Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

BALDINTZA TEKNIKOEN AGIRIA, ARRASATEKO UDALEAN ZIBERSEGURTASUN PROIEKTU BAT KONTRATATZEKO

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACION DE UN PROYECTO DE CIBERSEGURIDAD PARA EL AYUNTAMIENTO DE ARRASATE

1. XEDEA

Lehiaketa honen xedea Arrasateko Udalaren informazio-sistemak babesteko zibersegurtasuneko zerbitzu edo proiektu integral baten hornidura, ezarpena, mantentzea, prestakuntza eta laguntza teknikorako zerbitzuak kontratatzea da.

1. SORTA: zibersegurtasun plataforma konposatzen duten software, programa eta tresnen erosketa, ezarpen, mantentze, prestakuntza eta laguntza teknikorako zerbitzuak kontratatzea eragingo du. Modu honetara Administrazio publikoetan zein ingurune pribatuetan azken urteetan gertatzen ari diren eraso informatikoen aurrean udalak bere datu eta sistemak babesteko baliabide egokiak izatea ahalbidetuko du.

2. SORTA: udal langileen formakuntza eta kontzientziazio lanketarako irtenbide informatikoak hornitzeaz eta kudeatzeaz arduratuko da, zibersegurtasun alorrean. Honetaz gain formakuntza saio batzuk emango dizkiete udal langileei.

3. SORTA: Aholkularitza-zerbitzu bat kontratatzeaz arduratuko da, GAP analisia (arrakalen analisia) egiteko, ENS ziurtagiria (Segurtasun Eskema Nazionala) lortzeko beharrezko jarraibideak eta ekintzak zehazteko. Lote honen xedea ez da ENS ziurtagiria lortzea.

1. OBJETO

El objeto del presente concurso es la contratación del suministro, implantación, mantenimiento, formación y asistencia técnica de un servicio o proyecto integral de ciberseguridad para la protección de los sistemas de información del Ayuntamiento de Arrasate.

El **LOTE 1** implicará la contratación de servicios de adquisición, implantación, mantenimiento, formación y asistencia técnica de software, programas y herramientas que compongan la plataforma de ciberseguridad. De esta forma, el Ayuntamiento dispondrá de los medios adecuados para proteger sus datos y sistemas ante los ataques informáticos que se están produciendo en los últimos años tanto en las Administraciones públicas como en entornos privados.

El **LOTE 2** se encargará del suministro y gestión de las soluciones informáticas para el trabajo de formación y concienciación del personal municipal en materia de ciberseguridad, así como la impartición de varias charlas formativas a los empleados.

El **LOTE 3** Se encargará de la contratación de un servicio de consultoría para la realización de un análisis GAP (análisis de brechas), que determine las pautas y acciones necesarias para la obtención del certificado ENS (Esquema Nacional de Seguridad). No es objeto de este lote la obtención del certificado ENS.

Horretarako, nahiz eta lehenengo sorta kontratuaren xede osoaren zati handi bat izan, beharrezkoa da sorta bakoitzaren baldintzatzaile espezifikoak aztertzea eta ulertzea zibersegurtasun proiektu integral baten parte izango direla, ezingo delarik bateraezinak diren irtenbideak ematea hiru sorten artean. Bateraezinak diren edo ez erabakitzea kontratu honen balorazioa egingo duen lantaldearen esku geratuko da.

Soluzio osoak honako datu eta ezaugarri hartu beharko ditu kontutan:

a) Zibersegurtasuneko zerbitzu kudeatu bat kontratatzea, MDR (Gertakarien Detekzio eta Erantzun Zerbitzua) izenez ere ezagutzen dena, kanpoko erasoen arriskuak minimizatzeko (prebentzioa), eraso baten eraginpean egonez gero detektatzeko (detekzioa) eta kaltetutako elementuak arintzeko eta desagerrarazteko (deuseztatzea).

b) SOC/SIEM irtenbide baten instalazioa (Segurtasun eragiketen zentroa / Segurtasunari buruzko informazioa eta gertaeren kudeaketa), sare informatiko osoan zehar (ordenagailuak, zerbitzariak eta sareko trafikoan). Proposatzen den SIEM irtenbidea izan daiteke software oinarrizkoa edo hardware oinarrizkoa edo mixtoa. Derrigorrezkoa izango da udal sareko ordenagailu informatiko bakoitzean Endpoint motako software bat instalatzea segurtasun informazioa jasotzeko eta aparailua bera babesteko.

c) Gaur egun Arrasateko Udalak dituen firewalletan eta switchetan sortzen diren segurtasun-gertakariak integratzeko gaitasuna (2 firewall Forti 100 F HAn eta Cisco switchak), baita gaur egun instalatuta dauden sistemekin bateragarritasuna ere (Watchguarden Adaptative Defense 360 250 ordenagailutan, Microsoften eta Linuxen oinarritutako sistema eragileen sarea, posta elektronikorako Relay eta antispam zerbiztua Sarenetekin, eta Postfixen oinarritutako posta

Para ello, aunque el primer lote constituya una parte importante del objeto total del contrato, es necesario analizar los condicionantes específicos de cada lote y comprender que formarán parte de un proyecto integral de ciberseguridad, sin que sea posible aportar soluciones incompatibles entre los tres lotes. La determinación de las incompatibilidades quedará en manos del equipo de valoración del presente contrato.

La solución completa deberá tener en cuenta los siguientes datos y características:

a) Contratación de un servicio gestionado de ciberseguridad, también conocido como MDR (Servicio de Detección y Respuesta ante Incidentes), para minimizar los riesgos de ataques externos (prevención), detectar en caso de estar afectados por un ataque (detección) y soporte para la mitigación y erradicación de los elementos afectados (eliminación).

b) Instalación de una solución SOC/SIEM (Centro de Operaciones de Seguridad / Información de seguridad y gestión de eventos) en toda la red informática (ordenadores, servidores y tráfico en red). La solución SIEM propuesta puede ser basada en software, hardware o una solución mixta. Será obligatorio instalar en cada ordenador informático de la red municipal un software tipo Endpoint para recibir información de seguridad y proteger el propio aparato.

c) Capacidad de integración de los eventos de seguridad que se generen en los firewalls y switches que tiene actualmente el Ayuntamiento de Arrasate (2 firewalls Forti 100 F en HA y switches Cisco), así como compatibilidad con los sistemas instalados actualmente (Adaptative Defense 360 de Watchguard en 250 equipos, red de sistemas operativos basados en Microsoft y Linux, sistema de Relay y antispam de correo electrónico con Sarenet, y sistema de correo

elektronikoaren sistema). Esleipendunak proposatu dezake gaur egun dagoen Adaptative Defense 360 programa ordezkatzea EDR egoki batekin, baina proiektuaren prezioan barneratu beharko du kostu hori.

d) Faktore bikoitzarekin identifikatzeko integrazio-gaitasuna, dela web-aplikazioen bidez, dela smartphone-rako aplikazioen bidez, dela identifikazio-token bat duten gailu fisiko espezifikoen bidez.

e) Proposatzen den irtenbideak ENS arautegiak adierazten dituen gutxieneko ezaugarriak bete behar ditu, irtenbide osoa martxan jartzen den unean.

f) Proposatzen den udal langileentzako formakuntza planak bi esparru jaso behar ditu. Batetik formakuntza saio presentzial batzuen planifikazioa, eta bestetik tresna informatiko bereziekin egindako saio interaktiboak eta eraso zein segurtasun egoera larrien simulatzaileak. Proposamen honek aipatutako tresna informatiko espezifiko honen kostua ere adierazi behar du.

electrónico basado en Postfix). El adjudicatario puede proponer la sustitución del programa Adaptative Defense 360 por otro que cumpla los requisitos de un EDR y que deberá incluir en el precio del proyecto.

d) Capacidad de integración de identificación con doble factor ya sea a través de aplicaciones web, aplicaciones para smartphone, o dispositivos físicos específicos que contengan un "token" de identificación.

e) La solución propuesta debe reunir las características mínimas indicadas por la normativa ENS en el momento de la puesta en marcha de la solución completa.

f) El plan de formación para el personal municipal que se proponga deberá incluir dos ámbitos. Por un lado, la planificación de algunas sesiones formativas presenciales, y por otro las sesiones interactivas con herramientas informáticas específicas y simuladores de situaciones graves de ataques y seguridad. Esta propuesta debe incluir también el coste de esta herramienta informática específica mencionada.

Garbi adierazi beharko dira zein balio ekonomiko ezarriko dituen proposatutako eskaintzak bai hasierako esleipena osatzeko eta baita gainontzeko urteetan ordaintzeko ere.

Hurrengo zerrendan adierazten dira gaur egun udalak dituen hainbat baliabide informatiko, proposamenak aurkezten dituzten enpresek ondo ulertu dezaten zein testuinguru teknologikotan egin beharko duten haien eskaintza:

Postu informatikoak (Windows 11 eta 10): 250
Zerbitzariak Windows: 15
Zerbitzariak Linux: 3
Zerbitzarien birtualizazio sistema: VMWare
Posta Elektronikoa udal zerbitzarietan: Postfix
Segurtasun kopia sistemak: Veeam Backup

Se deberán indicar claramente que cantidades económicas se establecerán en la propuesta económica tanto pala la implantación inicial como para los posteriores años.

En el siguiente listado se indican una serie de recursos informáticos de los que dispone actualmente el Ayuntamiento para que las empresas que presenten sus propuestas comprendan el contexto tecnológico en el que deberán realizar su oferta:

Puestos de trabajo (Windows 11 y 10): 250
Servidores Windows: 15
Servidores Linux: 3
Plataforma de virtualización de servidores: VMWare
Correo Electrónico en servidores propios: Postfis
Sistema de copias de seguridad: Veeam Backup

Datu Baseak: SQL Server eta Postgress
Sistema ofimatikoa: Office 365 (One Drive gabe)

Azaldutako punturen bat EZ betetzea nahikoa baldintza izango da eskainitako zerbitzuaren proposamena baztertzeko.

Aurkezten den proposamenak aurreko puntu horiek adierazitakoa bete beharko ditu, helburu hauekin:

Bases de Datos: SQL Server y Postgress
Sistema ofimático: Office 365 (sin One Drive)

El NO cumplimiento de alguno de los puntos descritos será condición suficiente para descartar la propuesta del servicio ofertado.

La propuesta que se presente deberá cumplir con lo indicado en los puntos anteriores, con el objetivo de:

1. SORTA: Segurtasun-plataforma osatzen duten software, programa eta tresnen hornidura, ezarpena, mantentze-lanak, prestakuntza eta laguntza teknikoa.

Zibersegurtasun-zerbitzuak ezarriko dira zibersegurtasun-intzidenteen aurrean prebentzio-, babes-, detekzio- eta erantzun-gaitasunak hobetzeko, eta, besteak beste, arlo horretako adierazle nagusiak monitorizatzea ahalbidetuko duen jarraipen-sistema bat izango dute.

IT azpiegituraren konplexutasuna handitzen ari denez, eta erakundeek jasaten dituzten erasoak askotarikoak eta sofistikatuak direnez, ezinbestekoa da mehatxuen aurreko segurtasun- eta esposizio-maila zehaztea, aktiboei eragiten dieten kalteberatasunen bizi-zikloa behar bezala detektatuz eta kudeatuz.

Egon daitezkeen mehatxuak detektatzeko eta horiei aurre egiteko mekanismo egokiak ezarri beharko dira, bai eta hautemandako kalteberatasunen bizi-zikloaren jarraipena lortu ere, erakundearen inguruneak eskatzen dituen sistemetan, plataformetan eta zerbitzuetan segurtasun-maila egokia mantentzeko.

Udalaren gaitasuna gaituko du Udalari eragiten dioten segurtasun-mehatxuak prebenitzeko edo arintzeko beharrezkotzat jotzen dituen ekintzak gauzatzeko, arrisku nabarmenena dakarten kalteberatasunei lehentasuna emanez eta baliabideak

LOTE 1: Suministro, implantación, mantenimiento, formación y asistencia técnica de software, programas y herramientas que componen la plataforma de seguridad.

Se implantarán servicios de ciberseguridad destinados a mejorar las capacidades de prevención, protección, detección y respuesta ante incidentes de ciberseguridad, contando con un sistema de seguimiento que permita, entre otras, monitorizar. los principales indicadores en este ámbito.

Ante el incremento de la complejidad en la infraestructura IT y la gran variedad y sofisticación de los ataques a los cuales se encuentran expuestas las organizaciones, resulta imprescindible determinar el nivel de seguridad y de exposición frente a las amenazas, a través de una detección oportuna y gestión adecuada del ciclo de vida de las vulnerabilidades que afectan a los activos.

Se deberán establecer los mecanismos adecuados para detectar y contrarrestar las amenazas que pudieran existir, así como lograr un seguimiento del ciclo de vida de las vulnerabilidades detectadas para mantener un nivel adecuado de seguridad en los sistemas, plataformas y servicios exigidos por el entorno en el que se desenvuelve la organización.

Habilitará la capacidad del Ayuntamiento para llevar a cabo las acciones que considere necesarias para prevenir o mitigar las amenazas de seguridad que afectan al Ayuntamiento, priorizando y destinando recursos a aquellas vulnerabilidades que impliquen un

bideratuz.

Zibersegurtasun-zerbitzuaren kudeaketa-taldeak Arrasateko Udalari egiten dion jakinarazpen orok informazio zehatza izan beharko du, gutxienez jatorria, helmuga, larritasuna, intzidente-mota eta proposatutako ekintza xehatua adieraziz (konponketarako xehetasun teknikoa barne).

Era berean, ez da erantzun-ekintza kopuru mugatu bat egongo kontratuak irauten duen bitartean, eta ez da kostu gehigarririk egongo MDR zerbitzuak urtean jarduera edo esku-hartze kopuru bat baino gehiago behar izateak.

Jarduketa eta/edo esku-hartze horiek, Arrasateko udala ziber-eraso baten biktima izanez gero, mehatxuari eustea ez ezik, kaltetutako makinetan egon daitekeen programa gaiztoa garbitzea eta desagerraraztea ere barne hartu behar dute.

Horretarako, preskripzio teknikoen agiri honen bidez, zibersegurtasuneko operazio-zentro bat hedatu nahi da. Zentro horrek funtzionatzeko funtsezko elementuak jasoko ditu, hala nola perimetroko segurtasun-oztopoak, logak biltzeko eta zerrendatzeko sistema eta detekzio- eta erantzun-teknologia. Halaber, Segurtasun Eskema Nazionalera egokitu nahi da, segurtasunaren eredu homogeneo bat sustatzeko esparru gisa balioko baitu, eta aukera emango baitu bitartekoak erabiltzeko segurtasun-politika ezartzeko eta tratatutako informazioaren segurtasuna behar bezala bermatzeko.

Ildo horretan, eta Udalak helburu hori gauzatzeko baliabide teknikorik eta giza baliabiderik ez duenez, beharrezkoa da SIEM, SOC, CSIRT zerbitzuak eta aholkularitza-zerbitzuak kontratatzea, Arrasateko Udalaren Segurtasun Eskema Nazionalean arrakalak aztertzeko GAP bat egiteko.

riesgo más destacado.

Cualquier notificación que el equipo de gestión del servicio de ciberseguridad haga al ayuntamiento de Arrasate deberá incluir información precisa indicando como mínimo origen, destino, gravedad, tipo de incidente y acción propuesta detallada (incluido el detalle técnico para su remediación).

No existirá de igual modo, un número limitado de acciones de respuesta durante la duración del contrato ni concurrirán costes adicionales el hecho de que sean necesarias más de un número de actuaciones o intervenciones por parte del servicio MDR al año.

Dichas actuaciones y/o intervenciones en caso de que el ayuntamiento de Arrasate sea víctima de un ciber-ataque no solamente deben incluir la contención de la amenaza, sino también la limpieza y erradicación del posible programa maligno en la(s) máquina(s) afectada(s).

Para ello se pretende con el presente Pliego de prescripciones técnicas el Despliegue de un Centro de Operaciones de ciberseguridad que incorporará los elementos fundamentales para su funcionamiento, como barreras de seguridad perimetral, sistema de recolección y correlación de logs, y también tecnología de detección y respuesta., así como la adecuación al Esquema Nacional de Seguridad que servirá como marco para promover un modelo homogéneo de la seguridad y permitirá establecer la política de seguridad en la utilización de medios, así como garantizar adecuadamente la seguridad de la información tratada.

En esta línea, y dado que el Ayuntamiento no cuenta con los medios técnicos ni humanos para llevar a cabo este objetivo, se hace necesaria la contratación de los servicios SIEM, SOC, CSIRT, y los servicios de consultoría para la realización de un GAP análisis de brechas del Ayuntamiento de Arrasate en el Esquema Nacional de Seguridad

Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

Baldintza teknikoen agiri honen helburua da zibersegurtasuneko eta araudia betetzeko bulego bat abian jartzeko kontratazioa arautuko duten baldintzak ezartzea.

Este pliego de condiciones técnicas tiene como objetivo establecer las condiciones que regirán la contratación de la puesta en marcha de una oficina de ciberseguridad y cumplimiento normativo.

Bulego horretatik koordinatuko dira zibersegurtasuna hobetzera eta araudia betetzera bideratutako jarduera guztiak; horien artean, nabarmentzekoa da Segurtasun Eragiketen Zentro bat (SOC) abian jartzea. Zentro hori enpresa batek ustiatu beharko du, eta SOC Sare Nazionalari atxikita egongo da. Horrez gain, Segurtasun Eskema Nazionala hobeto betetzeko tresnak ezarriko dira.

Desde está oficina se coordinarán todas las actividades encaminadas a la mejora de la ciberseguridad y cumplimiento normativo, entre las que destaca la puesta en marcha de un Centro de Operaciones de Seguridad (SOC), que deberá ser explotado por una empresa que estará adherida a la Red Nacional de SOC y la implantación de herramientas que permitan mejorar el cumplimiento del Esquema Nacional de Seguridad.

Helburu nagusia Arrasateko Udalak eskaintzen dituen azpiegituren, komunikazioen eta zerbitzu digitalen segurtasuna bermatzea izango da, eta zibersegurtasuneko gorabeheren aurrean prebentzio-, detekzio- eta erantzun-gaitasunak hobetzea. Udalaren informazio- eta komunikazio-sistemen transakzioetan mehatxuak detektatzeko eta zaintzeko gaitasuna handitu nahi da, bai eta eraso posibleen aurrean erantzuteko gaitasuna hobetu ere.

El objetivo principal será garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por el Ayuntamiento de Arrasate y mejorar las capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad. Se pretende aumentar la capacidad de vigilancia y detección de amenazas en las transacciones de los sistemas de información y comunicaciones del Ayuntamiento, así como la mejora de su capacidad de respuesta ante posibles ataques.

Segurtasun perimetralaren arloan zibermehatxuetatik babestea lortu nahi da, bai eta behar bezala konfiguratzea, administratzea, kontrolatzea eta kudeatzea ere. Beste helburuetako bat da segurtasun-intzidente konplexuen aurrean sailen arteko koordinazioa eta zibersegurtasun-adimena partekatzea eta trukatzea bultzatuko duen eredu integral bateranzko bilakaera. Horretarako, zaintza-, prebentzio-, detekzio-, analisi-, erantzun- eta aholkularitza-tresnak, -prozesuak eta -zerbitzuak ezarriko dira.

Se pretende perseguir la protección en el ámbito de la seguridad perimetral frente a ciberamenazas, así como su correcta configuración, administración, control y gestión. Se marca como otro de los objetivos la evolución hacia un modelo integral que favorezca la coordinación interdepartamental ante incidentes de seguridad complejos y la compartición e intercambio de inteligencia de ciberseguridad, fijando para ello la implantación de herramientas, procesos y servicios de vigilancia, prevención, detección, análisis, respuesta y asesoramiento.

Helburua da Arrasateko Udalaren segurtasun-egoera eta haren ezagutza-maila hobetzea. Gainera, informazioaren segurtasunaren arloko erregulazioa betetzeko elementu bideratzaile gisa jardungo da, zehazki, Segurtasun Eskema Nazionalean (ENS),

Se persigue mejorar la situación de seguridad del Ayuntamiento de Arrasate y su grado de conocimiento. Además, se actuará como elemento facilitador para el cumplimiento de la regulación en materia de seguridad de la información, concretamente del Esquema

betetzeari dagokionez dauden gabeziak zehazteko beharrezko azterketak eta azterlanak barne hartuta, eta, oinarri horren gainean, SENen eskakizunak betetzen direla bermatzeko azpiegituran, aplikazioetan, zerbitzuetan, prozesuetan eta prozeduretan beharrezkoak diren egokitzapenak, aldaketak eta konfigurazioak proposatzea. Aplikatzen bada, dagokion adostasun-ziurtagiria lortzea bilatuko da.

Nacional de Seguridad (ENS), incluyendo los análisis y estudios necesarios para determinar las carencias en relación con el cumplimiento y, sobre esta base, proponer las adaptaciones, modificaciones y configuraciones necesarias en la infraestructura, aplicaciones, servicios, procesos y procedimientos para garantizar el cumplimiento de las exigencias del ENS. Si aplica, se perseguirá obtener la certificación de conformidad correspondiente.

Era berean, ahuleziei, konfigurazio-akatsei eta gorabeherei buruzko ikusgarritasun eta informazio gehiago lortu nahi da, eta, aldi berean, babes- eta erantzun-gaitasunak hobetu.

Asimismo, se pretende obtener más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, a la vez que se mejoren las capacidades de protección y respuesta.

SOCean Sare Nazionalarekiko integrazioa kudeatu beharko da. Hori guztia Segurtasun Eskema Nazionalean herritarrei emandako zerbitzuak bermatzeko jasotako eskakizunei lotuta dago, zerbitzu horiek zuzenean edo zeharka bitarteko elektronikoetan oinarritzen direnean tratatzen duten informazioa babestuz.

Se deberá llevar a cabo la gestión de la integración con la Red Nacional de SOC. Todo ello ligado a los requerimientos reflejados en el Esquema Nacional de Seguridad para garantizar los servicios prestados a la ciudadanía, protegiendo la información que estos servicios tratan, cuando se apoyan directa o indirectamente en medios electrónicos.

Hori guztia beharrezkoa da, ENSaren ezarpena bitarteko presentzial edo telematikoen bidez garatutako transakzio elektronikoen legezko baliozkotasunari eusteko bermea delako. Erakundearen informazio-sistemetako gertaerekin zerikusia duten intzidenteek, bai eta transakzio elektronikoetan esku hartzen duten dokumentu elektronikoen zaintza eta indarraldiaren kudeaketa desegokiak ere, lege-arazoak eragin ditzakete, eta Administrazioan bitarteko elektronikoak erabiltzeko inhibitzaile larria izan daitezke.

Todo ello es necesario porque la implementación del ENS es la garantía para mantener la validez legal de las transacciones electrónicas desarrolladas por medios presenciales o telemáticos. Los incidentes relacionados con eventos en los Sistemas de Información del Organismo, así como una inadecuada custodia y gestión de la vigencia de los documentos electrónicos que intervienen en las transacciones electrónicas, pueden derivar en problemas legales y pueden constituir un serio inhibidor en el uso de medios electrónicos en la Administración.

2. SORTA: Zibersegurtasunaren arloan udal-langileak prestatzeko eta kontzientziatzeko lanerako informatika-soluzioak hornitzea eta kudeatzea, eta plegu hauetan zehaztutakoaren arabera langileei zenbait prestakuntza-saio ematea.

LOTE 2: Suministro y gestión de las soluciones informáticas para el trabajo de formación y concienciación del personal municipal en materia de ciberseguridad, así como la impartición de varias sesiones de formación a los trabajadores según las especificaciones de

estos pliegos.

Segurtasunaren katebegirik ahulena enplegatua da beti, eta zibererasotzaileek arreta berezia eskaintzen diote. Beraz, segurtasuneko edozein estrategia osotan kontuan hartu behar da langile publikoek segurtasunaren eta zibermehatxuen arloan duten trebakuntza eta kontzientziazio egokia.

El eslabón más débil de la seguridad es siempre el empleado, al que los ciberatacantes dedican especialmente su atención, por lo que cualquier estrategia completa de seguridad debe tener en cuenta su adecuada capacitación y concienciación en materia de seguridad y ciberamenazas (de los empleados públicos).

Sorta honen esleipendunak prestakuntza-plan bat aurkeztu beharko du. Plan horretan, udaleko langileekin aurrez aurreko saioak (gutxienez 2) eta prestakuntzako tutorialak emango dituen software espezifiko bat bilduko dira, bai eta zibersegurtasun-erasoak simulatuko dituzten probak edo testak ere, langileak arlo horietan duen ezagutza eta portaera hobetzeko.

El adjudicatario de este lote tendrá que presentar un plan de formación que incluya una combinación de al menos dos sesiones presenciales con los empleados del ayuntamiento y un software especifico que proporcione tutoriales de formación, así como pruebas o test que simulen situaciones de ataques de ciberseguridad que deriven en la mejora del conocimiento y comportamiento del empleado en estas materias.

Arrasateko Udalean zibersegurtasuneko mehatxuen egungo maila neurtu da, baita mehatxu horiek gauzatzeak eskaintzen dituen zerbitzuen jarraitutasunean izango lukeen eragina ere. Horregatik, udalak aurrera egin behar du, ez bakarrik langileei zuzendutako kontzientziazio-ekintzetan, baizik eta haien alerta-maila, horien eraginkortasuna eta bilakaera neurtzeko gai izan behar du, ingurunera egokitzeko.

En el ayuntamiento de Arrasate se ha medido el nivel actual de las amenazas en ciberseguridad y el impacto que tendría su materialización en la continuidad de los servicios que ofrece. Es por ello por lo que el ayuntamiento se ve obligado a avanzar no solo en las acciones de concienciación dirigidas a empleados, sino en ser capaces de medir su nivel de alerta, eficacia de estas y evolución para adaptarlas al entorno.

Kontzientziazio-ekintzak benetan eraginkorrak izan daitezen, beharrezkotzat jotzen da plataforma automatizatu bat izatea, honako hauek ahalbidetuko dituena:

Para que las acciones de concienciación sean realmente efectivas se considera necesario disponer de una plataforma automatizada que permita:

- Arrasateko Udaleko pertsonen kontzientziazio-ekintzen eta alerta-mailaren arrisku-maila eta eraginkortasuna neurtzeko metrikak eta adierazleak izatea.
- Arrasateko Udaleko langileen zibersegurtasuneko alerta-egoera handitzea edo mantentzea.
- Talde espezifikoei zuzendutako ekintza-planak egitea eta prestakuntza-jarduerak egitea, hainbat formatutan.
- Kontzientziazio-hitzaldiak ematea erabiltzaileei eta goi-zuzendaritzari.

- Disponer de métricas e indicadores que permitan medir tanto el nivel de riesgo como la eficacia de las acciones de concienciación y el nivel de alerta de las personas del ayuntamiento de Arrasate.
- Aumentar o mantener el estado de alerta en ciberseguridad de los empleados del ayuntamiento de Arrasate.
- Elaborar planes de acción y realizar actividades de formación dirigidas a colectivos específicos en diferentes formatos.
- Realizar charlas de concienciación tanto a usuarios como a la alta dirección.

Goian adierazitakoaren zehaztapenak plegu tekniko hauetan zehaztuko dira.

Las especificaciones de lo indicado arriba se detallarán en estos pliegos técnicos.

3. SORTA: ENS izeneko ziurtagiri teknologikoa eskuratu ahal izateko ezarri beharreko jarraibideak zerrendatuko dituen aholkularitza lan bat kontratatzea.

LOTE 3: contratación de un trabajo de consultoría que enumere las pautas a seguir para la obtención del certificado ENS

Arrasateko Udalaren egungo egoera ezagutzeko txosten bat lortu nahi da, Segurtasun Eskema Nazionala arautzen duen 311/2022 Errege Dekretua betez Administrazio elektronikoko zerbitzuen ziurtagiria lortzeko, oinarrizko printzipioak eta gutxieneko baldintzak betetzen direla bermatuz.

Se pretende obtener un informe para conocer la situación actual del Ayuntamiento de Arrasate respecto a una próxima certificación de los servicios de Administración electrónica al cumplimiento del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, garantizando el cumplimiento de los principios básicos y requisitos mínimos.

40/2015 Legeak, urriaren 1ekoak, Administrazio Publikoek informazioaren teknologiak erabiltzeko duten betebeharra arautzen du, eta, horretarako, beren eskumenen barruan kudeatzen dituzten datuen, informazioen eta zerbitzuen erabilgarritasuna, benetakotasuna, osotasuna, konfidentzialtasuna eta trazabilitatea eta kontserbazioa bermatzen ditu.

La Ley 40/2015, de 1 de octubre, regula la obligación de las Administraciones Públicas de utilizar las tecnologías de la información asegurando la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Ildo horretan, Lege honek Segurtasunaren Eskema Nazionalarekiko betetze maila aztertzeko beharra ezartzen du, Eskema Nazionala arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuaren bidez garatu da.

En este sentido, esta Ley establece la necesidad de evaluar el cumplimiento del Esquema Nacional de Seguridad desarrollado a través del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Esleipendunak lanak egin beharko ditu udalak Segurtasun Eskema Nazionalaren ezarpenaren inguruan duen egoera jasoko duen txosten bat lortzeko, aipatutako arauek Arrasateko Udalari eskatzen dioten moduan, kontuan hartuta segurtasuna jarduera integraltzat hartu behar dela.

El adjudicatario deberá realizar labores para la obtención de un informe que refleje la situación del ayuntamiento respecto a una próxima implantación del Esquema Nacional de Seguridad en los términos exigidos al Ayuntamiento de Arrasate por las normas referenciadas, teniendo en cuenta que debe concebirse la seguridad como una actividad integral.

2. BALDINTZA OROKORRAK

2. CONDICIONES GENERALES

Kontratatutako zerbitzu guztiak Baldintza Teknikoen Agiri honetan, Administrazio Klausulen Agirian eta

Todos los servicios contratados serán proporcionados con estricta referencia a lo especificado en este Pliego

aukeratutako eskaintzaren edukian zehaztutakoa zehatz-mehatz aipatuta emango dira.

Hori dela eta, eskaintzaileek, aurkeztu beharreko dokumentazioaren barruan, eskainitako zerbitzu bakoitza zehaztu beharko dute, eta horiek gauzatzeko modua, edukia eta irismena zehaztu beharko dituzte.

3. NORAINOKOA

Sistemak udalaren azpiegitura informatikoan eta zerbitzu informatikoak erabiltzen dituzten udal-langileen gainean funtzionatu eta jardun beharko du.

4. BALDINTZA TEKNIKOAK

Proposatutako sistemek baldintza tekniko hauek bete beharko dituzte:

4.1. – 1 SORTA: Segurtasun-plataforma osatzen duten software, programa eta tresnen hornidura, ezarpena, mantentze-lanak, prestakuntza eta laguntza teknikoa.

Arrasateko Udalak, konpainiaren negozioaren jarraitutasuna bermatzeko bere informazio-sistemetan segurtasunak duen garrantziaz jabetuta, Segurtasun Eragiketen Zentro (SOC) baten laguntza behar du, Udalari laguntzeko bere babes-sistema perimetraletan ahalik eta eskuragarritasun eta eraginkortasunik handiena bermatzeko. Horretarako, informazioaren segurtasunaren arloko jardunbide onenak ezarri eta aplikatu behar ditu, lehendik ezagunak diren ureztatzeekiko esposizioa minimizatzeko, ezagutzen ez direnentzako babesa eta kanpoko nahiz barruko

de Prescripciones Técnicas y en el Pliego de Cláusulas Administrativas y en el contenido de la oferta seleccionada.

Por este motivo, los ofertantes deberán especificar, dentro de la documentación que se debe presentar, todos y cada uno de los diferentes servicios ofrecidos, definiendo su modo de ejecución, su contenido y su alcance.

3. ALCANCE

El sistema deberá funcionar y actuar sobre la infraestructura informática municipal, así como sobre los trabajadores municipales que hacen uso de los servicios informáticos.

4. REQUISITOS TECNICOS

Los sistemas propuestos deberán cumplir con los siguientes requisitos técnicos:

4.1. LOTE 1: Suministro, implantación, mantenimiento, formación y asistencia técnica de software, programas y herramientas que componen la plataforma de seguridad.

El Ayuntamiento de Arrasate consciente de la importancia que supone la seguridad en sus sistemas de información para garantizar la continuidad de negocio de la compañía, precisa contar con la ayuda de un Centro de Operaciones de Seguridad (SOC) que sirva de apoyo al Ayuntamiento para garantizar la máxima disponibilidad y eficacia en sus sistemas de protección perimetrales, estableciendo y aplicando las mejores prácticas en el ámbito de la seguridad de la información de cara a minimizar la exposición a riegos ya conocidos, la protección

balizko erasoak detektatu eta neutralizatzeko, bai eta Arrasateko Udalari beharrezko neurriak ezartzeko laguntza teknikoa ere, informazioaren segurtasunaren esparruan ENSak betetzen direla bermatzeko.

para los no conocidos y la detección y neutralización de posibles ataques tanto externos como internos, así como el apoyo técnico en la implementación de las soluciones para establecer las medidas necesarias que permitan al Ayuntamiento de Arrasate garantizar el cumplimiento de ENS dentro del ámbito de la seguridad de la información.

Lehen sorta honetarako proposatzen diren produktuak eta osagaiak Zentro Kriptografiko Nazionalak (CCN) informazioaren eta komunikazioaren teknologien segurtasun-produktuei buruz argitaratutako katalogoan jaso beharko dira, behintzat ENS-ak adierazitako sailkapen ERTAINean.

https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

Los productos y componentes que se propongan en la solución que se plantee para este primer lote, deberán estar recogidas en el catálogo publicado por el Centro Criptográfico Nacional respecto a los productos de seguridad de las tecnologías de la información y la comunicación, al menos en categoría de ENS MEDIA.

https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

SIEMek sarean gertatzen diren segurtasun-gertaera guztiak biltzen ditu modu zentralizatuan, informazioa iturri askotatik jasotzen du, bildutako datuak zerrendatzen ditu eta informazio ugari erakusten du paneletan. Jasotako gertaera horien azken 30 egunetakoak gorde beharko dira gutxienez.

El SIEM Captura y recopila todos los eventos de seguridad que se producen en la red de forma centralizada, de recibe información desde una gran cantidad de fuentes, correlaciona los datos recogidos y muestra una amplia variedad de información en paneles. Deberán quedar registrados al menos los últimos 30 días de dichos eventos recogidos.

- SIEM (Security Information and Event Management), segurtasun-gertaerak denbora errealean aztertzeko.
- Sareko segurtasuneko gertaerak jasotzen dituen zunda.
- EDR soluzioarekin integratzea. Erabiltzaile-postuan anomaliak antzematea.

- SIEM (Security Information and Event Management) para análisis en tiempo real de los eventos de seguridad.
- Sonda e Seguridad que recoja los eventos de la red..
- Integración con la solución de EDR. Detección de anomalías en puesto de usuario.

- Gertaerak atxikitzeko gaitasuna, korrelaziorako. Ekitaldiak 12 hilabetez gordetzen dira, eta horietatik gutxienez 7 egun beroan egin behar dira (aurreko 7 egunetan IOCren argitalpena berrikusi ahal izateko eta Arrasateko Udalak eraginik izan zuen jakiteko).

- Capacidad de retención de eventos para su correlación. Se almacenan eventos durante 12 meses, de los cuales, al menos 7 días deben realizarse en caliente (para poder revisar la publicación de IOC en los 7 días anteriores y saber si el Ayuntamiento de Arrasate se vio afectado).

Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

Hala, SOCak, bere SIEMen eta lotutako gainerako tresnen bidez, Arrasateko Udalaren testuingurura egokitutako prebentzio-, detekzio- eta erantzun-zerbitzu ezin hobea eskaintzeko beharrezkoak diren iturri guztiak integratzen eta monitorizatzen ditu.

SOC/SIEMen integratu beharreko iturriak:

- 2 Firewall FortiGate 100F
- Identifikazio tresna: Microsoft Active Directory.
- Antibirusa/EPP
- Zerbitzariak (monitorizazioa eta alertak soilik)
- Birtualizazio sistemak: VMWARE.
- Segurtasun kopia sistemak: Veeam Backup.
- Ofimatika tresnak: Microsoft Office 365

250 postu eta zerbitzariak kudeatzeko antibirus /EPP lizentziak sartzea + Windows duten sistema partxeak eguneratuta mantenduko dituen irtenbidea
Gutxi gorabeherako ondorioetarako, SIEM soluzioak 2.000 EPS gehitzen ditu (gertaerak segundoko).

- SIEM soluzioak gutxienez 15 iturri mota hartzea ahalbidetuko du.
- SIEM soluzioak 6.000 arau baino gehiago izango ditu, eta arau horietako gutxienez 250ek aldi berean funtzionatzea ahalbidetuko du.
- SOCak iturri berriak gehitu ahal izango ditu pixkanaka, Arrasateko Udalak egin ditzakeen gomendioei eta/edo Arrasateko Udalak eskuratzen dituen zibersegurtasuneko soluzio berriei erreparatuta.

- Gertaeren analisiaren funtzionaltasunerako, produktua gai da bildutako datuak definitutako arauen arabera aztertzeko, bidegabeko erabilerak edo jarduera maltzurrak identifikatzeko, eta analisien emaitza erregistratzeko.

- Produktuak ez du kredentzialik gordetzen memoria ez-hegazkorrean.

Así, El SOC, a través de su SIEM y resto de herramientas asociadas, integra y monitoriza todas aquellas fuentes que resultan necesarias para proporcionar un servicio de prevención, detección y respuesta óptimo y adaptado al contexto del Ayuntamiento de Arrasate.

Fuentes para integrar en el SOC/SIEM:

- 2 Firewalls FortiGate 100F
- Herramienta de identidad Microsoft Active Directory.
- Antivirus/EPP
- Servidores (solo monitorización y alertas)
- Sistemas de virtualización: VMWARE
- Sistemas de Backup: Veeam Backup.
- Herramientas de ofimática: Microsoft Office 365

Incluir licencias Antivirus/EPP para 250 puestos y servidores + solución actualizador parches de Windows
A efectos estimativos, la solución SIEM agrega 2.000 EPS (eventos por segundo).

- La solución SIEM permitirá la ingesta de al menos 15 tipos de fuentes diferentes.
- La solución SIEM dispondrá de más de 6.000 reglas y permitirá que al menos 250 de estas reglas funcionen de forma simultánea.
- El SOC podrá incorporar progresivamente nuevas fuentes, atendiendo a su vez a las recomendaciones que pueda realizar el Ayuntamiento de Arrasate y/o a las nuevas soluciones de ciberseguridad que adquiera el Ayuntamiento de Arrasate.

- Para la funcionalidad de análisis de eventos, el producto es capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos o actividades maliciosas, registrando el resultado de los análisis.

- El producto no almacena ninguna credencial en claro en memoria no volátil.

Ekitaldien analisiaren eta korrelazioaren funtzionaltasunerako, produktuak biltegiratutako gertaerak baimenik gabeko sarrera, aldaketa eta ezabaketetatik babesten ditu, eta biltegiratze-espazioa betetzeagatik gertaerak galtzea prebenitzen du.

Para la funcionalidad de análisis de eventos y correlación, el producto protege los eventos almacenados de accesos, modificaciones y borrados no autorizados, así como previene la pérdida de eventos por el llenado del espacio de almacenamiento.

Soluzioak irentsitako logen guztizko multzoaren eguneroko segurtasun-kopia bat izango du, haien erabilgarritasuna ziurtatzeko eta erregistroak galtzea ekar dezaketen kontingentziak estaltzeko. Backup hori hornitzaileak emandako kanpo-kokapen batean dago, SIEM tresnaren beraren kokapenaz bestelakoa, eta kokapen horren segurtasuna egiaztatzen du. Babeskopiek logak osorik berreskuratzea ahalbidetzen dute, 12 hilabeteko atxikipen-epearekin.

La solución contará con una copia de seguridad diaria del conjunto total de logs ingestados para asegurar su disponibilidad y cubrir posibles contingencias que pudieran suponer una pérdida de los registros. Dicho backup está alojado en una ubicación externa proporcionada por el proveedor, diferente a la ubicación de la propia herramienta de SIEM, acreditando la seguridad de dicha ubicación. Las copias de seguridad permiten una recuperación completa de los logs con un plazo de retención de 12 meses.

KPIak eta aginte-taula (dashboards) argiak eta konfiguratzeko errazak izango dira, Arrasateko Udalaren zibersegurtasun-egoera erakusteko.
Kudeatutako segurtasun-zerbitzua Segurtasun Eragiketen Zentro (KSA) batek eman beharko du 24x7x365ean.

Se dispondrá de KPIs y cuadros de mando (dashboards) claros y fáciles de configurar para mostrar el estado de ciberseguridad del Ayuntamiento de Arrasate.
El servicio de Seguridad Gestionada deberá ser prestado desde un Centro de Operaciones de Seguridad (SOC) en 24x7x365.

Zerbitzuaren barruan, adjudikaziodunak segurtasun-ekitaldiak eta -informazioa (SIEM, Security Information and Event Management) kudeatzeko zerbitzu bat eskaini beharko du, mehatxu informatikoak modu automatizatuan azkar detektatzeko, erantzuteko eta neutralizatzeko gai izango dena, gorabeheren aurreko erantzuna automatizatzeko plataformarekin integratuta, joerak errazago detektatzeko eta ohiz kanpoko ereduetan zentratzeko. SIEM sistemaren barruan, firewall-etatik eta sareko zundetatik datozen ekitaldiak integratu beharko dira, baina Arrasateko Udalak beste sistema batzuetako gertaerak integratzeko eskatu ahal izango du, hala nola antispam, postuko antibirus, zerbitzari eta abarrekoak.

Dentro del servicio, el adjudicatario deberá ofrecer un servicio para la gestión de eventos e información de seguridad (SIEM, Security Information and Event Management) capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas de forma automatizada, integrado con la plataforma para automatizar la respuesta ante incidentes, de forma que resulte más fácil detectar tendencias y centrarse en patrones fuera de lo común. Dentro del sistema SIEM deberán integrarse eventos provenientes de los firewalls y de las sondas de red, si bien El Ayuntamiento de Arrasate podrá solicitar la integración de eventos de otros sistemas tales como antispam, antivirus de puesto, servidores, etc.

Kudeatutako segurtasun-zerbitzua Arrasateko Udalaren segurtasun-plataformaren monitorizazio-zerbitzu iraunkor bat da (24x7x365). Esleipendunaren KSArekiko konexioa IPsec tunel seguru baten bidez egingo da, eta esleipendunaren kontura izango da Arrasateko Udalaren KSAn Datuak Prozesatzeko

El servicio de Seguridad Gestionada se trata de un servicio permanente de monitorización (24x7x365) de la plataforma de seguridad del ayuntamiento de Arrasate, la conexión con el SOC del adjudicatario se realizará mediante un túnel seguro IPsec, siendo por cuenta del adjudicatario el coste de las comunicaciones

Zentroarekin konektatzeko behar diren komunikazioen kostua. Zerbitzu horrek honako hauek eskainiko dizkio Arrasateko Udalari:

- Logen kudeaketa:

a) Merkatu-fabrikatzaile nagusiekin eta haien elementuekin integratzea. Elementu horietako batzuk dira: firewall-ak, WAF, IDS/IPS, kulunkagailuak, sare-ekipoak, zerbitzariak, lanpostuko segurtasuna eta EDR, CLOUD aplikazioak (Office365,...), posta elektronikoaren babesa, etab.

b) Arrasateko Udalak bere sistemen logs guztiak ikusi ahal izango ditu web kontsolan, behar bezala ordenatuta, sailkatuta eta bilaketa erraz eta intuitiboarekin.

c) Gordetako logak urtebete arte zaintzea, lege-ondorioetarako. Erabiltzailea identifikatzeko, Arrasateko Udalak Firewall dauka, FSSO bidez Direktorio Aktiboarekin integratua.

- Ekitaldien korrelazioa:

Esleipendunak zerbitzu hau eskaini beharko du:

a) Jasotako gertaerak bi zutabetan oinarritutako gertakariak detektatzeko prozesatzen dira: SIEMen euskarri den adimen artifizialaren gaitasun analitikoa, eta datuak adimen-hornitzaileekin gurutzatzea.

b) Alertak sortzen ditu intzidenteren bat detektatzen denean, eta ahalik eta gehien murrizten du erantzuteko denbora.

c) Identifikatu gertaera mota bakoitza denbora errealean, aurrez konfiguratutako erabilera-kasuekin, gehi kontuan hartzen dituzun erabilera-kasuak sortzeko gaitasuna. Esleipendunak zerbitzu bat eskaini beharko du, Arrasateko Udalak bere sistemen segurtasun-informazio guztia ikusi ahal izan dezan. Horrela:

a) Edozein segurtasun-gorabehera edo -mehatxu identifikatzea.
b) 2.000 ep-eko bolumetria.
c) Eragiketa eta erantzuna:

necesarias en su SOC para interconectar con el CPD del Ayuntamiento de Arrasate, dicho servicio ofrecerá a El Ayuntamiento de Arrasate:

- Gestión de logs:

a) Se integre con los principales fabricantes de mercado y sus elementos. Algunos de estos elementos son: firewalls, WAF, IDS/IPS, balanceadores, equipos de red, servidores, seguridad en el puesto y EDR, aplicaciones CLOUD (Office365, …), protección de correo electrónico, etc.

b) El Ayuntamiento de Arrasate podrá ver en consola web todos los logs de sus sistemas, debidamente ordenados, clasificados y con una búsqueda sencilla e intuitiva.

c) La custodia hasta 1 años de los logs almacenados para efectos legales. Para identificar al usuario, El Ayuntamiento de Arrasate dispone del Firewall integrado con el Directorio Activo mediante FSSO.

- Correlación de eventos:

El adjudicatario deberá ofrecer un servicio que:

a) Los eventos recibidos sean procesados para detectar incidentes basados en dos pilares; La capacidad analítica de la inteligencia artificial que da soporte al SIEM, y el cruce de los datos con proveedores de inteligencia.

b) Genere alertas cuando se detecte un incidente, reduciendo al máximo el tiempo de respuesta.

c) Identifique cada tipo de evento en tiempo real, con casos de uso preconfigurados más la capacidad de generar los casos de uso que considere. El adjudicatario deberá ofrecer un servicio que permita a El Ayuntamiento de Arrasate tener visibilidad de toda la información de seguridad de sus sistemas, de tal forma que:

a) Identifique cualquier incidencia o amenaza de seguridad.
b) volumetría de 2.000 eps.
c) Operación y respuesta:

d) Arrasateko Udalaren segurtasunari eragin diezaioketen mehatxuei aurrea hartu eta arindu.
e) Kontratuaren irismenaren barruan elementuen segurtasunaren kudeaketa kanpora ateratzeko aukera ematea.
f) Segurtasunaren, sistemen eta telekomunikazioen arloko aditu-talde batek emango du zerbitzua.

g) Jarduera segurtasun-sistemetara mugatuko da (firewall-ak, antibirusak, WAF, EDR, etab.). IT sistemak (Cloud zerbitzariak, etab.) Arrasateko Udalak kudeatuko ditu, eta erabateko koordinazioa izango du harekin. Hau da, KSAk elementu horiek monitorizatuko ditu eta alertak sortuko ditu, baina ez die eragingo.

h) Esleipendunak 24x7x365 zaintza- eta eragiketa-zerbitzua eskaini beharko du, zerbitzuan sartutako gailuen segurtasuna zaintzeko, segurtasun-arriskuak murrizteko eta gorabeheren aurrean erantzuna bizkortzeko.

- Ikuspena:

i) Dashboard bat izango da, atzemandako logei, alertei, kalteberatasunei eta abarri buruzko datuak kontsultatzeko. Dashboarderako sarbidea web motakoa izango da.
j) Teknikarien jardunari buruzko informazioa eskuratu beharko du, tiketen jarraipena egiteko tresna baten bidez.

- Gainera, zerbitzuak honako hauek eskaini beharko ditu:
- Euskarri teknikoa Arrasateko Udaleko Eraldaketa Digitala Sailari plataforma konfiguratzeko eta kudeatzeko zereginetan.

Konfigurazioa eta arkitektura hobetzeko proposamenak. Arrasateko Udalak bikaintasuna nahi du konpainiaren segurtasunaren kudeaketan, eta, beraz, esleipendunari lan proaktiboa eskatzen dio euskarri-zerbitzuari dagokionez.
- Sarea aztertzeko eta portaera anomaloa eta segurtasun-arriskuak antzemateko zunda hornitu eta instalatzea, denbora errealeko abisuekin.

d) Prevenga y mitigue las amenazas que pueden afectar a la seguridad del ayuntamiento de Arrasate.
e) Permita externalizar la gestión de la seguridad de los elementos dentro del alcance del contrato.
f) El servicio se preste por un equipo de personas expertos en Seguridad, Sistemas y Telecomunicaciones.

g) La actuación estará limitada a los sistemas de seguridad (firewalls, antivirus, WAF, EDR, etc). Los sistemas IT (servidores Cloud, etc) serán gestionados por El Ayuntamiento de Arrasate, con quién existirá plena coordinación. Es decir, el SOC monitorizará estos elementos y generará alertas, pero no actuará sobre ellos.

h) El adjudicatario deberá ofrecer un servicio de vigilancia y operación 24x7x365 de la seguridad de los dispositivos incluidos en el servicio, que permita reducir los riesgos de seguridad y acelerar la respuesta ante incidentes.

- Visibilidad:

i) Se dispondrá de un dashboard donde consultar datos referentes a los logs detectados, alertas, vulnerabilidades, etc. El acceso al dashboard será mediante una interfaz web.
j) Deberá tener acceso a la información de la actuación de los técnicos, mediante una herramienta de seguimiento de tiques.

- Además, el servicio deberá ofrecer:
- Soporte técnico al departamento Transformación Digital del ayuntamiento de Arrasate en las tareas de configuración y gestión de la plataforma.

- Propuestas de mejora sobre la configuración y arquitectura. El Ayuntamiento de Arrasate persigue la excelencia en la gestión de la seguridad de la compañía, por lo que requiere del adjudicatario un trabajo proactivo en cuanto al servicio de soporte.
- Suministro e instalación de Sonda de análisis de red y detección de comportamiento anómalo y riesgos de seguridad, con avisos en tiempo real.

• Kanpoko etengabeko kalteberatasunen analisia eta kudeaketa, Arrasateko Udalak azaldutako IP helbideetara, SIEMen integratuta, eta horiek zuzentzeko koordinazioan lagunduta.

• Análisis y gestión de vulnerabilidades continuo externo, a las direcciones IP expuestas del ayuntamiento de Arrasate, con integración en el SIEM, y soporte en la coordinación para la subsanación de estas.

• Gailuen auditoria. Esleipendunak plataformaren auditoria bat egin beharko du, eta, bertan, firewall arauak, segurtasun-profilak, argitaratutako zerbitzuak, baimendu gabeko sarbide-saiakerak, memoriaren erabilera, errendimendua eta konfigurazioa berrikusi beharko dira, gutxienez urtean behin. Esleipendunak auditoria horren txosten bat aurkeztu beharko du, hartu beharreko ekintzak kritikotasunaren arabera sailkatzeko. Txostenak. Astean behin eta/edo hilean behin, esleipendunak txostenak bidaliko dizkio Arrasateko Udalari. Txosten horietan, gutxienez, honako informazio hau agertuko da modu grafiko eta ordenatuan: Hilero txosten bat egingo da, gutxienez honako hauek zehaztuz: egoera orokorra, gertaera aipagarriak, segurtasunari eta sistemei buruzko adierazleak, proposatutako hobekuntza-ekintzak, artatutako gorabeherak, denborak eta hartutako konponbideak.

• Auditoria de los dispositivos. El adjudicatario deberá realizar una auditoría de la plataforma, que incluya la revisión de reglas de firewall, perfiles de seguridad, servicios publicados, intentos de acceso no autorizados, uso de memoria, rendimiento y su configuración; con una periodicidad al menos anual. El adjudicatario deberá entregar un informe de dicha auditoría donde se clasifiquen las acciones a tomar en base a la criticidad. Informes. Con periodicidad semanal y/o mensual el adjudicatario remitirá al Ayuntamiento de Arrasate informes en los que se muestre de forma gráfica y ordenada como mínimo la siguiente información: Mensualmente se emitirá un informe en el que se deberán detallar, al menos, el estado global, los eventos destacables, indicadores sobre la seguridad y sistemas, acciones de mejora propuestas, así como las incidencias atendidas, los tiempos y soluciones adoptadas.

• Konfigurazioaren eguneroko backupa: Esleipendunak segurtasun-ekipoen eta horien konfigurazioen eguneroko segurtasun-kopia bat egin beharko du. Kopia horiek esleipendunak zaindu beharko ditu, eta Arrasateko Udalaren esku utzi, hala eskatzen zaienean. Kopia horiek matxura baten aurrean ingurua lehengoratzeko erabiliko dira, eta horretarako ez dute Arrasateko Udaleko langileek esku hartu beharko. Esleipendunak plataformaren konfigurazioari buruzko backup bat egin beharko du egunero, 23:00etatik aurrera. Esleipendunak gutxienez azken 3 hilabeteetako backuparen kopia bat mantendu beharko du. Kopia hori Arrasateko Udalaren instalazioetatik kanpo gorde beharko da, baina eskuragarri, eskatuz gero.

• Backup diario de la configuración: El adjudicatario deberá realizar una copia de seguridad diaria de los equipos de seguridad y sus configuraciones. Estas copias deberán ser custodiadas por el adjudicatario y puestas a disposición del ayuntamiento de Arrasate cuando sean requeridas. Estas copias serán empleadas para la restauración del entorno ante una avería, sin que para ello deba intervenir el personal del ayuntamiento de Arrasate. El adjudicatario deberá realizar un Backup de la configuración de la plataforma a partir de las 23:00 horas cada día. El adjudicatario deberá mantener una copia del Backup como mínimo de los últimos 3 meses. Esta copia deberá almacenarse fuera de las instalaciones del ayuntamiento de Arrasate, pero accesible si se solicita.

• Firmwareen eta adabakien eguneraketak kudeatzea: Esleipendunak plataforman beharrezkoak diren eguneraketak eta adabakiak kudeatu beharko ditu, ahalik eta operatibitate eta prestazio gehien

• Gestión de actualizaciones de firmware y parches: El adjudicatario deberá realizar la gestión de actualizaciones y parches necesarios en la plataforma para garantizar el máximo nivel de operatividad y

bermatzeko; sartutako hobekuntzei buruzko informazio zehatza eman beharko du.

• Gorabeheren kudeaketa:
Enpresa esleipendunak, ezarritako kanalen bidez, Arrasateko Udalaren zerbitzuan edo zibersegurtasun-egoeran eragina duen edozein gorabeheraren berri ematen die eskalatzeko eta erabakiak hartzeko prozesuan parte hartzen duten Arrasateko Udaleko solaskideei.

• Euskarri aditu bat ematen da jakinarazitako segurtasun-gorabeheren edo -gorabeheren aurrean.
• Egungo Zerbitzu Mailari buruzko Akordioa (SLA.ANS Helburua):

Intzidentzia baten aurrean erantzuteko gehieneko denbora: 60 minutu
1. mailako intzidentzia ebazteko gehienezko denbora (zerbitzurik gabe) 8 lanordu
2. mailako intzidentzia ebazteko gehieneko denbora: (errendimendua edo beste baldintza batzuk, baina zerbitzua emanez) 24 lanordu
3. mailako intzidentzia ebazteko gehienezko denbora (gainerako gorabeherak) 48 lanordu
Informazio-eskaeren aurrean erantzuteko gehieneko denbora 24 lanordu
Zerbitzu berriak instalatzen direnean erantzuteko gehieneko denbora: 7 egun

BARNE-SAREKO ZUNDAK
Adjudikaziodunak Arrasateko Udaleko DPZ bakoitzean zunda bat hornitu eta inplementatu beharko du, inolako kosturik gabe, honako hauek detektatu ahal izateko: sare-eskaneatzeak, spiderrak, programa gaiztoak banatzeko saiakerak, ransomwarea, TOR sarearekiko konexioak, proxie-ekiko konexioak, gune edo domeinu berriekiko edo ospe txikikoekiko konexioak, DNSei legez kanpoko eskaerak, esplorazio masiboak, erasotzaile anonimoak, zerbitzuen aurkako erasoak, programa gaiztoak, etab.

Zerbitzu honen bidez, sare anomaloen trafikoan portaerak detektatu nahi dira, eraso ezagunen sinadurekin edo portaera susmagarriekin alderatuta, hala nola portuen eskaneatzea, pakete malformatuak,

prestaciones; ofreciendo información detallada de las mejoras incluidas.

• Gestión de Incidencias:
La empresa adjudicataria notifica, mediante los canales establecidos, a los interlocutores del Ayuntamiento de Arrasate que forman parte del proceso de escalado y toma de decisiones cualquier incidencia que afecte al servicio o bien al estado de ciberseguridad del Ayuntamiento de Arrasate.

• Se proporciona un soporte experto ante las incidencias o incidentes de seguridad notificados.
• Actual Acuerdo de Nivel de Servicio (SLA.ANS Objetivo):

Tiempo máximo de respuesta ante una incidencia 60 minutos
Tiempo máximo para resolución de incidencia de Nivel 1 (sin servicio) 8 horas laborales
Tiempo máximo para resolución de incidencia de Nivel 2: (rendimiento u otras condiciones, pero dando servicio) 24 horas laborales
Tiempo máximo para resolución de incidencia de Nivel 3 (resto de incidencias) 48 horas laborales
Tiempo máximo de respuesta ante peticiones de información 24 horas laborales
Tiempo máximo de respuesta ante instalación de nuevos servicios 7 días

SONDAS DE RED INTERNA
El adjudicatario deberá suministrar e implementar, sin coste alguno, una sonda en cada CPD del ayuntamiento de Arrasate, que permita detectar: escaneos de red, Spiders, intentos de distribución de programas malignos, ransomware, conexiones con Red TOR, conexiones con proxies, conexiones a sitios o dominios nuevos o de baja reputación, peticiones ilegales a DNS, exploraciones masivas, atacantes anónimos, ataques a servicios, programas malignos, etc.

Mediante este servicio se pretende detectar comportamientos en el tráfico de red anómalos comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el

etab.
Zundak sarearen kalitatea eta trafikoa edo zer trafiko mota den monitorizatzeaz gain, edukia eta portaera ere aztertzen ditu.

escaneo de puertos, paquetes malformados, etc.
La sonda no solo monitorizará la calidad y el tráfico de red o qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

Jarduera susmagarriari emandako erantzunaren bidez, KSA zerbitzuak firewall konfiguratu ahal izango du erasotzailearen saretik edo IPtik datorren trafikoa blokeatzeko.
Sistemak mehatxuak detektatzeko mekanismoak izango ditu, horizontalak zein bertikalak, bai eta logak eta monitorizazio-ekitaldiak biltegiratzeko, biltzeko eta aztertzeko gaitasuna ere.
Zundaren datu guztiak SIEMen egongo dira eskuragarri, eta, beraz, Arrasateko Udalak eskuragarri izango ditu web interfaze baten bidez.

La respuesta a la actividad sospechosa permitirá al servicio de SOC configurar el firewall para que bloquee el tráfico que proviene de la red o IP del atacante.
El sistema dispondrá de mecanismos de detección de amenazas tanto horizontales como verticales y capacidad de almacenamiento, recolección y análisis de logs y eventos de monitorización.
Todos los datos de la sonda estarán disponibles en el SIEM, y por lo tanto accesibles al Ayuntamiento de Arrasate a través de una interfaz web.

SEGURTASUN-EKIPOEN KONFIGURAZIOAREN AUDITORIA

TI segurtasun-sistemak (Firewalls, WAF, IDS/IPS, Antimalware, AntiSPAM, etab.) beharrezkoak dira IT sistemek zaintzen duten informazioan gutxieneko segurtasun-neurriak izateko. Gauza bera gertatzen da zerbitzarien, sistemen eta aplikazioen sistema eragileen berezko segurtasun-neurriekin.

AUDITORIA DE CONFIGURACION DE EQUIPOS DE SEGURIDAD

Los sistemas de seguridad TI (Firewalls, WAF, IDS/IPS, Antimalware, AntiSPAM, etc) son necesarios de cara a disponer de las medidas de seguridad mínima en la información custodiada por los sistemas de TI. Lo mismo sucede con las medidas de seguridad intrínsecas a los sistemas operativos de servidores, sistemas y aplicaciones.

Hala ere, konfigurazio txar batek edo konfigurazio zaharkitu batek segurtasunean arrakalak eragin ditzake, babestu beharreko aktiboen eraginpean gera daitezen.

No obstante, una mala configuración, o una configuración obsoleta, puede ocasionar brechas en la seguridad que dejen expuestos los activos a proteger.

Arrasateko Udalak lortu nahi duen helburu nagusia bere sistemen segurtasun-egoera ezagutzea da, sistema horien gainean konfigurazio egokia egiteko.

El objetivo fundamental perseguido por el Ayuntamiento de Arrasate es conocer el estado de seguridad de sus sistemas, al objeto de realizar la adecuada configuración sobre los mismos.

Ikuskapenean, dauden segurtasun-elementuak aztertuko dira, helburu hauek lortzeko:

Durante la auditoría, se analizarán los elementos de seguridad existentes, persiguiendo los siguientes objetivos:

Gailuei buruz
o Hardware elementuen zaharkitzea identifikatzea, eta instalatutako sistemak Arrasateko Udalaren azpiegiturarako egokiak diren identifikatzea.
o Segurtasun-sistemen software-bertsioen eguneratze-maila identifikatzea

Acerca de los dispositivos
o Identificar la obsolescencia de elementos hardware, y si los sistemas instalados son los adecuados a la infraestructura del Ayuntamiento de Arrasate
o Identificar el grado de actualización de las versiones software de los sistemas de seguridad

o Harpidetza-zerbitzuak (lizentziak, sinadurak, etab.) behar bezala konfiguratuta daudela eta sistemak behar bezala eguneratzen direla egiaztatzea.

Arkitekturari buruz
o Elementuen interkonexio-arkitektura optimoa den identifikatzea
o Erabilgarritasun handiko parametrizazio egokia (HA) badago, identifikatu.

Elementuen konfigurazio orokorra identifikatzea egokia da:
o Rolak eta erabiltzaileak
o Syslog eta beste txosten batzuk
o Data/ordua sinkronizatzea
o DNSak
o Routinga eta sarea
o etab.

Segurtasun-arauak identifikatzea
o Erabiltzen ez diren arauak identifikatzea
o Arau hilak identifikatzea (ezinezkoa baita trafiko bat harekin bat etortzea)
o Zehaztasun gutxiko arauak identifikatzea (any, all, etab.)
o Ohikoak ez diren edo arrisku handikoak diren protokoloen trafikoa ahalbidetzen duten arauak identifikatzea

Eragiketari buruz:
o Arau bakoitzaren arduradunaren/eskatzailearen identifikazioa.
o Backup eta berreskuratze-prozesuak identifikatzea
o Ekipoei aplikatutako jarraitutasun-planak identifikatzea
o Auditoretza-rolak identifikatzea

Gainera, sarearen diseinuak fabrikatzaileen diseinu-arauak betetzen dituen eta ISO 27001, PCI-DSS, Segurtasun Eskema Nazionala edo DBEO bezalako segurtasun-araudiekin koherentea den identifikatu nahi da.

o Comprobar que los servicios de suscripción (licencias, firmas, etc.) están correctamente configurados y los sistemas se actualizan debidamente

Acerca de la arquitectura
o Identificar si la arquitectura de interconexión de los elementos es la óptima
o Identificar, si existe, la adecuada parametrización de alta disponibilidad (HA)

Identificar la configuración general de los elementos es la adecuada:
o Roles y usuarios
o Syslog y otros reportes
o Sincronización de fecha/hora
o DNS's
o Routing y red
o etc

Identificación de reglas de seguridad
o Identificación de reglas en desuso
o Identificación de reglas muertas (por ser imposible que un tráfico coincida con ella)
o Identificación de las reglas poco específicas (any, all, etc)
o Identificación de reglas que permitan tráfico de protocolos poco habituales o de alto riesgo

Acerca de la operación:
o Identificación del responsable/solicitante de cada una de las reglas.
o Identificación de procesos de backup y recuperación
o Identificación de Planes de Continuidad aplicados a los equipos
o Identificación de roles de auditoría

Se desea además identificar si el diseño de la red cumple las buenas prácticas definidas las reglas de diseño de fabricantes y si es coherente con normativas de seguridad como ISO 27001, PCI-DSS, Esquema Nacional de Seguridad o RGPD.

KALTEBERATASUNAK AZTERTZEKO ZERBITZUA

SERVICIO DE ANÁLISIS DE VULNERABILIDADES

Prebentziozko babesa eta babes zuzentzailea behar bezala planifikatzeko, kalteberatasunen azterketa funtsezko jardueratzat hartu behar da. Zerbitzu honek IT sistemek dituzten kalteberatasunen berehalako ikuspen globala eskainiko du, mehatxuak etengabe identifikatuko ditu eta sarean gertatzen diren ustekabeko aldaketak gainbegiratuko ditu, segurtasun-arrakala bihurtu aurretik.

Zerbitzu horretan, aldizkako analisi jarraituak eta errepikakorrak egingo dira; zaurgarritasun baten bizi-zikloa identifikatu eta jarraituko da, agertzen denetik erabat desagerrarazi arte, eta sistemen segurtasunerako babesgabetasun-denborak minimizatuko dira. Zerbitzuak urrakortasunen azterketa jarraitua izan beharko du, atzemandako kalteberatasunak zehatz-mehatz identifikatu eta sailkatzeko eta lehentasunen arabera ordenatzeko.

Arrasateko Udalak WEB interfazearen bidez eskura izango ditu dauden kalteberatasunak, honako parametro hauek neurtu ahal izateko:

- AHULTASUN KRITIKOEK, ALTUEK, ERTAINEK eta BAXUEK eragindako kopurua, mota eta aktiboa (GZEKren arabera sailkatuak)
- Kalteberatasunak zuzentzeko plangintza
- Kalteberatasunak konpontzeko batez besteko denbora
- Aktiboak elkartzea eta kudeatzea

Kalteberatasunak etengabe aztertzeko eta kudeatzeko zerbitzua Arrasateko Udalaren helbide publikoen tartean egingo da (Klase bat aurrizki luzerarekin/22: 255.255.252.0).

CIBER THREAT INTELLIGENCE (MEHATXUEN INTELIGENTZIA) ZERBITZUA

Esleipendunak honako ezaugarri hauek bete beharko ditu mehatxu zibernetikoak detektatzeko, aztertzeko eta horiei erantzuteko beharrak bermatzeko:

- Jabariaren babesa:

Enpresak gai izan beharko du phishing, identitate-ordezkapena, DNS pozoitzea, izenaren imitazioa

Para una correcta planificación de protección preventiva y correctiva se debe considerar el análisis de vulnerabilidades como una actividad clave. Se trata de un servicio que ofrezca visibilidad inmediata y global de las vulnerabilidades que presentan los sistemas de TI e identificar las amenazas de forma continua y supervisar los cambios inesperados que se produzcan en la red antes de que se conviertan en brechas de seguridad.

Este servicio consistirá, mediante análisis periódicos, continuos y recurrentes; identificar y seguir el ciclo de vida de una vulnerabilidad desde que aparece hasta que sea completamente erradicada, minimizando los tiempos de desprotección para la seguridad de los sistemas. El servicio deberá incluir un análisis de vulnerabilidades continuo, para identificar y clasificar de forma precisa las vulnerabilidades detectadas y permita ordenarlas por prioridades.

El Ayuntamiento de Arrasate tendrá acceso, vía interfaz WEB a las vulnerabilidades existentes, para poder medir parámetros tales como:

- Número, tipo y activo afectado por vulnerabilidades CRITICAS, ALTAS, MEDIAS y BAJAS (Clasificadas en base a CVSS)
- Planificación de la subsanación de vulnerabilidades
- Tiempo medio de subsanación de vulnerabilidades
- Agrupación y gestión de activos

El servicio de análisis y gestión de vulnerabilidades continuo se realizará sobre el rango de direcciones públicas del ayuntamiento de Arrasate (Una clase con longitud de prefijo /22: 255.255.252.0).

SERVICIO CIBER THREAT INTELLIGENCE (INTELIGENCIA DE AMENAZAS)

El adjudicatario deberá cumplir con las siguientes características para garantizar las necesidades de detección, análisis y respuesta a amenazas cibernéticas:

- Protección del dominio:

La empresa deberá ser capaz de identificar y mitigar amenazas relacionadas con dominios falsos que pueden

(typosquatting) eta beste eraso-metodo batzuetarako erabil daitezkeen domeinu faltsuekin lotutako mehatxuak identifikatzeko eta arintzeko.

Helburua da eremu faltsu horiek aldez aurretik detektatzea eta horien gainean jardutea, konfiantza irabazi eta kalteak eragin baino lehen. Baldintzak hauek dira:
Domeinu maltzurren detekzio goiztiarra: denbora errealean domeinu faltsuak monitorizatu eta detektatzeko sistemen inplementazioa.

- Maltzurrak izan daitezkeen eremuen sorrera eta bilakaera aztertzeko gaitasuna.
- Tipografia eta domeinu-izenen antzekotasuna aztertzeko teknika aurreratuak erabiltzea.

Ekintza zuzentzaileak:

- Maltzurtzat jotako eremuak blokeatzeko edo kontrolatzeko metodoak ematea.

- Domeinuetako erregistratzaileekin eta agintariekin lankidetzan aritzea iruzurrezko domeinuak desegiteko.

Txostenak eta alertak:

- Berehalako alertak sortzea domeinu susmagarriak detektatzen direnean.
- Domeinu maltzurren jarduerari eta hartutako ekintzei buruzko txosten zehatzak ematea.

Kontu eta pasahitz iragaziak: Enpresak gai izan behar du iragazitako kontuei eta pasahitzei buruzko informazioa trukatzen duten datu-iturriak eta kanalak denbora errealean monitorizatzeko, informazio sentikorraren esposizioari buruzko alerta goiztiarrak emanez.

Baldintzak hauek dira:
Denbora errealeko monitorizazioa:

- Tresna eta teknika aurreratuak erabiltzea foroak, sare sozialak eta datu konprometituak trukatzeko beste kanal batzuk etengabe eskaneatzeko.

Alerta goiztiarrak:

Bezeroa inplikatzen duen edozein kontu eta pasahitzen filtraziori buruzko berehalako alertak

ser utilizados para phishing, suplantación de identidad, envenenamiento de DNS, imitación del nombre (typosquatting) y otros métodos de ataque.

El objetivo es detectar y actuar con antelación sobre estos dominios falsos antes de que ganen confianza y puedan causar daño. Los requisitos son:
Detección Temprana de Dominios Maliciosos: Implementación de sistemas para monitorear y detectar dominios falsos en tiempo real.

- Capacidad para analizar la creación y evolución de dominios potencialmente maliciosos.
- Uso de técnicas avanzadas de análisis de tipografía y similitud de nombres de dominio.

Acciones Correctivas:

- Proveer métodos para bloquear o tomar control de los dominios identificados como maliciosos.

- Colaborar con registradores de dominios y autoridades para desmantelar dominios fraudulentos.

Reportes y Alertas:

- Generar alertas instantáneas cuando se detecten dominios sospechosos.
- Proveer informes detallados sobre la actividad de dominios maliciosos y las acciones tomadas.

Cuentas y contraseñas filtradas: La empresa debe tener la capacidad de monitorear en tiempo real fuentes de datos y canales que intercambian información sobre cuentas y contraseñas filtradas, proporcionando alertas tempranas sobre la exposición de información sensible.

Los requisitos son:
Monitoreo en Tiempo Real

- Utilización de herramientas y técnicas avanzadas para escanear continuamente foros, redes sociales, y otros canales donde se intercambian datos comprometidos.

Alertas Tempranas:

- Proveer alertas instantáneas sobre cualquier filtración de cuentas y contraseñas que involucre al

ematea.

• Iragazitako datuak bezeroaren barne-sistemekin zerrendatzeko gaitasuna, urratutako kontuak identifikatzeko.

Arintze-ekintzak:
• Konprometitutako kontuak berehala eguneratzeko eta babesteko gomendioak eta tresnak eskaintzea.
• Pasahitzen segurtasun-politikei eta faktore anitzeko autentifikazioari buruzko aholkularitza
• Programa gaiztoa detektatzea:
• Sandboxak monitorizatzea: Sandbox publiko eta pribatu nagusiak aldian behin kontsultatzea, bezeroarekin lotutako programa gaiztoa identifikatzeko.

• Programa gaiztoa aztertzea sinadura digitalak, testu-kateak eta bezeroaren domeinuetarako konexioak detektatzeko.
• Ordezkapena detektatzea:
• Edukiak eskaneatzea eta aztertzea, bezeroaren identitatea ordezteko ahalegina adierazten duten esaldi eta patroien bila.

• Balizko ordezkapen-mehatxuei buruzko alertak eta txosten zehatzak sortzea.
• Prebentzio-ekintzak:
• Konprometitutako ziurtagiriak baliogabetzeko gomendioak ematea.
• Ziurtagirien hornitzaileekin eta agintariekin lankidetzan aritzea, programa gaiztoa ez hedatzeko.

• Datuak iragaztea:
• Datu-iturriak monitorizatzea:
• Foroak, datuak trukatzeko sareak eta iragazketa-guneak etengabe zaintzea.
• Bezeroa inplikatzen duten dokumentuak eta datu pertsonalak identifikatzea.

• Alertak eta txostenak:
• Berehalako alertak ematea bezeroari eragiten dion edozein datu-filtraziori buruz.
• Filtrazioaren izaerari eta jatorriari buruzko txosten zehatzak sortzea.

cliente.

• Capacidad para correlacionar datos filtrados con los sistemas internos del cliente para identificar cuentas vulneradas.

Acciones de Mitigación:
• Ofrecer recomendaciones y herramientas para la inmediata actualización y protección de las cuentas comprometidas.
• Asesoramiento sobre políticas de seguridad de contraseñas y autenticación multifactor
• Detección de programa maligno:
• Monitoreo de Sandboxes: Consulta periódica de las principales sandboxes públicas y privadas para identificar programa maligno relacionado con el cliente.

• Análisis de programa maligno para detectar firmas digitales, cadenas de texto y conexiones a dominios del cliente.
• Detección de Suplantación:
• Escaneo y análisis de contenidos en busca de frases y patrones que indiquen intento de suplantación de la identidad del cliente.

• Generación de alertas y reportes detallados sobre posibles amenazas de suplantación.
• Acciones Preventivas:
• Proveer recomendaciones para la revocación de certificados comprometidos.
• Colaborar con proveedores de certificados y autoridades para evitar la propagación de programa maligno.

• Exfiltración de datos:
• Monitoreo de Fuentes de Datos:
• Vigilancia constante de fuentes como foros, redes de intercambio de datos, y sitios de filtraciones.
• Identificación de documentos y datos personales que involucren al cliente.

• Alertas y Reportes:
• Proveer alertas inmediatas sobre cualquier filtración de datos que afecte al cliente.
• Generar informes detallados sobre la naturaleza y origen de la filtración.

• Arintze-ekintzak: • Iragazketaren eragina arintzeko beharrezko neurriei buruzko aholkularitza.	• Acciones de Mitigación: • Asesoramiento sobre las medidas necesarias para mitigar el impacto de la filtración.
• Lege- eta segurtasun-erakundeekin lankidetzan aritzea, konprometitutako informazioa biltzeko eta ezabatzeko. • Enpresak bezeroaren domeinuetako datuak hainbat iturrirekin gurutzatzeko aukera izan behar du, iragazitako dokumentazio edo eduki sentikorra detektatzeko, datu pertsonalak, kredentzialak eta bezeroa arriskuan jar dezakeen bestelako informazioa barne. Baldintzak hauek dira: • Phishing denbora errealean monitorizatzea: Phishing detektatzea:	• Colaboración con entidades legales y de seguridad para contener y eliminar la información comprometida. • La empresa debe poder cruzar datos de dominios del cliente con múltiples fuentes para detectar documentación o contenido sensible filtrado, incluyendo datos personales, credenciales y otra información que pueda comprometer al cliente. Los requisitos son: • Monitorización de Phishing en tiempo real: Detección de Phishing:
• Phishing kanpainak goiz detektatzeko sistemak inplementatzea. • Phishing-erasoei buruzko informazioa maila globalean biltzen duten iturriak etengabe monitorizatzea. • Alertak eta blokeoa: • Bezeroari zuzendutako phishing saiakerei buruzko berehalako alertak ematea. • Eraso horiek blokeatzeko eta arintzeko tresnak eta estrategiak eskaintzea.	• Implementación de sistemas para la detección temprana de campañas de phishing. • Monitoreo continuo de fuentes que recopilan información sobre ataques de phishing a nivel global. • Alertas y Bloqueo: • Proveer alertas instantáneas sobre intentos de phishing dirigidos al cliente. Ofrecer herramientas y estrategias para bloquear y mitigar estos ataques.
• Txostenak eta analisiak: • Antzemandako phishing-saiakerei eta egindako ekintzei buruzko txosten zehatzak sortzea. • Phishing-erasoen joerak eta ereduak aztertzea, etorkizuneko defentsak hobetzeko.	• Reportes y Análisis: • Generar informes detallados sobre los intentos de phishing detectados y las acciones tomadas. • Análisis de tendencias y patrones de ataques de phishing para mejorar las defensas futuras.
• Enpresak gai izan beharko du bezeroari zuzendutako phishing-saiakerak denbora errealean monitorizatzeko, saiakuntza horiek identifikatuz eta blokeatuz kalte esanguratsuak eragin baino lehen. Baldintzak hauek dira: Enpresak bezeroaren ziurtagiriekin sinatutako programa gaiztoa identifikatzeko gai izan behar du, edo bezeroaren jabetzako domeinuak erabili behar ditu banaketarako. Gainera, identitate-ordezkapena adieraz dezaketen esaldiak eta kateak bilatu behar ditu.	• La empresa deberá ser capaz de monitorear en tiempo real los intentos de phishing dirigidos al cliente, identificando y bloqueando estos intentos antes de que puedan causar daños significativos. Los requisitos son: La empresa debe ser capaz de identificar programa maligno firmado con certificados del cliente o que utilice dominios propiedad del cliente para distribución. Además, debe realizar búsquedas de frases y cadenas que puedan indicar suplantación de identidad.
Erantzun-denbora maximoa analisian hautemandako larritasunaren eta arriskuaren araberakoa izango da.	El tiempo de respuesta máximo dependerá de la gravedad y el riesgo detectado en el análisis. Se

Zerbitzuaren denbora hauek definituko dira:

Zerbitzuaren helburu-denborak (SLT):

- Kasu bat sortzeko epe objektiboa: 2 minutu, detektatzen denetik.
- Hasierako erantzuna emateko epe objektiboa: 30 min kasua sortzen denetik.

Zerbitzuaren adostutako denborak (SLA):

- Erantzuteko denbora gehienez 60 minutukoa izango da, hileko larritasun handiko kasuen ehuneko laurogeita hamarrean gutxienez (% 90).

Espero den zerbitzuaren batez besteko denborak (hirugarren analistaren batek neurtuak)

- Detekzioa: minutu 1.
- Ikerketa: 25 minutu.
- Erremediatzea: 12 minutu.

Hitzak:

- *Detekzioa: gertaera gertatzen denetik sailkatu arte.*
- *Ikerketa: gertaera gertatzen denetik zerbitzu-arduradunari jakinarazi arte.*
- *Erremediatzea: gertaera gertatzen denetik SLAn zehaztutako erremediora arte (ekipoa blokeatzea, sarea isolatzea...).*

Erantzuteko gaitasuna: 24x7

Urteko 24 orduetan eta 365 egunetan guztiz monitorizatzeko aukera bermatzeko, zerbitzuak beharrezko kaudimena izan behar du, zibersegurtasun-intzidentziaren bat gertatuz gero ahalik eta baliabide gehien eskaintzeko. Horretarako, MDR zerbitzuaren hornitzaileak geografikoki sakabanatuta dauden operazio-zentroak edo SOCak izan behar ditu, ordu-tarte desberdinekin, eta horien ordu-aldea 12 ordukoa izango da kasuren batean.

Jarraipena eta erantzuna mehatxuen aurrean

MDR zerbitzuak zerbitzu proaktiboa eta erreaktiboa

definirán los siguientes tiempos del servicio:

Tiempos objetivo del Servicio (SLT):

- Plazo objetivo para la creación de un Caso: 2 minutos desde la detección.
- Plazo objetivo para la acción de respuesta inicial: 30 min desde la creación del caso.

Tiempos acordados del servicio (SLA):

- Tiempo de respuesta no superior a (60) minutos en, al menos, el noventa por ciento (90%) de los casos mensuales de gravedad alta.

Tiempos promedio del servicio esperados (medidos por algún analista tercero)

- Detección: 1 minuto.
- Investigación: 25 minutos.
- Remediación: 12 minutos.

Términos:

- *Detección: Desde que se produce el evento hasta su clasificación.*
- *Investigación: Desde que se produce el evento hasta su notificación al responsable de servicio.*
- *Remediación: Desde que se produce el evento hasta la remediación definida en SLA (bloqueo de equipo, aislamiento de red, …).*

Capacidad de respuesta 24x7

Con el fin de garantizar una disponibilidad total de monitorización las 24h del día y los 365 días del año, el servicio ha de contar con la solvencia necesaria que le permita ofrecer el máximo de recursos en caso de un incidente de ciberseguridad. Para ello el proveedor del servicio MDR debe contar con distintos centros de operaciones o SOC dispersos geográficamente con franjas horarias diferentes y cuya diferencia horaria alcance las 12 horas en alguno de los casos.

Seguimiento y respuesta ante amenazas

El servicio MDR ha de ser un servicio tanto proactivo

izan behar du, eta, bertan, mehatxuak bilatzeko lanak (etengabeko triajearen eta jarraipenaren bidez) ez ezik, erantzun- eta erremediatze-lanak ere sartu behar dira. Zerbitzuak gai izan behar du, gutxienez, zeregin mota hauei kaudimenez ekiteko:

- **Mehatxu proaktiboak bilatzea:**
  - Adimen artifizialeko tresnak erabiliz hobetutako triajea, giza taldearen esperientziarekin eta beste elementu batzuekin (OSINT, jarduera maltzurraren detekzioa.) konbinatuta, erantzun-denborak murrizteko eta detektatzeko gaitasuna hobetzeko eta, aldi berean, positibo faltsuen kopurua eta jakinarazpenen bolumena murrizteko.
  - Mehatxuen panoraman kritikoak diren eragile edo kalteberatasun berriei buruzko jakinarazpenak, bai kudeaketa-plataformaren bidez, bai hileroko saioen edo fabrikatzailearen mintegien bidez.

como reactivo, en el que se incluyan no solo tareas de búsqueda de amenazas mediante el triaje y seguimiento continuo sino también tareas de respuesta y remediación. El servicio ha de ser capaz de acometer con solvencia al menos los siguientes tipos de tareas:

- **Búsqueda de amenazas proactiva:**
  - Triaje mejorado mediante el uso de herramientas de Inteligencia Artificial, combinado con experiencia del equipo humano y otros elementos (OSINT, detección de actividad maliciosa.) que reduzcan los tiempos de respuesta y mejoren la capacidad de detección a la vez que se reduce el número de falsos positivos y el volumen de notificaciones.
  - Notificaciones acerca de nuevos actores o vulnerabilidades críticas en el panorama de amenazas tanto a través de la plataforma de gestión como a través de sesiones mensuales o seminarios del fabricante.

- **Gertaerei erantzutea:**

Gertakari aktibo baten aurrean, MDR zerbitzua osatzen duten langileek ahalik eta denbora laburrenean gauzatu beharko dituzte erasoa ahalik eta denbora laburrenean gelditzeko aukera ematen duten ekintzak. Hurrengo adibideek puntu honetan espero diren ekintza batzuk erakusten dituzte:

- Ekipo bat urrunetik isolatzea
- IPak host-mailan ahokatzea
- Prozesuak amaitzea
- Erabiltzaile-saioen deslogatua behartzea
- Ekipo baten erabiltzaile-kontuak

- **Respuesta a Incidentes:**

Ante un incidente activo el personal humano que compone el servicio MDR deberá ser capaz de ejecutar en el menor tiempo posible aquellas acciones que permitan detener el ataque en el menor tiempo posible. Los siguientes ejemplos muestran algunas de las acciones esperadas en este punto:

- Aislar un equipo de manera remota
- Boquear IPs a nivel de host
- Terminar procesos
- Forzar el deslogado de sesiones de usuario
- Deshabilitar cuentas de usuario de un

desgaitzea

- Artefaktu maltzurrak desagerraraztea
- Hasheak politika mailan blokeatzea

- **Gorabeherak konpontzea:**

Behin eraso bat geldituta, MDR zerbitzuak ez du amaitu behar erantzunean duen esku-hartzea; aitzitik, intzidentea erremediatzeaz ere arduratu behar du. Horretarako, honako egoera hauek aurreikusi dira:

- Gertakariaren jarraipena erasoaren ondorengo asteetan
- Sustrai-kausaren analisia, sarrera-puntua zehazteko
- Elementu konprometituak identifikatzea
- Aurkitutako programa gaiztoen laginak laborategian aztertzea
- Logs garrantzitsuak berrikustea, erremediatzeko ekintzak egiteko eta gomendatzeko
- Babestutako elementu guztietan programa gaiztoak garbitzea

Arrasateko Udaleko langileen zerbitzua ikuskatzeko lanak arintzeko, gerta daitezkeen gorabeherei buruzko txosten eta informazio guztiak administrazio zentralizatuko kontsola horretan jaso eta biltegiratu beharko dira.

MDR zerbitzuko ekipoak berak iturri horien gaineko jarduera eta kontsulta proaktibo edo erreaktibo guztiak urrunetik eta administrazio zentraleko panel beraren bidez egiteko gaitasuna izan beharko du. MDR ekipoak erremediatze-ekintzak igorri ahal izango ditu, intzidenteak hala eskatzen badu, bai PC ekipoetan, bai zerbitzarian, bai zuzenean Firewall ekipoetan, IoCak

equipo

- Eliminar artefactos maliciosos
- Bloquear hashes a nivel de política

- **Remediación de incidentes:**

Una vez detenido un ataque, el servicio MDR no debe terminar su intervención en la respuesta, sino que debe ocuparse también de la remediación del incidente, para ello se contemplan los siguientes escenarios:

- Seguimiento del incidente en los días semanas posteriores al ataque
- Análisis de causa raíz para determinar el punto de entrada
- Identificación de elementos comprometidos
- Análisis en laboratorio de las muestras de programas malignos encontrados
- Revisión de logs relevantes con el fin de emitir y aconsejar acciones para la remediación
- Limpieza de los programas malignos en todos los elementos protegidos

Con el fin de agilizar las tareas de supervisión del servicio del personal del ayuntamiento de Arrasate, todos los reportes e información acerca de posibles incidentes que se puedan producir deberán quedar recogidos y almacenados en dicha consola de administración centralizada.

El propio equipo del servicio MDR deberá tener la capacidad de realizar todas las actuaciones y consultas proactivas o reactivas sobre dichas fuentes, de manera remota y a través del mismo panel de administración central. El equipo MDR podrá emitir acciones de remediación, si así lo requiere el incidente tanto sobre equipos PC como Servidor, así como directamente

blokeatuta.

IoC bat (Indicator of Compromise) sarean mehatxu edo intrusio bat egon daitekeela adierazten duen datu edo eredu bat da, eta firewall-ak jarduera susmagarria blokeatzeko, ohartarazteko edo erregistratzeko erabil dezake.

Segurtasun maila hobetzeko eta Arrasateko Udalean zerbitzua behar bezala ezartzen dela bermatzeko, zerbitzuaren proposamenean puntu hauek sartu ahal izango dira:

- Arrasateko Udaleko langileen prestakuntza, gutxienez bi saiotan, EDR/XDR soluzioak erabiltzeko eta arriskuak eta arriskuak goiz identifikatzeko.
- Biltegiratutako datuen atxikipena urtebete arte luzatzea.

Azpiegituraren segurtasun-egoera ebaluatzea, ENSaren esparruari jarraituz, eta ondoriozko txostena sortzea.

Telelanerako kanpoko ekipoak babestea

Telelanaren egungo egoera dela eta, Arrasateko Udaleko langile batzuek urrunetik konektatzen dituzte Udalaren sistemak eta aplikazioak beren ekipo pertsonalak erabiliz. Esleipendunak EPP software bat jarri beharko du Arrasateko Udalak kudeatzen ez dituen ekipo pertsonal horietan, sarera sartzen diren erabilera pertsonaleko ekipoen segurtasuna hobetzeko.

Soluzioan ez da beharrezkoa izango softwarea edo zerbitzariak instalatzea, kontsola zentral bat baitute hodeian, ekipamenduen hedapen-egoera administratzeko eta bistaratzeko.

sobre los equipos Firewall mediante el bloqueo de IoCs.

Un IoC (Indicator of Compromise) es un dato o patrón que indica la posible presencia de una amenaza o intrusión en la red, y que el firewall puede usar para bloquear, alertar o registrar actividad sospechosa.

De cara a mejorar el nivel de seguridad y garantizar la correcta implantación del servicio en el ayuntamiento de Arrasate, será posible incluir en la propuesta del servicio los siguientes puntos:

- Formación del personal del ayuntamiento de Arrasate, **en al menos dos sesiones**, en la utilización de soluciones EDR/XDR y la identificación de riesgos y peligros de manera temprana.
- Ampliación de la retención de datos almacenados hasta 1 año.

Evaluación del estado de seguridad de la infraestructura siguiendo el marco del ENS con la consiguiente generación del informe resultante.

Protección de equipos externos dedicados a Teletrabajo

Dada la situación actual de teletrabajo, cierto personal del ayuntamiento de Arrasate conecta de manera remota a los sistemas y aplicativos del ayuntamiento haciendo uso de sus equipos personales. El adjudicatario deberá proveer la instalación de un software EPP en dichos equipos personales, no gestionados por el ayuntamiento de Arrasate con el fin de mejorar la seguridad de los equipos de uso personal que acceden a la red.

La solución deberá incluir sin la necesidad de instalación de software o servidores locales con una consola central en la nube que permita administrar y visualizar el estado de despliegue en los distintos equipos.

Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

Baldintza hauek nahitaez bete beharko dira, eskainitako konponbiderako salbuespenik gabe:

- Zerbitzuak euskarri aktiboko kontratu bat izan beharko du aukeratutako fabrikatzailearekin, indarraldian zerbitzua eta eguneratzeak bermatzeko.

- Hodeian kudeaketa bakarreko kontsola. Aurreko puntuan bezala, soluzioak ez du eragile bakar bat bakarrik izan behar, kontsola bakarra ere izan behar du hodeian, eta hortik administratu ahal izango dizkizu bai MDR zerbitzua bai EPP/EDR soluzioa. Etorkizunean fabrikatzaile beraren beste zibersegurtasun soluzio batzuk kontsola berean gehitzeko aukera baloratu ahal izango da. Soluzioa kudeatzeko lokalean softwarea edo zerbitzariak instalatzea eskatzen duten soluzioak ez dira baliozkoak izango.

- Kontsolara hodeian sartzeko, autentifikazio-faktore bikoitza erabili beharko da, gutxienez hiru balidazio-sistema desberdinekin (adibidez Email, SMS eta OTP bidez QR) eta Passkeys erabilera.

- **Betetzeko tresnak: Konponbideak**, kudeaketa-kontsola berean, atal bat izan behar du, guztiz konfidentziala, kudeaketa eta egungo araudia betetzea errazteko. Horretarako, honako hauek jaso behar ditu:

    - Gorabeheren aurrean erantzuteko plan bat sortzen laguntzeko tresna
    - Gertaera bat sailkatzen laguntzeko

Los siguientes requisitos serán de obligado cumplimiento sin excepción para la solución ofertada:

- El servicio deberá disponer de un contrato de soporte activo con el fabricante elegido que garantice el servicio y las actualizaciones durante el periodo de vigencia.

- Consola de gestión única en cloud. Al igual que en el punto anterior, la solución no solo ha de constar de un agente único sino también de una consola única en la nube, desde la que podrá administrarte tanto el servicio MDR como la solución EPP/EDR. Será valorable la posibilidad de añadir en un futuro otras soluciones de ciberseguridad del mismo fabricante también en la misma consola. No serán válidas soluciones que requieran de la instalación de software o servidores en local para realizar la gestión de la solución.

- El acceso a la consola en cloud deberá ser mediante doble factor de autenticación con al menos tres sistemas de validación distintos (pej. Email, SMS y OTP vía QR) así como el uso de Passkeys.

- **Herramientas de cumplimiento**: La solución debe incorporar dentro de la misma consola de gestión un apartado, totalmente confidencial, dedicado a facilitar la gestión y el cumplimiento normativo actual, para ello debe incluir:

    - Herramienta de ayuda a la creación de un plan de respuesta ante incidentes
    - Herramienta de ayuda a la clasificación de un incidente

tresna

- ENS araudia betetzen den ebaluatzeko tresna

- Eraso-azalera murriztea. Agenteak babes-neurri hauek hartuko ditu, babestutako ekipamenduen esposizio-azalera murrizteko politika independenteen bidez konfigura daitezkeenak:

  - Periferikoen kontrola (USB, Bluetooth, MTP, Floppy...).
  - Nabigazioa kontrolatzea eta iragaztea, eta seguruak ez diren lekuetara sartzea.
    - Fitxategi arriskutsuen deskargak blokeatzea.
    - Jarduera kriminal, hacking eta antzeko kategorizatutako webguneetarako sarbidea.
  - Aplikazioen kontrola
    - Sistemen berezko tresnak (LOLBinn) eta asmo txarrez erabil daitezkeen beste batzuk (PowerShell, Rclone, Plink, etab.) ez erabiltzea ahalbidetzen duten aurrez definitutako sinadura eta aplikazio-kategoriekin.
  - DLP motorra, informazio-ihesa prebenitzeko

- Herramienta de evaluación del cumplimiento de la normativa ENS

- Reducción de superficie de ataque. El agente incluirá las siguientes medidas de protección, configurables mediante políticas independientes con el fin de reducir la superficie de exposición de los equipos protegidos:

  - Control de periféricos (USB, Bluetooth, MTP, Floppy, …).
  - Control y filtrado de la navegación y acceso a sitios no seguros.
    - Bloqueo de descargas de ficheros peligrosos
    - Acceso a sitios web categorizados como actividad criminal, hacking .. etc.
  - Control de aplicaciones
    - Con firmas y categorías de aplicaciones predefinidas que permitan evitar el uso de herramientas propias de los sistemas (LOLBinn) y otras como cuyo uso puede ser malintencionado como powershell, Rclone, Plink, etc
  - Motor DLP para prevenir fuga de información

Proposatutako irtenbidearen ekintza proaktiboak

Proposatutako sistemak PROAKTIBOA izan behar du, hau da, ekintza eta/edo gertaera susmagarriei buruzko informazioa eman behar du, konpromiso edo

Acciones Proactivas de la solución propuesta

El sistema que se proponga debe ser PROACTIVO, es decir, debe proporcionar información por sí mismo sobre acciones y/o eventos sospechosos, que pudieran

intrusio potentzial baten adierazle izan daitezkeenak eta ekipoetan edo erabiltzaileek exekutatzen dituztenak. Detekzio horiek baliagarriak izango dira administrazioko langileek ikerketa hasteko zantzuak izan ditzaten.

Zantzu horiek honela sailkatuta egon beharko dute:

- Arriskugarritasuna
- Zenbat aldiz ikusi den
- Noiztik ikusi den
- Eragindako makina
- MITRE ATT & CKren frameworkaren arabera behatutako taktika, teknika edo prozedura.
- Antzemandako balizko kasuari buruzko xehetasun laburtuak

ser indicadores de un potencial compromiso o intrusión y que sean ejecutados en los equipos o por los usuarios. Dichas detecciones servirán para que el personal de administración tenga indicios desde los cuales iniciar una investigación.

Dichos indicios deberán estar clasificados con:

- Peligrosidad
- Cuántas veces se ha visto
- Desde cuándo se ha visto
- Máquina afectada
- Táctica, Técnica o Procedimiento observado según el framework de MITRE ATT&CK
- Detalles resumidos sobre el posible caso detectado

Gainera, informazioa zabaldu ahal izango da, ikuspegi horretatik bertatik, plataforma berean ikerketak hasteko eta dokumentatzeko, eta, horrela, azterketan hurrengo urratsak errazteko, kasuak kudeatzeko sistema gisa, non posible izango den ikerketak administratzaile bati esleitzea, haren egoera eta oharrak adieraztea.

Además, será posible expandir la información para, desde esa misma vista, iniciar y documentar investigaciones dentro de la misma plataforma, facilitando así los siguientes pasos en su análisis, a modo de sistema de gestión de casos, donde sea posible asignar las investigaciones a un administrador, indicar su estado y anotaciones.

NDR sareko mehatxuak detektatzeko tresna

EPP + EDR/XDR tresnaz gain, Arrasateko Udalak Network Detection and Response (NDR) soluzio bat ere behar du, sarean ezkuta daitezkeen balizko mehatxu eta intrusioen aurrean ikusgarritasuna eta antzemateko gaitasuna emango duena.

Gaur egun Arrasateko Udalaren sarean dauden ekipo zaharrak, babestu gabeak, OT, IoT edo arriskutsuak izan daitezkeen beste elementu mota batzuk daudenez, elementu horietatik datozen edo horiei zuzendutako mehatxuak detektatzeko moduko konponbidea behar da.

Herramienta de detección de amenazas en red NDR

Adicionalmente a la herramienta EPP + EDR/XDR, el ayuntamiento de Arrasate requiere también de una solución de Network Detection and Response (NDR) que aporte visibilidad y capacidad de detección ante las posibles amenazas e intrusiones que pudieran ocultarse en la red.

La presencia de equipos antiguos, no protegidos, OT, IoT u otros tipos de elementos potencialmente peligrosos y presentes en la actualidad en la red del ayuntamiento de Arrasate, requieren de una solución capaz de detectar amenazas provenientes o dirigidas a estos elementos.

Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

Konponbide horrek ikuspen gehigarria emango die babesik gabeko gailuei, baimendu gabeko sareko baliabideei, barneko mehatxuei edo zero eguneko erasoei.
Horretarako, NDR soluzioak honako hau biltzeko proposamena egin du:

- Proposatutako EPP/XDR soluzioarekin bateragarria den soluzioa, kudeaketa-kontsolarekin eta eskainitako MDR zerbitzuarekin integratzeko gaitasuna duena, hasiera-hasieratik alertak eta detekzioak sortuz.
- Konponbideak ez du aldez aurretik entrenamendu-prozesurik beharko, ezta "prest jarri" beharrik ere, hedapena atzeratzeko edo Arrasateko Udaleko langileen esku-hartzea behar izateko.
- Arrasateko Udalaren erabiltzaileen ohiko jardunean disrupzioak saihesteko, soluzioak ez die blokeo automatikorik igorriko sareko elementuei, baizik eta MDR zerbitzuaren fabrikatzaile hornitzaileak zuzenean berrikusi eta zerrendatuko du.
- Soluzioak, gutxienez, detekzio-motor hauek izango ditu:
  - Babestu gabeko ekipoek sortutako datuak detektatzeko motorra
  - Paketeen ikuskapen sakona edo ehunka protokolorekin bateragarria den DPIa
  - Karga zifratuen analisia
  - Domeinuak sortzeko algoritmoak

Dicha solución será la encargada de aportar visibilidad adicional sobre dispositivos desprotegidos, recursos presentes en la red no autorizados, amenazas internas o ataques de día cero.
Para ello la solución NDR propuesta de reunir lo siguiente:

- Solución compatible con la solución EPP/XDR propuesta, con capacidad de integrarse tanto con la consola de gestión como con el servicio de MDR ofertado, generando alertas y detecciones desde el primer momento.
- La solución no requerirá de un proceso de entrenamiento previo ni “puestas a punto” que retrasen el despliegue o requieran de intervención por parte del personal del ayuntamiento de Arrasate.
- De cara a evitar disrupciones en la operativa habitual de los usuarios del ayuntamiento de Arrasate la solución no emitirá bloqueos automáticos a los elementos de la red si no que será revisada y correlada directamente por el fabricante proveedor del servicio MDR.
- La solución contará al menos con los siguientes motores de detección:
  - Motor de detección de datos generados por equipos no protegidos
  - Inspección profunda de paquetes o DPI compatible con varios cientos de protocolos
  - Análisis de cargas cifradas
  - Detección de algoritmos de generación

detektatzea

- Saioetan arriskua detektatzea

- Soluzioa hedatzeko ez da beharrezkoa izango makinetan agente gehigarririk jartzea.

Gailu mugikorrak babesteko tresna (tabletak eta mugikorrak)

Arrasateko Udalak UEM irtenbide bat behar du, hau da, mota guztietako gailuen kudeaketa globala ahalbidetzen duen kudeaketa-sistema bateratu bat, horien guztien administrazioa zentralizatuz. Nabarmendu behar da ezinbestekoa dela arauak betetzeko arauak sortzea, horrela, gailuek antolakundeak eskatutako gutxieneko segurtasuna betetzen dutela ziurtatu ahal izateko.

Beraz, honako hauek egiteko aukera emango duen tresna bat bilatzen da:

- MDM: Profilen kudeaketa gailuetan
- MAM: Gailuetako aplikazioen kudeaketa
- MCM: Dokumentuen kudeaketa gailuetan
- MTD: Segurtasunaren kudeaketa

UEM konponbiderako nahitaez bete beharreko baldintzak hauek dira:

- **MDM**
  - Compliance arauak: gailuak eskatzen diren gutxieneko baldintzak betetzen dituen egiaztatu ahal izatea, eta horretan oinarrituta ekintzak egin ahal izatea, horrela, postara sartzea ukatu, edukiontzia blokeatu edo atazaren bat bidali ahal izateko.
  - Segurtasun-arauak, hala nola pasahitzak, gailuen funtzioen erabilera (murrizketak), aplikazioen babesa

de dominios

- Detección de riesgo en sesiones

- El despliegue de la solución no requerirá de la instalación de agentes adicionales en las máquinas.

Herramienta de protección de dispositivos móviles (Tablets y móviles)

El ayuntamiento de Arrasate requiere de una solución UEM, es decir, un sistema de gestión unificado que permite la gestión global de todo tipo de dispositivos, centralizando la administración de todos ellos. Cabe destacar que es imprescindible el poder crear reglas de cumplimiento, para de este modo, poder certificar que los dispositivos cumplen con un mínimo de seguridad exigida por la organización.

Por tanto, se busca una herramienta que permita realizar:

- MDM: Gestión de perfiles en dispositivos
- MAM: Gestión de aplicaciones en dispositivos
- MCM: Gestión de documentos en dispositivos
- MTD: Gestión de la seguridad

Los requisitos de obligado cumplimiento para la solución UEM son:

- **MDM**
  - Reglas de compliance: poder verificar si el dispositivo cumple con los requisitos mínimos exigidos, así como poder realizar acciones en base a ello, para de este modo, poder denegar acceso al correo, bloquear contenedor o enviar algún tipo de tarea
  - Reglas de seguridad, como passwords, uso de funciones de los dispositivos (restricciones), protección de

(irekitzea saihestu), VPNen konfigurazioa, APNak eta ziurtagirien hedapena
- Konfigurazio-arauak. Emailaren parametroak, aplikazioen baimenak, haririk gabeko sareak, erabiltzaile-kontuak eta abar bidal daitezke.
- Ataza-paketeak sortzea, bete ezean automatikoki erremediatzeko.

aplicaciones (evitar su apertura), configuración de VPNs, APNs así como el despliegue de certificados
- Reglas de configuración, pudiendo enviar los parámetros de email, permisos de aplicaciones, redes inalámbricas, cuentas de usuario, etc.…
- Generación de paquetes de tareas para remediación automática en caso de no cumplimento.

- **MAM**
  - Gailuetako aplikazioak kudeatzea; aplikazioak instalatu eta desinstalatu ahal izango dira.
  - Aplikazioen denda propioa, denda publikoetan argitaratu gabeko app propioak eduki ahal izateko

- **MAM**
  - Gestionar las aplicaciones en dispositivos, pudiendo instalar y desinstalar éstas
  - Tienda propia de aplicaciones, de tal modo que sea posible tener las apps propias no publicadas en tiendas públicas

- **MCM**
  - Hainbat baimen-maila dituzten dokumentuak kudeatzea, eta horiek kontsola zentraletik guztietara zabaldu ahal izatea.
  - Biltegiratze segurua, pantaila-harrapaketen, datu-iragazketen, konplimenduaren araberako sarbide-kontrolaren, ordutegiaren eta abarren aurrean babestua.

- **MCM**
  - Gestión de documentos con diversos niveles de permisos, pudiendo éstos ser desplegados desde la consola central a todos ellos.
  - Almacenamiento seguro, protegido frente a capturas de pantalla, exfiltración de datos, control de acceso según compliance, horario, etc.…

- **MTD**
  - Programa maltzurren potentziala detektatzea, bai instalatutako aplikazioena, bai berriena, bai sistemarena.
  - SMS bidezko phishingaren aurkako babesa
  - MitM motako sare-erasoen aurkako babesa
  - Nabigazioa babestea eta kontrolatzea, gune arriskutsuetara eta kategorietara sartzea saihestuz.
  - Zerrenda zuriak eta zerrenda beltzak

- **MTD**
  - Detección de potencial de programas malignos, tanto de aplicaciones ya instaladas como nuevas, así como de sistema.
  - Protección contra phishing vía SMS
  - Protección contra ataques de red tipo MitM
  - Protección y control de la navegación, evitando el acceso a sitios peligrosos, así como categorías.
  - Listas blancas y listas negras

4.2 - 2 SORTA: Zibersegurtasunaren arloan udal-langileak prestatzeko eta kontzientziatzeko lanerako informatika-soluzioak hornitzea eta kudeatzea, eta plegu hauetan zehaztutakoaren arabera langileei zenbait prestakuntza-saio ematea.

ENS kontzientziazio- eta sentsibilizazio-programa:

Ziberdelitugileek gaur egun erabiltzen dituzten estrategiak edozein segurtasun-hesi gainditzea ahalbidetzen duten zenbait giza ezaugarri eta portaera aprobetxatzera bideratuta daudenez, beharrezkoa da Arrasateko Udalak pertsonengan ere fokatutako segurtasun-neurriak hartzea.

Horretarako, esleipendunak informazioaren segurtasunari eta zibersegurtasunari buruzko prestakuntza- eta kontzientziazio-plan bat eskaini beharko du, Arrasateko Udaleko langile guztientzat. Kontzientziazio-plan horrek honako hauek jaso beharko ditu gutxienez:

- Intzidentzien jakinarazpen mekanismoa
- Hileroko sentsibilizazio-ekintzak
- Informazioaren segurtasun-aholkuak eta datuen babesa betetzea
- Aurrez aurreko eta/edo urruneko hitzaldiak, bai zuzendaritza kideei zein langileei.
- Langileentzako laguntza eta euskarria
- Plana baloratzeko mekanismoren bat, hala nola azterketak, probak, etab.

4.2. LOTE 2: Suministro y gestión de las soluciones informáticas para el trabajo de formación y concienciación del personal municipal en materia de ciberseguridad, así como la impartición de varias sesiones de formación a los trabajadores según las especificaciones de estos pliegos.

Programa de concienciación y sensibilización ENS:

Dado que las estrategias actuales que emplean los ciberdelincuentes van encaminadas al aprovechamiento de ciertas características y comportamientos humanos que permiten saltar cualquier barrera de seguridad que se implemente, es necesario que El Ayuntamiento de Arrasate adopte medidas de seguridad enfocadas también en las personas.

Para ello, el adjudicatario deberá proporcionar un plan de formación y concienciación en Seguridad de la Información y Ciberseguridad, para todos los empleados del ayuntamiento de Arrasate. Este plan de concienciación deberá contemplar al menos:

- Mecanismo de notificación de incidentes
- Acciones mensuales de sensibilización
- Consejos de seguridad de la información y cumplimiento de protección de datos
- Charlas presenciales y/o remotas, tanto a alta dirección como a usuarios
- Asistencia y soporte a los empleados
- Algún mecanismo de valoración del plan tipo exámenes, pruebas, etc.

Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

Planak ahalik eta intrusiboena izan beharko du Arrasateko Udaleko langileen eguneroko jardueran, baina gutxienez hilean behin ekintza bat egin beharko du, hedapen-bide egokiena proposatuz (aurrez aurrekoa edo elektronikoa, intranet korporatiboan argitaratzea, etab.).

El plan deberá ser lo menos intrusivo posible en la actividad diaria de los empleados del ayuntamiento de Arrasate, pero deberá llevar al menos una acción mensual, proponiendo el medio de difusión más adecuado (presencial o electrónico a través de correo electrónico, publicación en la intranet corporativa, etc.)

- Zibersegurtasunari eta pribatutasunari buruzko kontzientziazioari buruzko hasierako hitzaldia (goi-zuzendaritza eta goi-kargudunak), ordubetekoa.

- Charla inicial de concienciación en Ciberseguridad y Privacidad (Alta Dirección y Altos Cargos) de 1 hora.

Esleipendunak konpromisoa hartuko du sentsibilizazio-hitzaldi presentzial bat emateko goi-zuzendaritzari, honako eduki hauekin:

- Zibersegurtasunaren egungo testuingurua
- Erregulazioa (IKT zuzenbidea: DBEO, LSSICE, NIS araudia, etab.)
- Segurtasun perimetrala (Zero Trust kontzepturako bilakaera)
- Segurtasunaren kudeaketa (ENS)
- Zibersegurtasun eta Pribatutasun (Erabiltzaileak) arloan kontzientziatzeko urteko hitzaldia, ordubetekoa.

El adjudicatario se comprometerá a impartir una charla presencial de sensibilización dirigida a la alta dirección cuyo contenido sea:

- Contexto actual de la Ciberseguridad
- Regulación (Derecho TIC: RGPD, LSSICE, Normativa NIS, etc.)
- Seguridad perimetral (evolución hacia el concepto Zero Trust)
- Gestión de la Seguridad (ENS)
- Charla anual de concienciación en Ciberseguridad y Privacidad (Usuarios) de 1 hora.

Esleipendunak konpromisoa hartuko du Arrasateko Udalaren erabiltzaileei sentsibilizazioari buruzko hitzaldi presentzial edo online bat emateko, honako eduki hauekin:

- Teknologia berriak erabiltzeko jardunbide egokiak.
- PCak, eramangarriak eta mugikorrak arduraz erabiltzea
- Gailu erauzgarrien politika
- Pasahitzak kudeatzeko politika

El adjudicatario se comprometerá a impartir una charla presencial u online de sensibilización dirigida a los usuarios del ayuntamiento de Arrasate que se considere, cuyo contenido sea:

- Buenas prácticas en el uso de las nuevas tecnologías
- Uso responsable de PC's, portátiles y móviles
- Política de dispositivos extraíbles
- Política de gestión de contraseñas
- Política de uso responsable de internet

- Internet arduraz erabiltzeko politika

- Posta elektronikoa arduraz erabiltzeko politika
- Mahaigaineko eta pantailako politika garbiak
- Egile-eskubideei lotutako materiala deskargatzeko politika
- Sarbideak kontrolatzeko eta erregistratzeko politika
- Datuak Babesteko 2016/679 Erregelamendu Orokorra (DBEO)
- Erantzun azkarra segurtasun-intzidenteen aurrean
- Erabiltzailearen erantzukizuna
- Phishing eta ingeniaritza sozialeko simulakroak eta prestakuntza-ariketak (urtean bat).

- Política de uso responsable del correo electrónico
- Política de escritorio y pantalla limpios
- Política de descarga de material sujeto a derechos de autor
- Política de control y registro de accesos
- Reglamento 2016/679 General de Protección de Datos (RGPD)
- Respuesta rápida ante incidentes de seguridad
- Responsabilidad del Usuario
- Simulacros y ejercicios formativos de phishing e ingeniería social (uno al año).

Esleipendunak phishing eta gizarte-ingeniaritzako simulakroak eta ariketak egiteko konpromisoa hartuko du, horien ondoren erabiltzaileei beharrezko prestakuntza-ekintzak bideratu ahal izateko.

El adjudicatario se comprometerá a realizar simulacros y ejercicios de phishing e ingeniería social de tal modo que tras ellos se pueda dirigir las acciones formativas necesarias a los usuarios.

- Urtean 6 ariketa Arrasateko Udaleko Eraldaketa Digitaleko langileei zuzendutako ikastaroetarako, segurtasunaren eta datuen babesaren arloko hainbat arlotan, gutxienez 20 ordukoak.

- 6 ejercicios al año para cursos dirigidos al personal de Transformación Digital del ayuntamiento de Arrasate, en diferentes materias de seguridad y protección de datos de al menos 20 horas de duración.

Software-plataforma bat behar da, pertsonei lotutako zibersegurtasun-arriskua ebaluatzeko eta zibersegurtasunaren eta arrisku handieneko mehatxuen hainbat arlotan kontzientziatzeko: ingeniaritza soziala, phishing, kontuen eta kredentzialen erabilera, etab.

Se requiere una plataforma software que permita evaluar el riesgo de ciberseguridad asociado a las personas y concienciar en diferentes áreas de la ciberseguridad y de las amenazas de mayor riesgo: ingeniería social, phishing, manejo de cuentas y credenciales, etc.

Prestakuntza horren osagarri praktiko gisa, gizarte-ingeniaritzako simulakroak egingo dira, ikasleei

Como complemento práctico a esta formación, se llevarán a cabo simulacros de ingeniería social, para

intzidenteen analisi eta detekzio goiztiarrean laguntzeko.

Simulazio horien emaitzei esker, ikasleen kontzientziazio- eta trebakuntza-maila erakutsi ahal izango da, era horretako zibererasoei behar bezala erantzuteko. Horri esker, zehatz-mehatz azaldu ahal izango dira iruzurrezko komunikazio horiek goiz detektatu izanaren zantzuak, eskola-saio gehigarrietan eta horien ostekoetan, gomendioak eta jardunbide egokiak izan daitezen.

Plataformak zibersegurtasuneko kontzientziazio- eta prestakuntza-edukiak sortzeko gai izan behar du, gutxienez euskaraz eta gaztelaniaz.

Plataforma honen helburu nagusia pertsonei lotutako segurtasun-arriskua ebaluatzea denez, aukera eman behar du alerta-egoeraren berri emango duten metrika-panelak eta adierazleak sortzeko, kolektiboen arabera sailkatutako informazioa emateko adina granularitatez. Adierazle-panel horiek aldian-aldian eguneratu behar dira, eta denboran izan duten bilakaera erakutsi. Ebaluazio horri esker, zibersegurtasunaren kontzientziaziorako ekintza-planak diseinatu ahal izango dira, une bakoitzeko alerta-mailen arabera.

Aipatutako granularitatea beharrezkoa da kontzientziazio-ibilbide pertsonalizatuak garatzeko ere, ekintza horien eraginkortasuna handitzeko, zibersegurtasuneko alerta-egoera handitzeko eta pertsona bakoitzari emaitzen eta bilakaeraren berri emateko.

Prestakuntza- eta kontzientziazio-gaitasunez gain, simulazio- eta entrenamendu-kanpainak ere egin behar dira, Arrasateko Udaleko pertsonek zibersegurtasun-mehatxu nagusien aurrean, pertsona bakoitzaren profilera (kolektiboa eta alerta-maila) egokitu ahal izateko. Horretarako, arrisku handieneko kolektiboei zuzendutako erasoak egitean lotutako alderdi psikologikoak txertatzeko tresnak eta algoritmoak txertatu behar ditu.

ayudar a los alumnos en el análisis y detección temprana de incidentes.

Los resultados de dichos simulacros permitirán demostrar el nivel de concienciación y capacitación de los alumnos, para reaccionar de forma adecuada a este tipo de ciberataques. Lo que permitirá explicar en detalle los indicios de detección temprana de dichas comunicaciones fraudulentas, durante las sesiones lectivas adicionales y posteriores a los mismos, que sirvan de recomendaciones y buenas prácticas.

La plataforma deber ser capaz de crear contenidos de concienciación y formación en ciberseguridad al menos en euskera y castellano.

Puesto que el objetivo fundamental de esta plataforma es la evaluación del riesgo de seguridad asociado a las personas, debe permitir la generación de paneles de métricas e indicadores que informen del estado de alerta con suficiente granularidad como para proporcionar información clasificada por colectivos. Estos paneles de indicadores deben actualizarse periódicamente y mostrar su evolución en el tiempo. Esta evaluación permitirá diseñar planes de acción en concienciación de ciberseguridad acordes a los niveles de alerta en cada momento.

La granularidad mencionada es necesaria también para el desarrollo de itinerarios de concienciación personalizados, con el objetivo de aumentar la eficacia de estas acciones, aumentar el estado de alerta en ciberseguridad e informar a cada persona de sus resultados y evolución.

Además de las capacidades de formación/concienciación, debe incluir la realización de campañas de simulación y entrenamiento ante las principales amenazas de ciberseguridad para las personas del ayuntamiento de Arrasate, de manera que pueda adaptarse al perfil de cada una (colectivo y nivel de alerta). Para ello debe incorporar herramientas y algoritmos que permitan incorporar los aspectos psicológicos asociados en la realización de ataques dirigidos a los colectivos de mayor riesgo.

Tresnaren beste funtsezko alderdi bat eraginkortasuna izan behar da, hau da, errendimendua maximizatu behar du, pertsona bakoitzak zibersegurtasunaren inguruko kontzientziazioan ematen duen denboraren arabera.

Otro aspecto fundamental de la herramienta debe ser su eficiencia, es decir debe maximizar el rendimiento al tiempo dedicado por cada persona a la concienciación en ciberseguridad.

Hornitzaileak pertsonei lotutako zibersegurtasuneko prestakuntza-plataformaren erabilera eskaini behar du. Plataforma horrek irakatsitako gaiari lotutako ezagutzen ebaluazioak egiteko aukera eman beharko du. Testuinguru horretan, esleipendunak kudeatu beharko du plataforma.

El proveedor debe ofrecer el uso de la plataforma de formación en ciberseguridad asociado a las personas. Esta Plataforma deberá permitir la realización de evaluaciones de conocimientos asociados a la materia impartida. En este contexto, la plataforma deberá ser gestionada por el adjudicatario.

Hornitzaileak langileen aurrerapenei buruzko hiru hilean behingo txosten bat eman beharko du, udalak erabakitako Prestakuntza Planaren jarraipena bermatuz.

El proveedor deberá facilitar un informe trimestral con el progreso de los empleados, garantizando un seguimiento del Plan de Formación estipulado por el ayuntamiento.

4.3. - 3 SORTA: ENS izeneko ziurtagiri teknologikoa eskuratu ahal izateko ezarri beharreko jarraibideak zerrendatuko dituen aholkularitza lan bat kontratatzea.

4.3. LOTE 3: contratación de un trabajo de consultoría que enumere las pautas a seguir para la obtención del certificado ENS

Adjudikaziodunak Segurtasun Eskema Nazionala aplikagarri zaien Arrasateko Udalaren informazio-sistemak zehaztuko ditu, hau da, eskubideak baliatzearekin, betebeharrak bitarteko elektronikoen bidez betetzearekin eta/edo erabiltzaileek bitarteko elektronikoen bidez informazioa eta administrazio-prozedura eskuratzearekin zerikusia duten sistemak. Alde horretatik, sistema elektronikoetan tratatutako informazioa babestuta egongo da, Datu Pertsonalak Babesteko araudian ezarritako irizpideak kontuan hartuta.

El adjudicatario determinará los sistemas de información del ayuntamiento de Arrasate a los que les sea de aplicación el Esquema Nacional de Seguridad, es decir, aquellos sistemas que estén relacionados con el ejercicio de derechos, con el cumplimiento de deberes por medios electrónicos y/o con el acceso por medios electrónicos de los usuarios a la información y al procedimiento administrativo. En este sentido, la información tratada en los sistemas electrónicos estará protegida teniendo en cuenta los criterios establecidos en la normativa de Protección de Datos de Carácter Personal.

Esleipendunak betetze-mailaren analisia egin beharko du ENSari dagokionez. Horretarako, udalak Segurtasun Eskema Nazionalari dagokionez duen betetze-maila ebaluatu beharko da. Era berean, erakundeak ezarri beharreko neurriak biltzen dituen txostena egin beharko da, lege-dekretuarekiko desbideratzeak identifikatuz.

El adjudicatario deberá realizar un análisis de cumplimiento con respecto al ENS. Para ello se requerirá la evaluación del grado de cumplimiento del ayuntamiento con respecto al Esquema Nacional de Seguridad. A su vez, se requerirá la realización de informe con las medidas necesarias a implementar por la organización identificando las desviaciones con respecto al decreto ley.

Alde horretatik, informazioaren eta zerbitzuen segurtasunean eragin negatiboa izateak dituen ondorioen balorazioa egiteko, kontuan hartuko da zer ondorio dituen organizazioak bere helburuak lortzeko duen gaitasunean, aktiboen babesean, zerbitzu-betebeharrak betetzean, legezkotasunaren errespetuan eta erabiltzaileen eskubideetan.

Informazio-sistemen kategorizazio hori bi fasetan egiten da:

1 Eskatutako maila zehaztuko da (BAXUA, ERTAINA edo ALTUA), informazio eta zerbitzu bakoitzerako segurtasun-dimentsio batean. Hau da, informazioaren edo zerbitzuen segurtasunari eragingo liokeen intzidente batek izango lukeen inpaktuaren balorazioaren arabera, haren eskuragarritasunari, benetakotasunari, osotasunari, konfidentzialtasunari eta trazabilitateari kalte eginez.

2 Sistemaren OINARRIZKOA, ERTAINA eta ALTUA kategoria zehaztuko da, honako baldintza hauen arabera:

3 Informazio-sistema bat HANDIA kategoriakoa izango da segurtasun-dimentsioetako bat ALTUA bada.

4 Informazio-sistema bat ERTAINA kategoriakoa izango da, baldin eta haren segurtasun-dimentsioetako bat maila ERTAINERA iristen bada eta bat ere ez bada goragoko mailara iristen.

Informazio-sistema bat OINARRIZKO kategoriakoa izango da segurtasun-dimentsioetako bat BEHEKO mailara iristen bada, eta bat ere ez bada goragoko mailara iristen.

En este sentido, se tendrá en cuenta la valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los usuarios.

Esta categorización de los sistemas de información se realiza en dos fases:

1 Se determinará el nivel requerido (BAJO, MEDIO o ALTO) en una dimensión de seguridad para cada información y servicio. Es decir, en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para su disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

2 Se determinará la categoría BÁSICA, MEDIA y ALTA del sistema, en base a las siguientes condiciones:

3 Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

4 Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Segurtasun Politika eta Prozedurak
Adjudikaziodunak segurtasun-politika bat ezartzen lagunduko du, Segurtasun Eskema Nazionalak eskatzen dituen oinarrizko printzipioetan eta gutxieneko

Política de Seguridad y Procedimientos
El adjudicatario ayudará a establecer una política de seguridad en base a los principios básicos y requisitos mínimos exigidos por el Esquema Nacional de

baldintzetan oinarrituta. Esleipendunak orientabidea emango dio Arrasateko Udalari, plana ezarri, bete eta onartzeko egin beharreko urratsei dagokienez.
Zehazki, eta gutxienez, segurtasun-politikak prozedura hauek deskribatu eta jasoko ditu:

Segurtasun-prozesua antolatzea eta ezartzea
Segurtasunak erakundeko kide guztiak konprometitu beharko ditu. Segurtasun-politika betetzeaz eta administrazio-erakundeko kide guztiek ezagutzeaz arduratuko diren arduradun argi batzuk identifikatuko ditu segurtasun-politikak.

Arriskuen analisia eta kudeaketa
Sistemaren eraginpean dauden arriskuen analisiaren eta tratamenduaren bidez egingo da kudeaketa. Arriskuak arintzeko edo ezabatzeko hartutako neurriak justifikatu egingo dira, eta, nolanahi ere, proportzionaltasuna egongo da neurrien eta arriskuen artean.

Langileen kudeaketa
Prozesu osoan zehar, informazioarekin eta sistemekin lotutako langileei prestakuntza eta kontzientziazio espezifikoa emango zaie, segurtasunaren arloan dituzten betebeharrei eta betebeharrei dagokienez. Haien jarduerak gainbegiratu egingo dira, ezarritako prozedurak betetzen direla egiaztatzeko. Horrela, sistemen segurtasuna beren bizi-zikloaren fase guztietan (instalazioa, mantentze-lanak, gorabeheren kudeaketa eta eraispena) trebatutako, dedikatutako eta ikasitako langileek zaindu, berrikusi eta ikuskatuko dute.

Profesionaltasuna
Arrasateko Udalak, Segurtasun Eskema Nazionalean oinarrituta, prozedurak ezarri behar ditu segurtasun-zerbitzuak ematen dizkieten erakundeek kudeaketa-maila eta heldutasun-maila egokiak izan ditzaten exijitzeko, modu objektiboan eta diskriminaziorik gabe. Segurtasun Eskema Nazionalean ziurtatuta egon beharko dute, eta beste ziurtagiri batzuk ere eduki ahal izango dira, hala nola ISO27001 edo ISO22301.

Seguridad. El adjudicatario orientará al Ayuntamiento de Arrasate en relación con los pasos a seguir para su implantación, cumplimiento y aprobación.
En concreto y como mínimo, la política de seguridad describirá y contendrá los siguientes procedimientos:

Organización e implantación del proceso de seguridad
La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad identificará unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

Análisis y gestión de los riesgos
Se realizará la gestión por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Las medidas adoptadas para mitigar o suprimir los riesgos se justificarán y, en todo caso, existirá proporcionalidad entre ellas y los riesgos.

Gestión de personal
A lo largo de todo el proceso se formará y concienciará de forma específica al personal relacionado con la información y los sistemas en relación con sus deberes y obligaciones en materia de seguridad. Sus actuaciones serán supervisadas para verificar que se siguen los procedimientos establecidos. De esta forma, la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Profesionalidad
El ayuntamiento de Arrasate, en base al Esquema Nacional de Seguridad, debe establecer procedimientos para exigir, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados. Debiendo estar certificados en Esquema Nacional de Seguridad y siendo valorable disponer de otras certificaciones, como la ISO27001 o la ISO22301.

5. SISTEMAKO BALDINTZAK

Sistemak honako baldintza hauek bete behar ditu:

Berariaz zehaztu behar da sistema oinarritzen den hodeian, zerbitzari lokaletan ala bezeroak zehaztu dezakeen. Proposatzen den sistemak kontratu honen barruan ezartzeak dakartzan gastu guztiak hartuko ditu barne, eta ezin izango du udalak proposatutako konponbidea abian jartzeko gastu gehigarririk izan.

a) Kontratuaren xedean sartuko dira hornitzailearen erantzukizuna izango diren zerbitzuak (zerbitzari lokalean edo hodeian): inplementazioa eta prestakuntza; soluzioaren modulu integratu guztien euskarri teknikoa; erabilera-orientazioa; eta IT (informazioaren teknologia) errendimendu teknikoaren gainbegiratzea.

b) Zerbitzua ITko euskarri-talde batek eta zibersegurtasun sektorean esperientzia egiaztatua duen talde batek ziurtatu behar du. Teknikarien kalifikazioen deskribapen zehatza emango da.

c) SOC zentruaren informazio-sistemak datu-zentro propio batean edo/eta Datuak Babesteko Erregelamendu Orokorraren betetze-ziurtagirian egon behar du.

d) Jabetza eta konfidentzialtasuna - Sortutako datuen eta emaitzen jabetza erakunde kontratatzailearena dela aitortu behar du hornitzaileak. Hornitzaileak erakunde kontratatzailearen informazio guztia eta jasotako datu guztiak konfidentzialak direla bermatu behar du.

5. REQUISITOS DEL SISTEMA

El sistema debe cumplir los siguientes requisitos:

Se debe especificar explícitamente si el sistema se basa en la nube, en servidores locales o puede ser determinado por el cliente. El sistema que se proponga incluirá todos aquellos gastos derivados de su implantación dentro de este contrato, no pudiendo derivar en gastos adicionales al ayuntamiento para la puesta en marcha de la solución propuesta.

a) Se incluirán en el objeto del contrato los servicios responsabilidad del Proveedor (ya sea en los servidores locales o en la nube): implementación y formación; soporte técnico de todos los módulos integrados de la solución; orientación de uso; y supervisión del rendimiento técnico de TI (tecnología de la información).

b) El servicio debe ser asegurado por un equipo de soporte de TI y de servicios de ciberseguridad con experiencia comprobada en el sector. Se proporcionará una descripción detallada de las calificaciones del cuerpo técnico.

c) El sistema de información del SOC debe estar alojado en un centro de datos propio y / o certificado de cumplimiento con el Reglamento General de Protección de Datos.

d) Propiedad y confidencialidad - El proveedor debe reconocer la propiedad de los datos y resultados generados como de la entidad contratante. El proveedor debe garantizar la confidencialidad de toda la información de la entidad contratante como de todos los datos

recibidos.

e) Eguneratzeak eta mantentze-lanak: - Eguneratzeak (upgrade) eta sisteman ezarritako funtzionalitateen mantentzeak Arrasateko Udaleko Zerbitzu Teknikoek erabiltzeko prest egon behar dute

e) Actualizaciones y mantenimiento: - las actualizaciones (upgrades) y el mantenimiento de las funcionalidades implementadas en el sistema deben estar disponibles para uso de los Servicios Técnicos de Arrasateko Udala.

f) Hornitzaileak, ahal den neurrian, gutxienez astebete lehenago zehaztu behar ditu softwarea mantentzeko eta eguneratzeko beharrezkoak diren zerbitzu-etenak.

f) El proveedor debe especificar, en la medida de lo posible, las interrupciones de servicio necesarias para efectuar mantenimiento y actualización del software con al menos 1 semana de antelación.

5. SORTA GUZTIETAKO ZERBITZUAK ABIAN JARTZEA, ETA HORIEN JARRAIPENA ETA KONTROLA EGITEA

Enpresa esleipenduna ondorengoaz arduratuko da:

Hasieran, esleitua izan zaion sorta bakoitzaren ustiapen zehatzaren baldintzatzaile espezifikoak eta proiektuan parte hartzen duen ingurune teknologikoaren Datu-Ereduak aztertzeko fase bat egingo du.

Horretarako, Laneko Plangintza bat proposatu beharko du eta eskakizunen Datuak hartzea jasoko du; plangintza hori Arrasateko Udaleko Proiektu-Arduradunak onartu beharko du.

Proiektuko Datu-iturriak honako hauek dira:

- Gaur egungo sare egitura (firewallak, switchak, zerbitzariak, ordenagailuak,…)
- Gaur egungo sistema informatikoetan instalatutako programak (sistema eragileak, antibirusak, segurtasun kopia sistemak, birtualizazio sistemak,…)
- Udaletxeko informatikarien lantaldearekin batera osatuko du sortan adierazi duen

5. PUESTA EN MARCHA, SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DE LOS SERVICIOS EN TODOS LOS LOTES

La empresa adjudicataria se encargará:

Inicialmente realizará una fase de análisis de los condicionantes específicos de la explotación concreta de cada lote que se le ha adjudicado, así como de los Modelos de Datos del entorno tecnológico participante en el proyecto.

Para ello deberá plantear un Plan de Trabajo en el que se incluya la toma de Datos de requerimientos que deberá ser aprobado por el responsable del Proyecto de Arrasateko Udala.

Las fuentes de Datos del Proyecto son:

- Arquitectura de red actual (firewalls, switches, servidores, ordenadores, …)
- Programas actuales instalados en los sistemas informáticos (sistemas operativos, antivirus, sistemas de backup, sistemas de virtualización…)
- Completará junto al equipo de informáticos municipal la información y documentación necesaria para la puesta en marcha de la

irtenbidea abian jartzeko behar duen informazio eta dokumentazio guztia.

Esleipendunak komunikazio teknikoak izan beharko ditu Arrasateko Udalean ezarritako soluzioen hornitzaileekin eta Sistema Adituaren proiektu honetan parte hartzen dutenekin (Antivirus Adaptative Defense 360, Sarenet bidezko posta elektronikoko Relay sistema, VMWare birtualizazio-sistema, Veeam Backup segurtasun-kopien sistemak, FortiNet firewall-ak, Cisco switcheak...), soluzioa ezartzeko beharrezko ezaugarri teknikoak ezagutzeko. Horretarako, plan bat planteatu beharko du, eta Arrasateko Udala proiektuaren arduradunak onartu beharko du. Aurkeztutako proposamen ekonomikoaren guztizko zenbatekoan sartuko da jakinarazpen horien kostua.

Kontratua behar bezala zuzendu eta kontrolatzeko, honako egitura eta funtzionamendu-modu hauek ezarri dira sorta guztietarako:

5.1. Arrasateko Udalaren zuzendaritza.

Lote guztietarako, Arrasateko Udalak kontratuaren arduradun bat izendatuko du, kontratuaren gauzatzea gainbegiratzeko. Kontratazio-organoak agintzen dizkion eginkizun guztiak izango ditu. Horien artean, adierazpen gisa, baina ez modu mugatzailean, honako hauek daude:

- Solaskide gisa jardutea enpresa esleipendunak izendatutako zerbitzuen arduradunarekin.
- Kontratua gauzatzeko erabakiak gainbegiratzea eta hartzea, kontratazio-organoak emandako ahalmenen barruan.
- Zerbitzu-mailako akordioak ez betetzeagatik zigorrak aplikatzeko proposamena egitea.
- Kontratua behar bezala betetzen dela zaintzea eta enpresa esleipendunak egindako lanen

solución propuesta en el lote adjudicado.

El adjudicatario deberá mantener comunicaciones técnicas con los diferentes proveedores de las soluciones implantadas en Arrasateko Udala y participantes en este proyecto de Sistema Experto (Antivirus Adaptative Defense 360, sistema de Relay de correo electrónico con Sarenet, sistema de virtualización VMWare, sistemas de copias de seguridad Veeam Backup, firewalls FortiNet, switches Cisco,…...) para conocer las características técnicas necesarias para la implantación de la solución. Para ello deberá plantear un Plan al respecto que deberá aprobar el responsable del Proyecto de Arrasateko Udala estando incluido el coste de las citadas comunicaciones en el importe total de la propuesta económica presentada.

Para la adecuada dirección y control de la ejecución del contrato, se establece la siguiente estructura y modo de funcionamiento para todos los lotes:

5.1. Dirección por parte del Ayuntamiento de Arrasate.

Para todos los lotes, el ayuntamiento de Arrasate designará un responsable del contrato que supervisará la ejecución de éste. Sus funciones serán todas aquellas que le sean encomendadas por el Órgano de Contratación. Entre ellas, a modo enunciativo, pero no limitativo, se encuentran:

- Actuar como interlocutor con el responsable de los servicios designado por la empresa adjudicataria.
- Supervisar y adoptar decisiones respecto a la ejecución del contrato dentro de las facultades otorgadas por el órgano de contratación.
- Realizar la propuesta de aplicación de penalidades por incumplimiento de los Acuerdos de Nivel de Servicio (ANS).
- Velar por el adecuado cumplimiento del

kalitatea egiaztatzea.

- Arrasateko Udalak kontratuan zehaztutako lanak eta entregagaiak onartzea.
- Kontratazio-organoak agintzen dizkion guztiak.

5.2. Enpresa esleipendunaren zuzendaritza.

Bestalde, enpresa esleipendunak arduradun bat izendatuko du. Arduradun horrek funtzio hori behar bezala garatzeko aukera emango dion eginkizun bat izan beharko du enpresan.

Bere funtzioen artean, adierazpen gisa, baina ez mugatzaile gisa, honako hauek daude:

- Solaskide gisa jardutea Arrasateko Udaleko Kontratuaren arduradunarekin, kontratuarekin lotutako alderdi estrategiko eta taktikoei dagokienez, bai merkataritzakoak (betetzea, Arrasateko Udalaren beharrak, merkataritza alderdiak, etab.), bai teknikoak (plangintza, zerbitzuen kalitatea, behar operatiboak, etab.).
- Kontratuaren prestazioa behar bezala gauzatzen dela ziurtatzea.

Enpresari jarraibideak ematea, Arrasateko Udaleko Kontratuaren arduradunak hartutako erabakietan oinarrituta.

- Zerbitzu Mailako Akordioak betetzen direla egiaztatzea.
- Arrasateko Udalari kontratua gauzatzean gertatzen den edozein gorabeheraren berri

contrato y verificar la calidad de los trabajos realizados por la empresa adjudicataria.

- Aprobar por parte del ayuntamiento de Arrasate los trabajos y entregables definidos en el contrato.
- Todas aquellas que le sean encomendadas por el Órgano de Contratación.

5.2. Dirección por parte de la Empresa Adjudicataria.

Por su parte, la empresa adjudicataria designará a un responsable, que deberá tener una función en la empresa que le permita desarrollar adecuadamente esta función.

Entre sus funciones, a modo enunciativo, pero no limitativo, se encuentran:

- Actuar como interlocutor con el responsable del Contrato del ayuntamiento de Arrasate en lo relativo a aspectos estratégicos y tácticos relacionados con el contrato, tanto comerciales (cumplimiento, necesidades del ayuntamiento de Arrasate, aspectos comerciales, etc.) como técnicos (planificación, calidad de los servicios, necesidades operativas, etc.).
- Asegurar la correcta realización de la prestación del contrato.

Dictar instrucciones a la empresa y en base a las decisiones adoptadas por el responsable del Contrato del ayuntamiento de Arrasate.

- Verificar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).
- Informar al ayuntamiento de Arrasate de cualquier incidencia que se produjera durante

ematea.

- Ezarpen-fasean:
  a) Ezarpena garaiz eta behar bezala egiten dela zaintzea, eta ezarpenaren azken arduraduna izatea.

- Mantentze-fasean:
  a) Kontratua behar bezala betetzen dela zaintzea, eta enpresa esleipenduneko langileek egindako zerbitzuen kalitatea eta lanen kalitate teknikoa egiaztatzea.
  b) ANSei dagozkien aldizkako txostenak egitea, Arrasateko Udalak egiazta ditzan.

- Edozein fasetan:
  a) Arrasateko Udalari jarduketa operatiboak eta horien plangintza proposatzea, onar ditzan.
  b) Enpresa esleipendunaren lantaldeko langileei jarraibideak ematea, hartutako erabakietan oinarrituta.
  c) Kontratua gauzatzean gertatzen den edozein gorabeheraren berri ematea Arrasateko Udalari.

5.3. Txostenak.

Kontratuaren jarraipen egokia egiteko, enpresa esleipendunak aurreko puntuetan deskribatutako txostenak egingo ditu, eta, ondoren, formatu elektronikoan, ezartzen den formatuaren arabera.

Txosten bakoitzaren eredu xehatua, eduki zehatza eta banaketa proiektuaren hasieran zehaztuko dira, enpresa esleipendunak eta Arrasateko Udalak izendatutako langileek batera.

la ejecución del contrato.

- Durante la fase de implantación:
  b) Velar por que la implantación se ejecute en tiempo y forma, siendo el responsable último de la misma.

- Durante la fase de mantenimiento:

a) Velar por el adecuado cumplimiento del contrato y verificar la calidad de los servicios y la calidad técnica de los trabajos realizados por el personal de la empresa adjudicataria.
  b) Emitir los informes periódicos correspondientes a los ANS para su comprobación por parte del ayuntamiento de Arrasate.

- En cualquier fase:

a) Proponer al ayuntamiento de Arrasate, para su aprobación, las actuaciones operativas y su planificación.
  b) Dictar instrucciones al personal del equipo de trabajo de la empresa adjudicataria en base a las decisiones adoptadas.
  c) Informar al ayuntamiento de Arrasate de cualquier incidencia que se produjera durante la ejecución del contrato.

5.3. Informes.

Para el adecuado seguimiento del contrato, la empresa adjudicataria emitirá los informes que se describen en los puntos anteriores, y a continuación, en formato electrónico de acuerdo con el formato que se establezca.

El modelo detallado de cada informe, el contenido concreto y su distribución será definido en el arranque del proyecto de forma conjunta entre la empresa adjudicataria y el personal designado por el ayuntamiento de Arrasate.

Código Exp.: 2025CHOZ0016 **Asunto:** Zibersegurtasun proiektuaren ezarpena

Txostenak garaiz eta kalitatez entregatzea, batez ere aldizkako txostenetan eta txosten arautuetan, funtsezkoa da kudeaketa-zerbitzuak ondo funtziona dezan.

Arrasateko Udalak beretzat gordetzen du eskainitako kalitate-parametroen betetze-mailari buruzko auditoriak egiteko eskubidea, bai bertako langileekin, bai kanpoko enpresa independenteen bitartez. Horretarako behar diren baliabide guztiak jarri beharko ditu bere esku operadore esleipendunak.

La puntualidad y calidad en la entrega de informes, especialmente en los informes periódicos y reglados, es de importancia primordial para el buen funcionamiento del servicio de gestión.

El ayuntamiento de Arrasate se reserva el derecho de realizar auditorías sobre el grado de cumplimiento de los parámetros de calidad ofrecidos, bien con personal propio, o bien a través de empresas externas independientes, debiendo poner el operador adjudicatario a su disposición, todos los medios necesarios para ello.

Arrasaten, 2026ko urtarrilaren 16an

UDAL INFORMATIKARIA

ARRASATEKO UDALA
AYUNTAMIENTO DE MONDRAGÓN

IKER.AGIRRESAROBE.URDANPILLETA
2026/01/16