Usurbilgo Udala

USURBILGO UDALAREN DATU-SAREAREN SEGURTASUN-EBALUAZIOA KONTRATATZEKO ETA SAREKO EKIPAMENDU ELEKTRONIKOA HORNITZEKO ETA MANTENTZEKO BALDINTZA TEKNIKOEN AGIRIA

1.- SARRERA

Usurbilgo Udalak, eraldaketa digitalerako eta bere sistemen segurtasuna hobetzeko estrategiaren barruan, lizitazio hau abian jarri du bere sare informatikoaren babesa indartzeko helburuarekin. Horretarako, udal-sare lokalaren zibersegurtasunaren egoeraren ebaluazio osoa egingo da, izan daitezkeen ahuleziak detektatzeko, hobetzeko beharrak identifikatzeko eta Segurtasun Eskema Nazionalean (SEN) ezarritako eskakizunak zenbateraino betetzen diren egiaztatzeko. Lortutako emaitzetan oinarrituta, eguneratu behar diren ekipoak berrituko dira, perimetroko firewall-a ordeztea lehentasunezko lana izango delarik, firewall horren euskarri teknikoa 2026an amaituko baita. Gainera, kontratuan sarea eta ekipoak mantentzeko lanak sartuko dira, bai eta beharrezko lizentziak eta euskarriak eskuratzeko lanak ere. Horrela, herritarrei kalitatezko zerbitzu digitalak eskaintzeko ingurune teknologiko seguruagoa eta egokiagoa izatea bermatuko da.

Usurbilgo Udalak sareko elektronikako ekipoak ditu bere komunikazioen ardatz gisa. Sareko elektronikaren funtzioa funtsezkoa da sareen konektagarritasuna, segurtasuna eta errendimendu optimoa bermatzeko.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA EVALUACIÓN DE SEGURIDAD DE LA RED DATOS Y SUMINISTRO Y MANTENIMIENTO DEL EQUIPAMIENTO ELECTRÓNICO DE RED DEL AYUNTAMIENTO DE USURBIL

1.- INTRODUCCIÓN

El Ayuntamiento de Usurbil, en el marco de su estrategia de transformación digital y mejora de la seguridad de sus sistemas, pone en marcha esta licitación con el objetivo de reforzar la protección de su red informática. Para ello, se llevará a cabo una evaluación completa del estado de la ciberseguridad de la red local municipal, que permitirá detectar posibles vulnerabilidades, identificar necesidades de mejora y verificar el grado de cumplimiento de los requerimientos establecidos en el Esquema Nacional de Seguridad (ENS). En base a los resultados obtenidos, se renovarán los equipos que sea necesario actualizar, incluyendo, de manera prioritaria, la sustitución del firewall de perímetro, cuyo soporte técnico finalizará en 2026. Además, el contrato incluirá el mantenimiento de la red y los equipos, así como la adquisición de las licencias y soportes necesarios, garantizando así un entorno tecnológico más seguro y preparado para ofrecer servicios digitales de calidad a la ciudadanía

El Ayuntamiento de Usurbil dispone de equipos de electrónica de red como núcleo de sus comunicaciones. La función de la electrónica de red es esencial para garantizar la conectividad, la seguridad y el rendimiento óptimo de las redes

Nabarmendu behar da udal eraikin ezberdinak, zuntzezko eraztun baten bidez (edo izar eran kasu batzuetan) lotuta daudela. Horretaz gain, udalak, firewall bat du, sarbide perimetrala kontrolatzeko funtsezko sistema gisa. Firewallak segurtasun-hesi gisa jokatzen du, eta sarearen trafikoa gainbegiratu eta kontrolatzen du, erakundearen helburu eta betekizunekin bat datozen segurtasun-politika jakin batzuetan oinarrituta. Segurtasun-sistema egonkorra eta eraginkorra bermatzeko, beharrezkoa da gailu hau eguneratuta izatea eta asistentzia tekniko egokia izatea.

2.- KONTRATUAREN XEDEA

Lizitazio honen helburua Usurbilgo Udalaren sarearen egoeraren zibersegurtasun mailari dagokion ebaluazio tekniko integrala egitea da, sare horretara konektatutako ekipo elektroniko eta sistema guztiak barne.

Ebaluazio horren emaitzetatik abiatuta, enpresa esleipendunak azpiegitura teknologikoa hobetzeko beharrezko jarduerak proposatu eta inplementatu beharko ditu, beharrezkotzat jotzen diren sare-ekipoen hornidura, instalazioa, konfigurazioa eta abiaraztea barne.

Lehentasuna eman beharko zaio perimetroko firewall berria hornitu, instalatu, konfiguratu eta abian jartzeari, gaur egun erabiltzen ari den ekipoaren euskarria 2026an amaituko baita.

Zibersegurtasunaren ebaluazioaren helburuak hauek izango dira:

- Udalaren azpiegitura teknologikoaren egungo segurtasun-maila egiaztatzea
- Informazioaren konfidentzialtasuna, osotasuna edo erabilgarritasuna arriskuan jar dezaketen kalteberatasunak edo arriskuak identifikatzea.

Usurbilgo Udala

Cabe destacar que los diferentes edificios municipales están unidos por un anillo de fibra (o en algunos casos, en forma de estrella). Además, el ayuntamiento dispone de un firewall que desempeña un papel crucial como sistema de control de acceso perimetral. El firewall actúa como una barrera de seguridad que supervisa y controla el tráfico de red conforme a un conjunto de políticas de seguridad alineadas con los objetivos y requisitos de la organización. Para garantizar un sistema de seguridad estable y eficiente, es necesario que este dispositivo se mantenga actualizado y cuente con soporte técnico adecuado.

2.- OBJETO DEL CONTRATO

El objeto de la presente licitación es la realización de una evaluación técnica integral de ciberseguridad del estado de la red del Ayuntamiento de Usurbil, incluyendo todos los equipos electrónicos y sistemas conectados a dicha red.

A partir de los resultados de esta evaluación, la empresa adjudicataria deberá proponer e implementar las actuaciones necesarias para la mejora de la infraestructura tecnológica, incluyendo el suministro, instalación, configuración y puesta en marcha de los equipos de red que se consideren necesarios.

Se deberá priorizar el suministro, instalación, configuración y puesta en marcha de un nuevo firewall de perímetro, dado que el soporte del equipo actualmente en uso finalizará en 2026.

La evaluación de ciberseguridad tendrá como objetivos:

- Verificar el nivel de seguridad actual de la infraestructura tecnológica del Ayuntamiento.
- Identificar posibles vulnerabilidades o riesgos que puedan comprometer la confidencialidad, integridad o disponibilidad de la información.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

- Segurtasun Eskema Nazionalaren (SEN) betetze-maila aztertzea, dagokion mailan, maiatzaren 3ko 311/2022 Errege Dekretuan ezarritakoaren arabera.

- Lotutako sistemetan, sareetan edo prozesuetan gabezia tekniko eta antolamendukoak antzematea, eta zuzentzeko edo hobetzeko neurriak proposatzea.

Halaber, plegu tekniko honen xedea ere bada honako hauek bermatzea:

- Sare lokalaren eta sareko elektronikako ekipoen mantentze-zerbitzua kontratatzea.

- Hornitutako ekipoen fabrikatzaileei dagozkien euskarriak eta lizentziak erostea.

Kontratazioaren irismenak barne hartzen du aipatutako sarearen eta ekipoen mantentze prebentiboa eta zuzentzailea, bai eta kontratuaren xede diren ekipoei buruzko kontsulta eta zalantza teknologikoen aurrean aholkularitza ematea ere.

Ekipoen lizentziak zuzenean kontratatu beharko dira ekipoen fabrikatzaileekin. Kontratuaren esleipenduna izango da lizentzia kudeaketa egingo duena fabrikatzailearekin. Horretaz gain, ekipoen mantentze-lana egiteaz eta dagokion asistentzia teknikoa emateaz ere arduratuko da.

- **Justifikazioa eta testuingurua**

Ekintza hau funtsezko oinarria da Udalaren eraldaketa digitalerako estrategiaren baitan. Gaur egungo azpiegitura teknologikoak mugak ditu zibermehatxu modernoei aurre egiteko eta herritarrei eskaintzen zaizkien zerbitzu digital gero eta ugariagoei behar bezala erantzuteko.

Usurbilgo Udala

- Analizar el grado de cumplimiento con el Esquema Nacional de Seguridad (ENS), en el nivel que le corresponda, conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo.

- Detectar deficiencias técnicas y organizativas en los sistemas, redes o procesos asociados, y proponer medidas correctoras o de mejora.

Asimismo, es también objeto del presente pliego técnico garantizar:

- La contratación del servicio de mantenimiento de la red local y de los distintos equipos de electrónica de red.

- La adquisición de los soportes y licencias correspondientes a los fabricantes de los equipos suministrados.

El alcance de la contratación incluye el mantenimiento preventivo y correctivo de la red y los equipos mencionados, así como de asesoramiento ante consultas y dudas tecnológicas sobre los equipos objeto del contrato.

Las licencias de los equipos deberán contratarse directamente con los fabricantes de los equipos. El adjudicatario del contrato será quien realice la gestión de la licencia con el fabricante. Asimismo, se encargará, también, del mantenimiento del equipamiento y de la asistencia técnica correspondiente.

- **Justificación y contexto**

Esta actuación constituye un pilar fundamental dentro de la estrategia de transformación digital del Ayuntamiento. La infraestructura tecnológica actual presenta limitaciones para hacer frente a las ciberamenazas modernas y para dar soporte al creciente número de servicios digitales que se ofrecen a la ciudadanía.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Inbertsioa erabat justifikatuta dago, Segurtasun Nazionalaren Esparrua (SEN) arautzen duen 311/2022 Errege Dekretuan, maiatzaren 3koa, ezarritako eskakizun tekniko eta antolakuntza-eskakizunak betetzeko beharragatik.

Azpiegitura berriak honako hauetarako aukera emango du:

- Udal sare lokalerako sarrera kontrola hobetzea.
- Datu eta sistema sentikorrak babesteko sarearen segmentazio egokia bermatzea.
- Zibersegurtasun erasoen aurrean, monitorizazio, detekzio eta erantzuteko gaitasunak indartzea.

3.- ZERBITZUAREN IRISMENA

Kontratuaren irismenak ekipo eta osagai hauen mantentzea jasotzen du:

- **Udal-azpiegiturako rack ezberdinen zuntzaren interkonexioa: Zuntz eraztuna**

  E= Eraikina

Usurbilgo Udala

La inversión se encuentra plenamente justificada por la necesidad de cumplir con las exigencias técnicas y organizativas establecidas en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS). Concretamente, la nueva infraestructura permitirá:

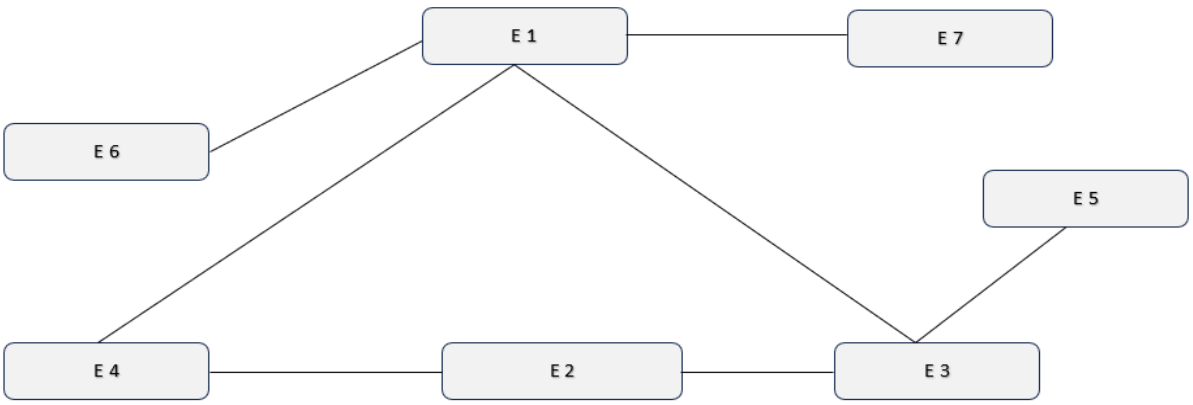
- Mejorar el control de acceso a la red interna.
- Garantizar una segmentación de red adecuada para proteger los sistemas y datos sensibles.
- Reforzar las capacidades de monitorización, detección y respuesta ante incidentes de seguridad.

3.- ALCANCE DEL SERVICIO

El alcance del contrato incluye el mantenimiento de los siguientes equipos y componentes:

- **Interconexión de la fibra de los diferentes racks de la infraestructura municipal: anillo de fibra**

  E= Edificio



Zuntzaren konfigurazioa: 24 zuntz kable batean, monomodo, monotubo eta metalezko

Configuración de fibra: 24 fibras en un cable con monomodo, monotubo y revestimiento metálico.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

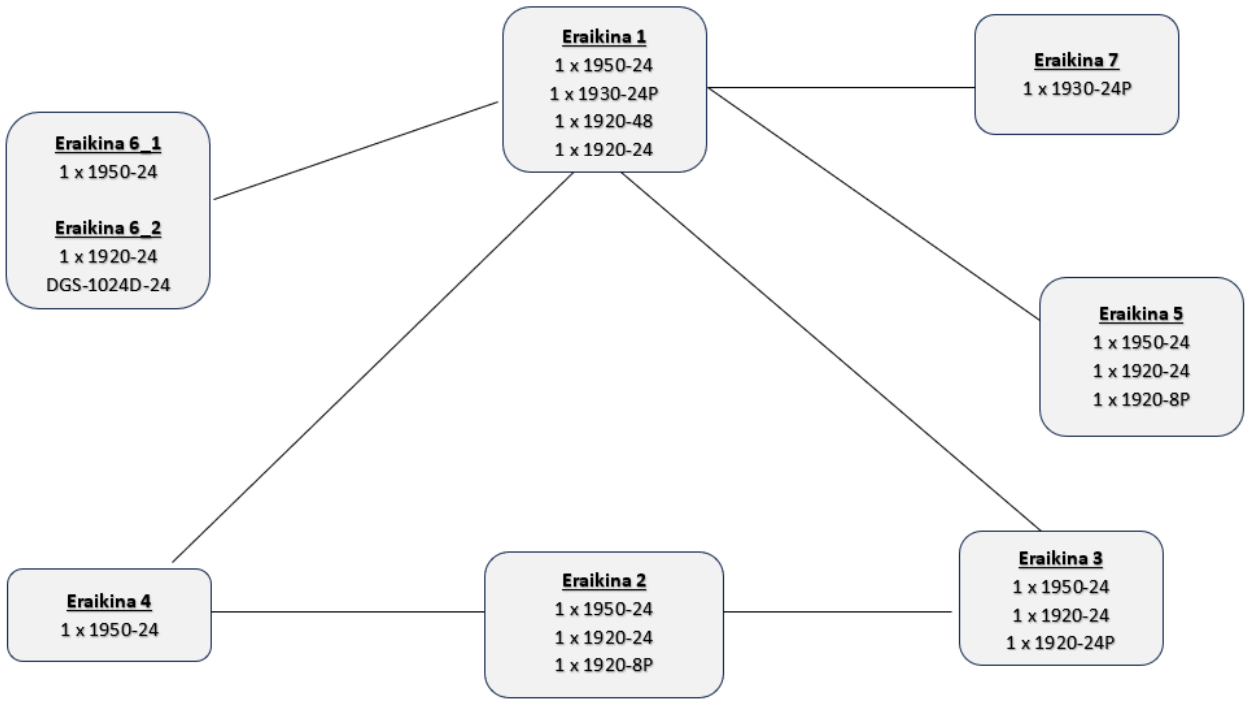
estaldurarekin.

Egoitzen arteko konexioak eraztun eran eginda daude, 3 eraikin izan ezik (E5, E6 eta E7). Azken hauek, zuzenean konektatuta daude beste eraikin batzuetatik, izar eran.

Las conexiones entre las sedes están realizadas en forma de anillo, excepto 3 edificios (E5, E6 y E7). Estos 3, están conectados directamente desde otro edificio en forma de estrella.

- **Switch-ak eta APak:**

- **Switches y APs:**



Guztira / Total		
HP ProCurve 1950-24G Switch	6	2017
HP ProCurve 1920-48G	1	2017
HP ProCurve 1920-24G Switch	4	2017
HP ProCurve 1920-24G PoE Switch	1	2017
HP ProCurve 1930-24G PoE Switch	3	2024
Switch HP 1920-8G-PoE+ (65W)	2	2017
D-Link DGS-1024D	1	2025
HP ProCurve X121 1G SFP+ LC SR Transceiver	32	2017
HP ProCurve X132 10G SFP+ LC LR Transceiver	0	
Antena Sophos	17	2017

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

- **Firewall-a:**

Udalak, udal-sarearen babesa bermatze aldera, Sophos SG 210 firewall bat erabiltzen du. Gailu honek sareko trafikoaren azterketa zehatza egiten du, egokiak diren konexioak ahalbidetuz eta mehatxu diren edo egokiak ez diren konexioak blokeatuz. Halaber, intrusioen prebentzio eta edukien iragazketa sistema integratuek baimenik gabeko sarbideak saihesten dituzte eta azpiegitura eraso zibernetikoetatik babesten laguntzen dute

Firewall honek, gainera, VPN (Sare Pribatu Birtuala) eta zifratze-funtzionalitateak eskaintzen ditu, eta erabiltzaile anitzeko konexio seguruak modu eraginkorrean kudeatzeko gaitasuna ematen du.

Egungo firewall-ak 2026an izango du bizitza baliagarriaren amaiera (End of Life), eta beraz, fabrikatzailearen segurtasun- eta euskarri teknikoko eguneratzeak jasotzeari utziko dio. Hori dela eta, lehentasunezkotzat jotzen da amaiera data hori baino lehen berritzea, azpiegituraren babesa arriskuan ez jartzeko.

Firewall berriak udal-sarearen segurtasuna eta jarraitutasuna bermatu beharko ditu, Segurtasun Eskema Nazionalaren (ENS) printzipioak eta neurriak betez, dagokion mailan.

Gutxienez, honako ezaugarri hauek izan beharko ditu:

- Gutxieneko funtzioak: firewall stateful, VPN IPsec/SSL IKEv2 euskarriarekin, IPS, lotura-ateko antibirusa eta URL/DNS iragaztea.
- Funtzio aurreratuak (ENS sistema kritikoetarako): zero eguneko sandboxinga, detekzioa eta erantzun hedatua (XDR), DNS iragazki aurreratua eta endpoint babesa, edo funtzionalitate baliokidea.
- Sarbide segurua kontrolatzeko funtzionalitateak, SD-WAN bidez trafikoa optimizatzeko aukera, birusen aurkako babesa sarrera-puntuan, intrusioak prebenitzeko sistema (IPS), sarea aurkitu eta monitorizatzea (Network Discovery), eta gutxienez 365 egunez, erregistroak hodeian edo sistema baliokide batean atxikitzea (logs).

- **Firewall:**

El Ayuntamiento dispone de un firewall Sophos SG 210, que asegura la protección de la red municipal. Este dispositivo realiza un análisis detallado del tráfico de la red, permitiendo conexiones legítimas y bloqueando aquellas que representen una amenaza o no sean adecuadas. Además, su sistema de prevención de intrusiones y filtrado de contenido ayuda a prevenir accesos no autorizados y proteger la infraestructura contra posibles ataques cibernéticos.

Este firewall, además, ofrece VPN (Red Privada Virtual) y funcionalidades de cifrado, y proporciona la capacidad de gestionar de forma eficaz conexiones seguras multiusuario.

El firewall actual alcanzará su fin de vida útil (End of Life) en 2026, lo que implica que dejará de recibir actualizaciones de seguridad y soporte técnico por parte del fabricante. Por ello, se considera prioritaria su renovación antes de dicha fecha para no comprometer la protección de la infraestructura.

El nuevo firewall deberá garantizar la seguridad y continuidad de la red municipal, cumpliendo los principios y medidas del Esquema Nacional de Seguridad (ENS), en el nivel que le corresponda.

Deberá contar, al menos, con las siguientes características:

- Funciones mínimas: firewall stateful, VPN IPsec/SSL con soporte IKEv2, IPS, antivirus de puerta de enlace y filtrado de URL/DNS.
- Funciones avanzadas (para sistemas críticos ENS): sandboxing de día cero, detección y respuesta extendida (XDR), filtrado DNS avanzado y protección de endpoints, o funcionalidad equivalente.
- Funcionalidades de control de acceso seguro, optimización de tráfico mediante SD-WAN, protección antivirus en el punto de entrada, sistema de prevención de intrusiones (IPS), descubrimiento y monitorización de red (Network Discovery), y retención de registros (logs) en la nube o en sistema equivalente durante al menos 365 días.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

- Erabilgarritasun handia: arkitektura erredundante aktibo-aktiboa edo aktibo-pasiboa, degradaziorik gabeko zerbitzu-jarrairako.
- Gutxieneko edukiera: errendimendu egokia eta latentzia baxua duten aldi berean konektaturiko 200 gailurentzat babesa.
- Kudeaketa zentralizatua: lehendik dagoen kudeaketa-plataforman integratzea, segurtasun-politiken, alerten eta txostenen kudeaketa bateratua ahalbidetuz.

- **Aurreko ekipoetara konektatutako interkonexio-elementuak: Stack moduluak, zuntz-modulua, …**

- **Udal-azpiegiturako rack ezberdinen zuntzaren interkonexioa.**

Zerbitzuen irismenak bai hardwarearen bai softwarearen osagaiak hartuko ditu, bai eta interkonexio-elementuak eta dagozkien lizentzien kudeaketa ere.

4.- KONTRATATUKO DIREN ZERBITZUAK

Jarraian agiri honen bidez eskatzen diren zerbitzuen gutxieneko irismena adierazten da:

- **Zibersegurtasun mailaren ebaluaketa:**

Sareko ekipamenduaren mantentze-lanen kontratuaren irismenaren barruan, esleipendunak zibersegurtasun-ebaluazio bat egin beharko du, kontratuaren xede diren ekipoak eta sareko azpiegitura osoa barne hartuta. Ebaluazio horren helburua izango da ahuleziak, arriskuak eta balizko eraso-bektoreak identifikatzea, eta neurri zuzentzaileak edo arintze-neurriak proposatzea.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

- Alta disponibilidad: arquitectura redundante activo-activo o activo-pasivo para continuidad de servicio sin degradación.

- Capacidad mínima: protección de al menos 200 dispositivos concurrentes con rendimiento adecuado y baja latencia.

- Gestión centralizada: integración en la plataforma de administración existente, permitiendo gestión unificada de políticas, alertas e informes de seguridad.

- **Elementos de interconexión conectados a los equipos anteriores: módulos de stack, módulos de fibra, …**

- **Interconexión de fibra de los diferentes racks, de la infraestructura municipal.**

El alcance de los servicios abarcará tanto los componentes de hardware como los de software, así como sus elementos de interconexión y la gestión de las licencias correspondientes.

4.- SERVICIOS A CONTRATAR

A continuación, se indica el alcance mínimo de los servicios solicitados a través del presente expediente:

- **Evaluación del nivel de ciberseguridad:**

Dentro del alcance del contrato de mantenimiento del equipamiento de red, el adjudicatario deberá realizar una evaluación de ciberseguridad que abarque tanto los equipos objeto del contrato como la infraestructura de red en su conjunto. Esta evaluación tendrá como objetivo identificar vulnerabilidades, riesgos y posibles vectores de ataque, proponiendo medidas correctivas o de mitigación.

Ebaluazioa Segurtasun Eskema Nazionalean (SEN) ezarritako printzipioen eta betekizunen arabera egin beharko da, erakunde kontratatzaileari aplikatu beharreko segurtasun-mailan, eta, honako alderdi hauek izango ditu kontuan, gutxienez:

- Sareko gailuen konfigurazio seguruaren azterketa (suebakiak, kommutadoreak, bideratzaileak, sarbide-puntuak, etab.).
- Sare-arkitektura aztertzea, segmentazioan, trafiko-kontrolean, sarbide-puntuetan eta kanpo-sareekiko esposizioan egon daitezkeen ahuleziak identifikatuz.
- Tresna automatizatuen bidez ahuleziak detektatzea eta sistemak eskuz berrikustea.
- Hardware, firmware eta softwarearen egoera egiaztatzea, bertsio zaharkituak edo kalteberatasun ezagunak dituztenak identifikatuta.
- Sarbide- eta autentifikazio-politikak saihestea, pasahitzen, rolen eta urruneko sarbideko mekanismoen erabilera barne.
- SENek ezarritako segurtasun-neurriak betetzen direla egiaztatzea, batez ere komunikazio-azpiegitura babesteari dagokionez.
- Emaitzen txosten xehatua, honako hauek barne:
  - Antzemandako ahuleziak eta horien kritikotasun-maila
  - Zuzenketa gomendio teknikoak.
  - Azpiegituraren segurtasuna indartzeko ezarri beharreko jardunbide egokiak.

Ebaluazioa, kontratuaren hasieran egin beharko da, eta, ondoren, urtean behin gutxienez, edo azpiegituran aldaketa nabarmenak egiten direnero.

- **Ekipo berrien instalazioa:**

Zibersegurtasunaren ebaluazio teknikoaren ondorioz, segurtasunaren arloan antzemandako akatsak konpontzeko, sare lokalaren eta konektatutako ekipoen babes egokia bermatzeko

Usurbilgo Udala

La evaluación deberá realizarse conforme a los principios y requisitos establecidos en el Esquema Nacional de Seguridad (ENS), en el nivel de seguridad que resulte de aplicación a la organización contratante, y contemplará, al menos, los siguientes aspectos:

- Análisis de configuración segura de los dispositivos de red (firewalls, switches, routers, puntos de acceso, etc.).
- Revisión de la arquitectura de red, identificando posibles debilidades en la segmentación, control de tráfico, puntos de acceso y exposición a redes externas.
- Detección de vulnerabilidades mediante herramientas automatizadas y revisión manual de los sistemas.
- Comprobación del estado del hardware, firmware y software, identificando versiones obsoletas o con vulnerabilidades conocidas.
- Revisión de políticas de acceso y autenticación, incluyendo el uso de contraseñas, roles y mecanismos de acceso remoto.
- Comprobación del cumplimiento de medidas de seguridad establecidas por el ENS, especialmente en relación con la protección de la infraestructura de comunicaciones.
- Informe detallado de resultados, incluyendo:
  - Vulnerabilidades detectadas y su nivel de criticidad.
  - Recomendaciones técnicas para su corrección.
  - Buenas prácticas a implementar para fortalecer la seguridad de la infraestructura.

La evaluación deberá realizarse al inicio del contrato y, posteriormente, con una periodicidad mínima anual o tras cambios significativos en la infraestructura.

- **Instalación de Nuevos Equipos y Componentes de Seguridad**

Como resultado de la evaluación técnica de ciberseguridad, la empresa adjudicataria deberá proponer, suministrar, instalar y configurar los equipos, componentes o soluciones técnicas

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

eta Segurtasun Eskema Nazionalak (SEN) eskatzen dituen baldintzak betetzen direla ziurtatzeko, enpresa esleipendunak beharrezko ekipo, osagai eta soluzio teknikoak proposatu, hornitu, instalatu eta konfiguratu beharko ditu

necesarias para subsanar las deficiencias detectadas en materia de seguridad, garantizar la protección adecuada de la red local y de los equipos conectados y asegurar el cumplimiento de los requisitos exigidos por el Esquema Nacional de Seguridad (ENS).

Ekipamendu berriak guztiz bateragarria izan beharko du egungo azpiegiturarekin, eta lehentasuna eman beharko die egungo baliabideak ahalik eta gehien berrerabiltzeko konponbideei eta alferrikako dimentsionatzeak edo inbertsioak saihestekoei.

El nuevo equipamiento deberá ser totalmente compatible con la infraestructura existente, priorizando soluciones que maximicen la reutilización de los recursos actuales y eviten sobredimensionamientos o inversiones innecesarias.

Bereziki baloratuko da proposatutako kommutazio- edo segurtasun-ekipoak ezaugarri hauek betetzea:

Se valorará especialmente que los equipos de conmutación o seguridad propuestos cumplan las siguientes características:

Switchak:

Switches:

Switchek portu espezifikoen bidezko pilaketa fisikorako gaitasuna izan beharko dute, throughput altua eta pilaren barne-zirkulazioan latentzia txikia bermatzeko adinako banda-zabalera erantsia izan dezaten. Horrela, pilaketa-lotura ez da botila-lepo bat izango ekipoaren portuen guztizko errendimenduari dagokionez.

Los switches deberán disponer de capacidad de apilamiento físico mediante puertos dedicados, que permitan un ancho de banda agregado suficiente para garantizar un throughput elevado y una baja latencia en el tráfico interno de la pila, de modo que el enlace de apilamiento no constituya un cuello de botella respecto al rendimiento total de los puertos del equipo.

Era berean, administrazio-plataformatik kudeaketa zentralizatu bateratua bermatu beharko dute, kableatutako ekipamenduak (switching) eta Wi-Fi sarbide-puntuak elkarrekin kudeatu ahal izateko, sareko azpiegitura osoaren administrazio koherentea eta efizientea ziurtatuz

Asimismo, deberán garantizar una gestión centralizada unificada desde la plataforma de administración, de modo que se puedan gestionar conjuntamente los equipos cableados (switching) y los puntos de acceso Wi-Fi, asegurando una administración coherente y eficiente de toda la infraestructura de red.

Sarbide switchak (2 maila kudeagarria):

Switches de acceso (nivel 2 gestionables):

Sarbide-switchek 2. mailakoak izan behar dute, kudeagarriak, VLAN, QoS eta segurtasuneko oinarrizko funtzionaltasunekin, eta pilaketa fisikorako gaitasuna izan behar dute, aurrez deskribatutakoaren arabera, gutxieneko throughput agregatu altuarekin. Throughput-a gutxienez 80 Gbps-koa izatea baloratuko da.

Los switches de acceso deberán ser de nivel 2 gestionables, con funcionalidades básicas de VLAN, QoS y seguridad, y capacidad de apilamiento físico mediante puertos dedicados, según lo descrito anteriormente, con un throughput agregado mínimo elevado. Se valorará que el throughput sea de, al menos, 80 Gbps.

Switchek elikatze-iturri bikoitza instalatzeko aukera izan beharko dute, soluzioaren sendotasuna bermatzeko.

Los switches deberán contar con la posibilidad de instalar doble fuente de alimentación, para garantizar la robustez de la solución.

Banaketako/koreko switchak (3. maila):

Switches de distribución/core (nivel 3):

Banaketako/koreko switchek 3. mailakoak izan beharko dute eta VLANen arteko bideratze-

Los switches de distribución/core deberán ser de nivel 3, con funcionalidades de enrutamiento

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

funtzionaltasuna, trafikoaren eta segurtasunaren kontrol aurreratua, portuen bidez pilatzeko gaitasun fisikoa, aurrez deskribatutakoaren arabera, throughput erantsi altu batekin, sarearen beharren araberakoa eta banaketa- edo core-inguruneetara bideratua (400 Gbps edo gehiagoa izatea baloratuko da).

Switchek elikatze-iturri bikoitza instalatzeko ahalmena izango dute, konponbidearen sendotasuna bermatzeko. Core switchek gutxienez 8 uplink SFP+ ataka izateko gaitasuna izan beharko dute.

Soluzioak beharrezko 10Gbps SFP+ moduluak izan beharko ditu Coreko Switch-en eta kokapen ezberdinetan banatutako Access switch desberdinen arteko konexioa egin ahal izateko.

2. mailako sarbide-switchek eta 3. mailako core-switchek Multigigabit atakak izan beharko dituzte (gutxienez 1 Gbps eta 2,5 Gbps). Abiadura handiagokoekin bateragarriak izatea balioetsiko da (5 Gbps eta 10 Gbps), Wi-Fi 6 edo handiagoko sarbide-puntuekiko konektagarritasun optimoa bermatzeko.

Soluzioaren iraupena bermatzeko eta uneko errendimendu onena izateko, Wi-Fi sarbide-puntuek Wi-Fi 6 teknologia edo altuagoa izan beharko dute. Positiboki baloratuko da eskaintzen den teknologia Wi-Fi 7 izatea.

Switchen eta Wi-Fi sarbide-puntuen azpiegitura berriaren kudeaketa errazteko, kontrol-panel bakar eta bateratu batetik kudeagarriak izan behar dute. Ekipamenduak gutxienez 3 urteko lizentziak izan behar ditu hodeian oinarritutako gailuak kudeatu eta kontrolatzeko.

Proposatutako ekipamenduak —Firewallak, switchak eta Wi-Fi sarbide puntuak— gutxienez 3 urteko fabrikatzailearen laguntza izan behar du. Laguntza horrek honako hauek barne hartuko ditu:

- Hardwarearen ordezkapena, matxura gertatuz gero
- Firmware eguneraketen eskuragarritasuna, aipatutako aldian.

Usurbilgo Udala

entre VLANs, control avanzado de tráfico y seguridad, y capacidad de apilamiento físico mediante puertos dedicados según lo descrito anteriormente, con un throughput agregado elevado, acorde a las necesidades de la red y orientado a entornos de distribución o core (Se valorará que sea de 400 Gbps o superior).

Los switches contarán con la capacidad de instalar doble fuente de alimentación, para garantizar la robustez de la solución. Los switches Core deberán disponer de la capacidad de contar con al menos 8 puertos uplink SFP+.

La solución deberá incluir los módulos SFP+ 10Gbps necesarios para poder realizar la conexión entre los Switches de Core y los diferentes switches de Acceso repartidos en las diferentes ubicaciones.

Tanto los switches de acceso de nivel 2 como los switches de core de nivel 3 deberán disponer de puertos Multigigabit (al menos 1 Gbps y 2,5 Gbps). Se valorará la compatibilidad con velocidades superiores (5 Gbps y 10 Gbps) para garantizar la conectividad óptima con puntos de acceso Wi-Fi 6 o superiores

Con el fin de prever la longevidad de la solución y disponer del mejor rendimiento actual, los puntos de acceso Wi-Fi deberan contar con la tecnología Wi-Fi 6 o superior. Se valorará positivamente que la tecnología ofrecida sea Wifi 7.

Con el fin de facilitar la gestión de la nueva infraestructura de switches y puntos de acceso wifi, deben de poder gestionarse desde un mismo panel de control unificado en la nube. Los equipos deben contar con al menos 3 años de licencias para gestión y control de los dispositivos en la nube.

El equipamiento planteado —Firewalls, Switches y Puntos de acceso Wifi— debe contar con al menos 3 años de soporte por parte de fabricante. Este soporte incluirá los siguientes conceptos

- Reposición HW en caso de rotura
- Disponibilidad de actualizaciones de firmware durante el periodo mencionado

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

- Fabrikatzailearekin zuzenean kasuak irekitzeko aukera.

Instalazioak barne hartu beharko ditu ekipoen martxan jartzea, konfigurazio eta baliozkotze funtzionala, dokumentazio teknikoaren eguneraketa eta erakunde kontratatzaileak izendatutako teknikariei ezagutza transferitzea.

- **Lizentziak eta asistentzia fabrikatzailearekin kudeatzea:**
  - Kontratuaren xede diren ekipoen lizentziak urtero berrituko dira: Firewall-a, switchak, …
  - Fabrikatzailearen euskarri ofizialeko kontratua: Esleipendunak, kontratua indarrean dagoen bitartean, bermatu beharko du, firewall fabrikatzailearekin (gaur egun, Sophos) euskarri ofizial aktibo bat dagoela eta mantentzen dela. Euskarri horretan, gutxienez, honako hauek jasoko dira:
    - Argitaratutako firmwareen eta segurtasun-partxeen eguneratze guztietarako sarbidea
    - Gorabehera kritikoen kasuan eskalatzeko gaitasuna duen fabrikatzaile-mailako euskarri tekniko kualifikatua
    - Matxura baten ondorioz, hardwarea birjarri edo ordezkatzea, kontratatutako berme-baldintzen edo ordezkapen zerbitzuen arabera
    - Produktua erabilera seguru eta guztiz funtzionaleko baldintzetan mantentzeko beharrezkoak diren lizentziak eta harpidetzak eguneratzeko eskubidea

    Esleipendunak euskarri hori kudeatzeko, berritzeko eta dokumentazioaren egiaztapena egiteko ardura izango du, kontratuak irauten duen bitartean
  - Intzidentziak dauden kasuan, gorabeheren ticketen kudeaketa fabrikatzailearekin.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

- Posibilidad de apertura de casos directamente con el fabricante.

La instalación deberá incluir la puesta en marcha, configuración y validación funcional de los equipos, actualizar la documentación técnica y la transferencia de conocimiento al personal técnico designado por la entidad contratante.

- **Gestión de licencias y soportes con el fabricante:**
  - Las licencias de los equipos objeto de contrato se renovarán anualmente: Firewall, switches, …
  - Contrato de soporte oficial del fabricante: El adjudicatario deberá garantizar, durante toda la vigencia del contrato, la existencia y mantenimiento de un soporte oficial activo con el fabricante del firewall (actualmente Sophos), que incluya como mínimo:
    - El acceso a todas las actualizaciones de firmware y parches de seguridad publicados
    - Soporte técnico cualificado de nivel fabricante con capacidad de escalado en caso de incidencias críticas.
    - La reposición o sustitución del hardware en caso de avería conforme a los términos de garantía o servicios de reemplazo contratados.
    - El derecho a actualizaciones de licencias y suscripciones necesarias para mantener el producto en condiciones de uso seguro y plenamente funcional

    El adjudicatario será responsable de la gestión, renovación y verificación de la documentación de dicho soporte durante la vigencia del contrato.
  - Gestión de tickets de soporte con el fabricante en caso de incidentes.

Usurbilgo Udala

- **Sareko elektronikaren gestioa:**

  - Fabrikatzaileak gomendatutako segurtasun-eguneratzeak eta partxeak aplikatzea.
  - Firewalleko arauen konfigurazioan, VPNan, NATan, etab-en asistentzia.

- **Gestión de electrónica de red:**

  - Aplicación de actualizaciones y parches de seguridad recomendados por el fabricante.
  - Soporte en configuración reglas del firewall, VPNs, NATs, etc.

- **Mantentze-zerbitzua zuzentzailea**:

Zerbitzu honen barne egongo da sistemen erabateko funtzionamendua eta erabilgarritasuna eragozten duen edozein gorabehera, arazo, matxura edo disfuntzio fisiko zein logiko konpontzea, haien gaitasun operatibo osoa bermatuz. Zerbitzua urrunetik nahiz presentzialki eskainiko da, beharraren arabera, konponbiderik egokiena bermatuaz.

Zerbitzu honek, gutxienez, zeregin hauek izan behar ditu:

  - Fabrikatzaileak elementu matxuratuak konpontzea eta/edo ordezkatzea.
  - Ekipoen birkonfigurazioa: Ekipoen akats logikorik edo deskonfiguraziorik izanez gero, enpresa esleipendunak intzidentzia lehenbailehen konpontzen dela bermatu beharko du, kritikotasun-ingurune bakoitzerako esleitutako denboren arabera
  - Erroreak, argitaratutako inzidentziak edota fabrikatzaileen gomendioen ondorioz softwarea instalatzea.
  - Fabrikatzaileetara eskalatzea.

- **Servicio de mantenimiento correctivo**:

Este servicio incluye la reparación de cualquier incidencia, problema, avería o disfunción tanto física como lógica que impida el pleno funcionamiento y disponibilidad de los sistemas, asegurando así su completa capacidad operativa. El servicio será ofrecido tanto de manera remota como in situ, según sea necesario, para asegurar una respuesta óptima a las incidencias.

Este servicio deberá incluir como mínimo las siguientes tareas:

  - Reparación y/o sustitución de elementos averiados por parte del fabricante.
  - Reconfiguración de equipos: En caso de fallo lógico o desconfiguración de los equipos, la empresa adjudicataria deberá garantizar una pronta resolución de la incidencia según los tiempos asignados para cada entorno de criticidad.
  - Instalación de software por fallo, vulnerabilidades publicadas o por indicación del fabricante.
  - Escalado a fabricantes.

- **Mantentze-zerbitzu prebentiboa:** modu erregularrean egin beharko dira aurrez planifikatutako eta sistematizatutako jarduerak, hutsegiteak eta matxurak aurreikusi edo ahalik eta gehien murrizteko, gailuen bizitza baliagarria luzatzeko eta haien funtzionamendu fidagarria bermatzeko.
- **Sareko elektronika-ekipoen denbora errealeko monitorizazio-zerbitzua** eta alerten kudeaketa

- **Servicio de mantenimiento preventivo:** se deberán de realizar tareas planificadas y sistemáticas de manera regular con el fin de prevenir o minimizar la aparición de fallos y averías, prolongar la vida útil de los equipos y garantizar su funcionamiento confiable.
- **Servicio de monitorización en tiempo real y gestión de alertas** de los equipos de electrónica de red.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

- Sareko gailu guztien konfigurazioaren **asteko Backup zerbitzu automatizatua,** akatsak, informazio-galerak edo azpiegiturari egindako erasoak gertatzeko arriskua minimizatzeko.
- Kontratuaren xede diren ekipoen gaineko kontsultak eta zalantza teknologikoak ebazteko **Aholkularitza-zerbitzua**.

- **Ekipoen arteko loturen diagnostikoa:**
  - Firewall-ak edo bestelako arreta berezia eskatzen duten ekipamenduak dauden armairu edo racketan kableatua begiz eta fisikoki berrikustea
  - Kudeatutako ekipoen konektagarritasunari eragiten dioten kable egituratuak ziurtatzea eta egiaztatzea. Beharrezkoa da erreflektometria egitea eraikin bereko rack ezberdinak lotzeko zuntz optikoko loturen egoera zehazteko.

- **Formazioa:** Udaleko teknikariak segurtasun-azpiegitura berrira egokitzen laguntzeko, enpresa esleipendunak, firewall-aren funtzionamenduari eta instalatutako segurtasun-sistema berriei buruzko prestakuntza berezia eman beharko du.

- **Txostenak:**

Dokumentazio tekniko guztia udalaren zerbitzarian egongo da, horretarako berariaz egokitutako direktorioan, eta eguneratuta egon beharko du une oro.

Gutxienez, honako dokumentazioa jaso beharko da:

- Topologiak, konfigurazioak, lizentziak,… buruzko informazioa.
- Kontratuak estaltzen dituen ekipoen inbentario eguneratua.
- Firewallaren kudeaketari buruzko txostenak.
- Zibersegurtasun alorrean, segurtasun neurriak hobetzeko eta arriskuak arintzeko txostenak.

Usurbilgo Udala

- **Servicio de Backup automatizado semanal** de la configuración de todos los dispositivos de red, con el objetivo de minimizar el riesgo ante fallos, pérdidas de información o ataques a la infraestructura.
- **Servicio de asesoramiento** para resolver consultas y dudas tecnológicas sobre los equipos objeto del contrato.

- **Diagnóstico de los enlaces entre equipos:**
  - Revisión visual y física del cableado en armarios o racks donde se alojan los firewalls u otros equipos sensibles
  - Certificación y verificación del cableado estructurado que afecten la conectividad de los equipos gestionados. Se requiere realizar la reflectometría para determinar el estado de los enlaces de fibra óptica de unión entro los diferentes racks dentro de un mismo edificio.

- **Formación:** Con el fin de facilitar la adaptación del personal técnico del Ayuntamiento a la nueva infraestructura de seguridad, la empresa adjudicataria deberá impartir una formación específica sobre el funcionamiento del firewall y los nuevos sistemas de seguridad instalados

- **Informes:**

Toda la documentación técnica estará en el servidor municipal, en el directorio habilitado al efecto y, además, deberá estar actualizada en todo momento.

Deberá contener, al menos, la siguiente documentación

- Información sobre las topologías, configuraciones, licencias, …
- Inventario actualizado de los equipos cubiertos por el contrato.
- Informes sobre la gestión de Firewall.
- Informes de mejora de las medidas de seguridad y mitigación de riesgos en materia de ciberseguridad.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

- Gertakarien inbentarioa: Antzemandako gertakari guztien erregistro egituratua mantendu beharko da. Erregistro horrek honako informazioa jaso beharko du gutxienez: gertakariaren deskribapena, gertaera data eta ordua, kaltetutako sistema edo zerbitzuak, larritasun-maila, gertakariaren erroa (ezagutzen bada), aplikatutako zuzenketa-neurriak eta ebazpen-egoera. Inbentario hori udal zerbitzarian gordeko da, horretarako egokituriko direktorioan. Eguneratuta mantendu beharko da eta jarraipen teknikoko bileretarako eskuragarri egon beharko du.

- **Bilerak:**

Honako bilera hauek egitea aurreikusten da:

- Jarraipen teknikoko bilerak. (bi hilean behin)
- Firewallaren txostenak aztertu eta zibersegurtasunaren egoera ebaluatzeko bilerak. (sei hilean behin)
- Bilera estrategiko edo plangintza-bilera: Urteko plangintza- eta azterketa estrategikoko bilera bat egingo da, zerbitzuaren emaitzak ebaluatu, etorkizuneko behar teknologikoak aztertu eta hobekuntza-proposamenak egiteko.
- Ezohiko bilera edo eskatutakoak: Ezohiko bilerak deitu ahal izango dira gertaera kritikoak gertatzen direnean, eguneratze garrantzitsuak daudenean edo arduradun teknikariaren berehalako arreta eskatzen duen edozein egoeratan.

- **Zibersegurtasun aholkularitza:**

Kontratuaren esleipendunak etengabeko aholkularitza-zerbitzua eskaini beharko dio Udalari zibersegurtasunaren arloan, udal-sistema informatikoen, sareen, gailuen eta datuen babesa bermatzeko.

Aholkularitza horrek, gutxienez, honako ekintza hauek barne hartuko ditu

Usurbilgo Udala

- Inventario de incidencias: Se deberá mantener un registro estructurado de todas las incidencias detectadas, incluyendo, al menos, su descripción, fecha y hora de la incidencia, sistemas o servicios afectados, gravedad, causa raíz (si se conoce), acciones correctivas aplicadas y su estado de resolución. Este inventario se guardará en el servidor municipal, en el directorio habilitado para ello. Deberá estar actualizado y disponible para su revisión en las reuniones de seguimiento técnico.

- **Reuniones:**

Se prevén las siguientes reuniones

- Reuniones de seguimiento técnico (bimensual)
- Reunión de análisis de informes del firewall y estado de la ciberseguridad (semestral)
- Reunión estratégica o de planificación: Se realizará una reunión anual de planificación y análisis estratégico para evaluar los resultados del servicio, analizar las necesidades tecnológicas futuras y realizar propuestas de mejora.
- Reuniones extraordinarias o a demanda: Se podrán convocar reuniones extraordinarias en caso de incidentes críticos, actualizaciones relevantes o cualquier situación que requiera atención inmediata por parte del personal técnico responsable

- **Asesoramiento en Ciberseguridad:**

El adjudicatario del contrato deberá prestar al Ayuntamiento un servicio de asesoramiento continuo en materia de ciberseguridad, con el fin de garantizar la protección de los sistemas informáticos, redes, dispositivos y datos municipales.

Este asesoramiento incluirá, como mínimo, las siguientes acciones:

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

- Udalaren azpiegitura teknologikoan zibersegurtasunaren egoeraren urtekako ebaluazioa, ahulezia edo konfigurazio desegokiei arreta berezia eskainiz. Kontratuaren hasieran egoeraren hasierako ebaluazioa egingo da.
- Segurtasun neurriak hobetzeko eta arriskuak arintzeko neurrien (teknikoak zein antolaketakoak) proposamena. Neurri horiek sei hilean behingo txosten batean aurkeztu beharko dira, edo gorabehera garrantzitsuak hautematen direnean
- Informatika-sistemak, hodeiko zerbitzuak, zerbitzariak, gailu mugikorrak, WiFi sareak eta horiekin lotutako beste elementu batzuk eguneratzeari, konfigurazio seguruei eta jardunbide egokiei buruzko gomendioak
- Informazioaren segurtasunari dagokionez, datuen babesaren arloko araudia betetzeari buruzko aholkularitza (DPBEDBLO eta DBEO).
- Segurtasuneko barne-politikak zehazten laguntzea, sarbide-protokoloak, pasahitzen kudeaketa, informazio-babesa eta gorabeheren aurreko erantzuna barne.
- Zibersegurtasun-intzidenteen kasuan laguntza ematea, etorkizunean errepikapenak saihesteko analisia, arintzea eta gomendioak barne.

Esleipendunak zibersegurtasunaren arloko langile kualifikatuak eta esperientzia egiaztatua izan beharko ditu, eta Udalak edozein unetan eskatu ahal izango du hori egiaztatzen duen dokumentazioa.

- **Zerbitzuaren beste hainbat ezaugarri:**

Gorabeherei erantzun eraginkor eta egoki bat emateko, zerbitzua urrutitik edo in situ eskainiko da, beharren arabera. Horregatik, eta konponketa-denbora egokia dela bermatzeko, esleipendunak 70 km-tik beherako distantzia batean izan beharko du ordezkaritza edo egoitza.

ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9

Usurbilgo Udala

- Evaluación anual del estado de la ciberseguridad en la infraestructura tecnológica del Ayuntamiento, con especial atención a posibles vulnerabilidades o configuraciones inadecuadas. Se realizará una evaluación inicial de la situación al inicio del contrato.
- Propuesta de mejora de medidas de seguridad y mitigación de riesgos, tanto técnicas como organizativas, que deberán presentarse en un informe semestral o cuando se detecten incidencias relevantes.
- Recomendaciones sobre actualizaciones, configuraciones seguras y buenas prácticas en el uso de sistemas informáticos, servicios en la nube, servidores, dispositivos móviles, redes WiFi y otros elementos relacionados.
- Asesoramiento sobre el cumplimiento normativo en materia de protección de datos (LOPDGDD y RGPD) en lo que respecta a la seguridad de la información.
- Colaboración en la definición de políticas internas de seguridad, incluyendo protocolos de acceso, gestión de contraseñas, respaldo de información y respuesta ante incidentes.
- Asistencia en caso de incidentes de ciberseguridad, incluyendo análisis, mitigación y recomendaciones para evitar futuras recurrencias.

El adjudicatario deberá contar con personal cualificado y experiencia acreditada en materia de ciberseguridad, pudiendo el Ayuntamiento requerir en cualquier momento documentación que lo acredite

- **Otras características del servicio:**

El servicio se proporcionará tanto de forma remota como in situ, según sea necesario, para garantizar una respuesta efectiva y oportuna a las incidencias. Por ello, y para garantizar que el tiempo de resolución sea el adecuado, el adjudicatario deberá disponer de delegación o sede a una distancia inferior a los 70 km.

Erantzun-denbora hauexek ezartzen dira adjudikaziodunak bete beharreko gutxieneko baldintza gisa:

- Gehieneko erantzun-denbora: hornitzaileak gehienez ere ordubeteko epean erantzun beharko du, intzidentzia jasotzen denetik.
- Intzidentzien konponketa-denbora: ekiporen batek gaizki funtzionatzen badu zerbitzua gelditu gabe, intzidentzia hurrengo lanegunaren aurretik konpondu beharko da.
- Larrialdietarako erantzun-denbora: Berehalako erantzuna behar duen zerbitzu bat eteten bada, hornitzaileak intzidentzia gehienez ere 4 orduko epean konpontzeko ardura izango du.
- Funtzionamenduari eta konfigurazioari buruzko kontsulten inguruko gehieneko erantzun denbora 2 lanegunekoa izango da.

Informatika Saileko Arduraduna

Usurbilgo Udala

Se establecen los siguientes tiempos de respuesta como requisitos mínimos que deberá cumplir el adjudicatario:

- Tiempo de respuesta máximo: el proveedor deberá proporcionar una respuesta en un plazo máximo de una hora desde la recepción de la incidencia.
- Tiempo de resolución de incidencias: en caso de mal funcionamiento sin parada de servicio, se requerirá que la incidencia se resuelva antes del siguiente día laborable.
- Tiempo de respuesta para emergencias: en caso de parada de un servicio que requiera de una respuesta inmediata, el proveedor tendrá la responsabilidad de solucionar la incidencia en un plazo máximo de 4 horas.
- El tiempo máximo de respuesta para consultas sobre funcionamiento y configuración será de 2 días laborables.

Responsable del Departamento de Informática

EKS | CSV: ESKUdccc85c1-1ae0-4f9e-bb3f-6c4a3592acb9
Egiaztatu dokumentu honen osotasuna eta sinadura hurrengo URL edo QR kodean sartuz: https://udal.egoitza.gipuzkoa.eus?De=07310
Compruebe la integridad y firma de este documento, accediendo a la siguiente URL o código QR: https://udal.egoitza.gipuzkoa.eus?De=07310