines en marxa són les que ha activat l'equip de recuperació, i que no se n'ha activat cap altra. Es tracta d'un seguiment detallat, i en directe, de la detecció de màquines que s'inicien, i comprovar que la resta estan apagades.

L'equip de monitorització haurà de lliurar un informe mensual, a mode de resum executiu, de la situació de tot el parc informàtic, amb el contingut que s'especifica a l'annex corresponent, posant èmfasi en les incidències mitjanes i greus detectades.

L'equip de monitorització haurà de realitzar en els primers 6 mesos, i després cada any, un informe indicant les millores que considera necessàries tant per poder oferir millor els seus serveis, com millores generals en la seguretat que l'Ajuntament hauria de realitzar, tant en arquitectura com a mesures a aplicar.

Es definirà un equip de treball amb l'Ajuntament, que serà l'únic que tindrà accés a la informació que es generi amb aquest projecte, i seran els únics autoritzats com a interlocutors d'aquest projecte.

L'equip de monitorització haurà de signar un acord de confidencialitat pel qual no podrà comunicar cap contingut relacionat amb aquest projecte: ni les infraestructures, ni el seu contingut, ni per descomptat les vulnerabilitats trobades.

MESURES ACTUALS

Es disposa de l'antivirus Sophos ja desplegat a tots els ordinadors, excepte els servidors, amb EDR activat, i parcialment configurat per al seu funcionament correcte.

L'Ajuntament disposa del SIEM SPLUNK Cloud, configurat per rebre logs dels servidors més exposats o delicats, de l'antivirus i el tallafocs.

El tallafoc central disposa de regles específiques per detectar accions sospitoses, la detecció de les quals hauria de llançar les corresponents alertes.

L'ajuntament disposa de GPO ja configurades específiques per a seguretat de Windows, ja desplegades.

TASQUES CONCRETES A REALITZAR

- Com a mínim (però no limitat a aquesta llista si no s'aconsegueix l'objectiu principal) s'han de realitzar les tasques següents:
- Instal·lar l'agent SPLUNK a la resta dels servidors
- Instal·lar els sniffers necessaris per analitzar totes les xarxes indicades
- Analitzar el contingut de totes les xarxes cercant coses que no haurien d'estar, relacionades amb la seguretat
- Crear un sistema d'alertes centralitzat
- Formar el personal de l'ajuntament a les eines utilitzades perquè puguin realitzar tasques puntuals
- Un cop al mes, llançar anàlisis de vulnerabilitats i test de penetració. També cal poder llançar en qualsevol moment de forma esporàdica
- Realitzar els oportuns informes mensuals i anuals
- Analitzar el programari instal·lat a tots els ordinadors
- Informar de programari amb vulnerabilitats o desactualitzat
- Realitzar tasques de comprovació d'accessos: provar ports específics (RDP, VNC, SMB) a tots els ordinadors, intentar identificar-se com Anonymous, intentar accés com SAMBAv2, suplantar un servidor de fitxers
- Realitzar proves de Man-in-the-middle en serveis DNS, SAMBA, PROXY
- Detectar serveis i ports oberts a totes les màquines: DNS pirata, PROXY fals

- Alertar de serveis que no haurien d'estar en certes màquines (DNS)
- Alertar de configuracions incorrectes (GPO no aplicada, firewall desactivat)
- Alertar si es detecta trànsit Tor o VPN
- Alertar si hi ha màquines intentant accedir a servidors C2C
- Alertar si hi ha un trànsit inusual a internet (enviar moltes gigues a la nit)
- Sol·licitar les alertes centralitzades que l'SPLUNK pot relacionar i que són necessàries per aconseguir l'objectiu
- Instal·lar, configurar i monitoritzar els honeypots

7..2 REDUIR L'ABAST I ELS DANYS D'UN ATAC ACTIU

L'equip de resposta primerenca és responsable de reduir el dany produït per un atac prenent les mesures que consideri necessàries, entre les quals hi ha: aïllar xarxes, apagar servidors, bloquejar comunicacions activant regles especials del tallafoc, activar aïllament de màquina proporcionat per l'antivirus Sophos, o qualsevol altra mesura que consideri oportuna per evitar que un ransomware es propagui o segueixi executant-se als servidors infectats.

Cal disposar d'un equip 24x7 rebent alertes i monitoritzant punts crítics, amb la capacitat de prendre decisions capaces de frenar o aturar un atac.

RESUM

L'equip de resposta és responsable de reduir el dany produït per un atac prenent les mesures que consideri necessàries, entre les quals hi ha: aïllar xarxes, apagar servidors, bloquejar comunicacions activant regles especials del tallafoc, activar aïllament de màquina proporcionat per l'antivirus Sophos , o qualsevol altra mesura que consideri oportuna per evitar que un ransomware es propagui o executi als servidors infectats.

És important indicar que les dades que contenen els servidors estan en un disc dur independent del sistema operatiu, de manera que un ordinador infectat pot ser recuperat només substituint el sistema operatiu, així que és de vital importància reduir els danys que el ransomware estigui realitzant sobre les dades com més aviat millor: un cop s'inicia un atac de ransomware, és important aturar-lo com més aviat millor per reduir els danys que aquest pot fer.

Per fer-ho, cal disposar d'un equip 24x7 els 365 dies a l'any, amb accés a la

monitorització del sistema i amb els privilegis suficients per prendre les mesures de contenció que considerin necessàries. És habitual que els atacs de ransomware s'iniciïn justament quan el personal d'informàtica no treballa: divendres nit, caps de setmana, festius.

L'equip de resposta primerenca ha de tenir prou coneixement de la infraestructura física i virtual de l'entorn, de manera que sigui capaç de prendre les mesures més oportunes de contenció en funció de les diferents alertes que rebi, i ha de ser capaç de diferenciar les alertes d'un atac ransomware de les de la resta.

En col·laboració amb l'equip de sistemes, disposareu d'una llista d'accions possibles a realitzar en funció del tipus d'atac i de la seva criticitat, però és la vostra obligació prendre les mesures que considereu oportunes, llevat que l'Ajuntament ho hagi indicat explícitament.

L'equip de resposta primerenca disposarà de les eines i els equips que consideri necessaris, i que sol·licitarà a l'Ajuntament, per poder dur a terme el seu objectiu. Com a mínim, disposarà de 2 equips dedicats exclusivament per a les seves tasques, que estarà fora del domini i amb totes les mesures de seguretat que siguin necessàries per mantenir-lo segur, des del qual podrà fer totes les accions que consideri oportunes. Un dels equips serà físic i l'altre virtual, ubicats a diferents xarxes.

Un d'aquests equips és el principal i l'altre és el secundari, que en cas d'atac no s'ha de fer servir fins a garantir que no es pot infectar.

Es definirà un indicador anomenat “DEFCON” que indicarà la situació d'amenaça en què es troba el sistema, que tots els involucrats han de conèixer-ne el significat i que podrà ser consultat per saber ràpidament la situació. Els seus valors són:

- DEFCON 5: situació normal
- DEFCON 4: rebudes alertes que necessiten ser investigades
- DEFCON 3: evidències d'un atac lleu
- DEFCON 2: evidències d'un atac greu
- DEFCON 1: no es pot aturar l'atac

L'activació a partir de DEFCON 3 a DEFCON 1, anirà associada a una llista de comunicacions que s'hauran de fer dins d'uns terminis estrictes indicats al corresponent Annex.

El procediment per dur a terme quan es generin alertes es defineix al corresponent annex, i serà acordat tant per l'Ajuntament com per l'equip de

resposta primerenca durant l'execució del projecte. Bàsicament es tractarà de discernir entre les diferents alertes per centrar-se en les que poden ser part d'un atac, validar-les obtenint evidències, i fer les tasques de contenció que siguin oportunes, sempre buscant complir l'objectiu d'aquest projecte. El nivell de DEFCON ha d'estar actualitzat a cada moment.

Un cop l'any, o quan l'Ajuntament ho consideri oportú, es farà una simulació de tot el procés, sota l'amenaça d'un atac fictici, fins al nivell que l'Ajuntament consideri necessari.

Setmanalment, l'equip de resposta primerenca farà proves d'accés als sistemes per comprovar que teniu accés a totes les mesures que heu de prendre, i realitzareu algunes de les accions de control per comprovar que realment funcionen.

Mensualment, realitzarà un informe com s'indica als annexos, l'objectiu del qual és indicar l'estat de les proves setmanals, les incidències detectades aquest mes, i les millores que necessita per assegurar-ne l'objectiu.

En cas de realitzar alguna acció, es realitzarà un informe excepcional indicant les alertes que van donar lloc a l'activació de la resposta, el resultat de les accions realitzades, i les incidències produïdes durant aquestes.

Es definirà un únic responsable de l'Ajuntament al qual s'informarà en cas d'incidències. L'equip de resposta primerenca signarà un acord de confidencialitat pel qual no es comunicarà res a ningú més. En cas d'usar canals públics, només es farà servir podrà utilitzar el terme DEFCON, sense entrar en detalls.

S'emportarà en tot moment un registre confidencial, de tot el que ha passat des que es va iniciar el projecte fins al moment actual, en què s'ha d'incloure el nivell de DEFCON, les amenaces detectades, les evidències d'atacs, les mesures preses i totes les comunicacions fetes a qualsevol col·laborador, persona o institució.

És important recalcar que l'accés amb nivell d'administrador total de què disposarà l'equip de resposta primerenca pot ser una bretxa de seguretat, per la qual cosa la confidencialitat i el registre del seu ús és de compliment estricte. Una infecció a l'equip de resposta primerenca es pot convertir en un vector d'atac amb conseqüències fatals.

És de compliment obligat que l'equip de resposta primerenca ha de disposar d'un ciber segur que el cobreixi sota qualsevol circumstància.

Les taules d'actuacions i actes, indicades en aquest document, són únicament com a exemple per indicar la càrrega de treball i com s'actuarà, però es detallaran a mesura que evolucioni el projecte.

Serà responsabilitat de l'equip de resposta primerenca realitzar els corresponents documents, segons el seu criteri, per a una correcta execució per part del propi personal, tenir-los ben documentats i actualitzats, segons s'acordi amb l'Ajuntament. El personal autoritzat per part de l'Ajuntament haurà de poder accedir a aquesta documentació quan ho consideri oportú, tant per a la revisió com per proposar noves actuacions.

S'acordarà una manera d'emmagatzemar les credencials d'accés de manera segura i confidencial.

7..3 ACONSEGUIR QUE TOTS ELS EQUIPS DE L'AJUNTAMENT SIGUIN INVULNERABLES A LA MAJORIA D'ATACS

L'equip de protecció és el responsable de prendre totes les mesures de protecció necessàries a tots els ordinadors de l'Ajuntament per aconseguir que un atacant remot no els pugui comprometre, dins d'una seguretat raonable.

RESUM

L'equip de protecció és el responsable de prendre totes les mesures de protecció necessàries a tots els ordinadors de l'Ajuntament per aconseguir que un atacant remot no els pugui comprometre, dins d'una seguretat raonable.

Això inclou, però no es limitada a, configurar i instal·lar els antivirus, les polítiques de seguretat i tota la resta de mesures de seguretat necessàries per aconseguir que els ordinadors de l'Ajuntament (PCs, servidors dins de domini, servidors fora de domini i cabines)) es considerin raonablement segurs davant d'un atac remot.

Concretament, inclou la instal·lació dels antivirus o antimalware, l'actualització del programari obsolet o amb pegats, la desactivació dels serveis que no siguin necessaris, l'aplicació de pegats urgents per a atacs zero-day, l'actualització no evolutiva dels sistemes operatius de els servidors i la configuració de les mesures de seguretat que s'acordi amb sistemes.

No entra dins de les seves funcions la configuració del tallafoc extern, però sí tot el que s'ha de fer dins dels ordinadors, com és la configuració del tallafoc intern de Windows, com també la de sol·licitar a sistemes les restriccions al tallafoc que consideri oportunes per protegir els servidors.

Tampoc no entra dins de les seves funcions la migració evolutiva de versió dels sistemes operatius, que correspon a sistemes.

DETALL

Per aconseguir l'objectiu, cal prendre accions diferents a cadascun dels diferents

grups d'ordinadors (PCs, Servidors i cabines).

Les mesures a prendre seran les proposades pel propi equip de protecció, per l'equip de sistemes i les necessàries per protegir les vulnerabilitats i les debilitats detectades per l'equip de monitorització de vulnerabilitats.

Actualment, l'equip de sistemes ja ha implantat tant l'antivirus com les GPO necessàries per tenir una part de la seguretat contemplada, i manté els ordinadors actualitzats. S'hauran de corregir, continuar i ampliar aquestes mesures per aconseguir l'objectiu principal. És responsabilitat de l'equip de protecció tenir aquests punts al dia.

Pel que fa als PCs, les mesures hauran de ser les necessàries per protegir un ordinador client, que no fa les funcions de servidor i que per tant no necessita que ningú ni res se'l connecti excepte per als casos especificats als annexos.

Pel que fa als servidors, cadascú té diferents serveis per oferir, i ha de ser l'únic al que se li pot accedir des de qualsevol ordinador. Un cas especialment delicat són els servidors de fitxers de dades, que s'han de restringir amb molta cura.

Pel que fa a les cabines, hauran de seguir les mateixes filosofies que els servidors.

De manera general, les principals vies d'infecció de les màquines han d'estar restringides i limitades per IP, concretament l'accés RDP, SAMBA i el servei de cua d'impressió.

S'han de configurar tant els servidors com els PC perquè totes les comunicacions estiguin encriptades i signades -quan això sigui possible- per evitar atacs de man in the middle o d'adquisició de dades per un sniffer. Aquestes comunicacions inclouen, però no limitades a les comunicacions RDP, VNC, SAMBA, SQLServer, SMTP, IMAP, POP3

L'equip de protecció haurà d'aportar el seu coneixement i experiència per sol·licitar a l'equip de sistemes allò que sigui necessari per protegir els ordinadors, tenint especial dedicació a les vulnerabilitats que estiguin sent explotades en el moment present (in the wild). En concret, haurà d'assessorar l'equip de sistemes pel que fa al que necessita per evitar atacs de robatori de contrasenyes, en concret els atacs de man-in-the-middle, protocols febles, i evitar robatori de tiquets kerbers.

De forma mensual, haurà de fer un informe de situació en què detalli l'evolució de la protecció dels ordinadors, com es detalla a l'annex corresponent:

- visió global de l'estat de protecció dels ordinadors

- estat de la llista de mesures a prendre
- llista de problemes trobats a l'hora d'aplicar les mesures de protecció
- llista de peticions a altres equips de l'Ajuntament pel que fa a la seguretat

MESURES ACTUALS

- firewall local activat i configurat adequadament
- firewall central configurat i restringit
- servidors únicament amb ports oberts que necessiten
- cabines - no s'ha aplicat cap mesura

TASQUES CONCRETES A REALITZAR

- Informe de màquines gestionades, agrupades per PC, servidors, cabines o altres.

7..4 GARANTIR LA RESTAURACIÓ DE LES CÒPIES DE SEGURETAT, FINS I TOT EN CAS D'UN SABOTATGE INTERN DE MÀXIM NIVELL

Fer, verificar i restaurar les còpies de seguretat de manera fiable

RESUM

L'equip de recuperació és el responsable de tot el procés de les còpies de seguretat: des de la realització fins a la restauració, en col·laboració amb el personal de l'Ajuntament.

L'equip haurà de fer les còpies de seguretat dels actius, comprovar que estan ben fetes i es poden restaurar, custodiar-les de manera que un sabotatge remot no les pugui destruir, i restaurar-les en cas necessari.

Es faran servir diferents tipus de còpies de seguretat, alineades amb les polítiques de l'Ajuntament, unes proporcionades per l'Ajuntament (clons de màquines virtuals online i offline) i altres proporcionades per l'equip al vostre criteri.

Els actius seran els elements crítics de l'Ajuntament: les màquines virtuals, la configuració del tallafocs i dels switches principals.

La restauració haurà de tenir com a objectiu aixecar el sistema en el temps definit als annexos, per nivells importants de cada sistema.

Per garantir el compliment d'aquests objectius, s'han de fer simulacions tant de

restauració com de validació de les còpies de seguretat.

Queda fora de l'abast d'aquest projecte, la recuperació del contingut al núvol (Gmail)

DETALL

L'equip de recuperació haurà de continuar amb les mesures actuals de còpia de seguretat ja implementades, ampliant i millorant la seva realització amb les mesures pròpies que consideri oportunes per aconseguir l'objectiu fixat, i que proporcionarà sense cost addicional dins del context d'aquest projecte. Les noves mesures complementaran les actuals, sense substituir-les en cap cas.

El nou sistema de còpies de seguretat haurà de permetre aixecar les màquines virtuals fins al nivell 5 sense necessitat d'haver de restaurar-les prèviament en una altra cabina. Aquest emmagatzematge es publicarà a l'actual sistema VMWare de l'Ajuntament, i al segon CPD de contingència que encara no està en producció.

S'han de prendre les mesures oportunes per mantenir segur el sistema de còpies de seguretat, tant el ja existent com el proporcionat per l'equip de recuperació, per evitar que un atac remot el pugui comprometre, dins d'una seguretat raonable.

Les màquines virtuals es classifiquen en 10 nivells d'importància, i l'1 és el més crític per aixecar el sistema, 5 el que és just i necessari per aixecar l'Ajuntament, i 10 la recuperació total de tot el sistema. Cadascuna té la seva pròpia definició de validesa de les còpies de seguretat, i el temps que pot estar aturat el servei.

Les màquines crítiques per aixecar el sistema (entre altres, els controladors de domini i vCenter de VMWare) es duplicaran periòdicament en un sistema aïllat i independent, de manera que tingui un pla alternatiu per ser aixecat, i que normalment estarà a offline. Aquestes mesures es prendran 4 cops l'any.

La infraestructura maquinari (les cabines, el tallafocs i els switches principals), també han de tenir còpies de seguretat de la seva configuració, i en el cas concret del tallafocs es contempla poder restaurar un tallafoc virtual, amb ajuda d'un proveïdor extern.

La validació de les còpies de seguretat s'ha de fer de manera contínua per assegurar que es té el control d'aquestes còpies, en concret que la contrasenya de xifratge no hagi canviat, i que tot el sistema és estable i permet restaurar-ne el contingut .

La simulació de restauració s'ha de fer almenys una vegada a l'any i ha de contemplar la recuperació total en un entorn extern de tot el sistema fins al nivell

5. L'objectiu d'aquesta restauració és demostrar que es pot aconseguir que tot funcioni en aquest altre entorn , i si no, localitzar els problemes, errors i formes de treballar ineficients que poden dificultar obtenir aquest objectiu.

Una vegada aconseguit el nivell 5 en el temps definit als annexos, es mesurarà quant de temps es triga a tenir restaurada la resta dels nivells, fins al nivell 10. Aquests resultats seran els que avaluïn la qualitat del procés de la còpia de seguretat. És obligatori realitzar els canvis necessaris per aconseguir els temps definits als annexos.

Part d'aquesta simulació consistirà a recuperar discos diferents de moments diferents d'una màquina virtual: el disc del sistema operatiu de fa un mes, i el disc de les dades de fa 2 dies. L'objectiu d'aquesta simulació és mesurar el cost en temps i la dificultat de recuperar màquines virtuals crítiques unint diferents backups per minimitzar la pèrdua de dades.

La restauració, quan sigui necessari, serà l'execució en producció de les simulacions realitzades anteriorment.

L'equip de restauració tindrà previst, en el sistema nou que proposi, que les còpies de seguretat s'hauran de seguir fent després d'una restauració forçosa, fins i tot quan aquesta no estigui del tot garantida com a vàlida i neta de virus. Dit d'una altra manera, quan es facin les restauracions, les còpies de seguretat han de continuar protegint les dades immediatament, dins d'un marge raonable.

Tot i que l'objectiu de les còpies de seguretat és la restauració total del sistema, també ha de permetre la recuperació parcial de fitxers per a tasques d'administració i gestió.

Mensualment, i durant cada simulació, es farà un informe, com es detalla a l'annex, que indiqui la situació de les mesures de recuperació: visió global dels ordinadors protegits, de l'espai que ocupa i els temps estimats de recuperació.

Al principi del projecte, un cop implantat el sistema de còpia de seguretat proposat per l'equip de recuperació, aquest documentarà tot el procediment de còpies i restauració per poder ser usat com a guia per a l'equip de sistemes en cas de desastre.

L'equip de recuperació dotarà l'Ajuntament d'un espai al núvol on allotjar tota la documentació referent a les mesures de recuperació (i altres mesures relacionades amb la seguretat) perquè estigui disponible fins i tot si la infraestructura de l'Ajuntament no estigui disponible. Aquest espai només contindrà documentació.

Tota la documentació s'haurà de revisar com a mínim una vegada a l'any per garantir que és correcta i es correspon amb la realitat.

TASQUES CONCRETES PER REALITZAR, SEMPRE VINCULADES A L'OPERACIÓ DEL SERVEI

- Comprovació diària de l'execució de les tasques de còpies de seguretat: dels clons, els snapshots i les mesures addicionals que proposi l'equip de recuperació.
- Comprovació diària, i després setmanal, que les còpies de les màquines crítiques estan ben fetes i es poden restaurar
- Comprovació setmanal i després mensual que les còpies importants, a offline, estan ben realitzades.
- Simulació mensual a semestral, en funció de l'estabilitat del sistema, de la restauració de les màquines crítiques, importants i de tot el sistema.
- En cas de necessitat, suport i restauració de tot el sistema, seguint els mateixos passos que a les simulacions.
- Aportar un sistema addicional estàndard de còpies de seguretat, sense cap cost per a l'Ajuntament, plenament configurat i operatiu, amb la capacitat suficient i necessària per al backup de les màquines fins al nivell 8, complint-ne els temps històrics.
- Suport al personal de l'Ajuntament en la definició i l'administració de les tasques de còpies de seguretat del sistema nou.
- Formació del nou sistema, al personal de l'Ajuntament a nivell d'operador, amb l'objectiu que puguin ser capaços de fer còpies i restauracions de manera independent.
- Formació genèrica al personal de l'Ajuntament dels sistemes moderns de còpies de seguretat: funcionalitats, requisits i limitacions.
- Garantir els temps de recuperació estipulats als annexos, independentment de si els sistemes actuals ho aconsegueixen o no.
- Quan ho sol·liciti l'Ajuntament, haurà de realitzar una restauració a nivell de màquina o fitxers, amb l'objectiu de comprovar el sistema.