

**IRUNGO UDALAREN
SEGURTASUN-OPERAZIOEN ZENTROA (SOC)
MANTENTZEKO ETA KUDEATZEKO KONTRATAZIOA**

- BALDINTZA TEKNIKOEN PLEGUA -

**CONTRATACIÓN DEL MANTENIMIENTO Y GESTIÓN
DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)
DEL AYUNTAMIENTO DE IRUN**

- PLIEGO DE PRESCRIPCIONES TÉCNICAS -

ARLO SUSTATZAILEA/ ÁREA PROMOTORA: GOBERNU IREKIAREN ETA HERRITARRENTZAKO ARRETAREN
ARLOA / AREA DE GOBIERNO ABIERTO Y ATENCIÓN CIUDADANA
EXPEDIENTE KODEA/ CÓDIGO EXPEDIENTE: 2024ZAUN0103

1. KONTRATUAREN XEDEA

Irungo Udalaren helburua 2023tik aurrera garatutako proiektuari jarraipena ematea da. Proiektu horren bidez, Segurtasun Operazioen Zentro bat (SOC) hedatu eta kudeatu da, partzialki kanporatuta. Zentro horrek zibersegurtasunaren eta ziberzaintzaren arloan dituen gaitasunak nabarmen handitu eta hobetu ditu, eta segurtasun-monitorizazioa, intzidenteen detekzio goiztiarra eta mehatxuen eta kalteberatasunen zaintza eta analisi automatizatu eta sustatu ditu, ziberintzidenteen aurrean erreakzionatzeko, erantzuteko eta berreskuratzeko gaitasuna ere hobetuz.

Horren arabera, lizitazio honen helburua zera kontratatzea da:

1. Irungo Udalaren Segurtasun Operazioen Zentroa (SOC) azpiegituraren mantenimendu perfektiboa eta ebolutiboa
2. Urrutiko CyberSOC zerbitzuak ematea, ezarritako SOC azpiegitura monitorizatzeko eta kudeatzeko beharrezkoak direnak.

Aldaera hauetarako aukerarekin:

➤ **A ALDAERA:** Udalaren sistemetan "on

1. OBJETO DEL CONTRATO

El Ayuntamiento de Irun tiene como objetivo dar continuidad al proyecto, desarrollado desde 2023, consistente en el despliegue y gestión, parcialmente externalizada, de un Centro de Operaciones de Seguridad (SOC), que ha supuesto una importante ampliación y mejora de sus capacidades en ciberseguridad y cibervigilancia, automatizando y potenciando la monitorización de seguridad, la detección temprana de incidentes, y la vigilancia y análisis de amenazas y vulnerabilidades, mejorando también su capacidad de reacción, de respuesta y de recuperación ante ciberincidentes.

De acuerdo con ello, el objeto de esta licitación es siguiente:

1. El mantenimiento, perfectivo y evolutivo, de la infraestructura SOC del Ayuntamiento de Irun.
2. La prestación de los servicios de CyberSOC remoto, necesarios para la monitorización y gestión de dicho SOC.

Con opción a las siguientes variantes:

➤ **VARIANTE A:** SOC ya implantado e integrado

premise" ezarritako eta integratutako SOC, Udal Informazio Sistemaren babes-premia gero eta handiagoetara egokituz, Agiri honetan ezarritako preskripzioen arabera, gaur egun Zibersegurtasun Operazioetarako Zentroen Sare Nazionalen integratuta mantenduz, eta integrazio hori CCN-CERTek ezar ditzakeen jarraibide berrien arabera garatuz.

- **B ALDAERA:** SOC soluzio berria: SIEM alternatibo bat ezartzea 2.3.2 B.1) atalean adierazitako ezaugarrien arabera, eta online eta cloud modalitatean ezartzea onartuko da.

(Enpresa bakoitzak proposamen bakarra aurkeztu ahal izango du: A SAIHESBIDEA edo B SAIHESBIDEA, ez biak).

2. EZAUGARRI TEKNIKOAK ETA PROIEKTUAREN IRISMENA.

2.1 JARDUERA ESPARRUA.

Administrazio Publiko osoak bezala, konektatutako gizarte honetan oro har edozein erakundek bezala, Irungo Udalak aurre egin behar die zibermehatxuen gero eta bolumen eta sofistikazio handiagoari, gero eta konplexutasun handiagoko TI-ko inguruneetan, erakundeak barne-funtzionamenduan eta herritarrei, enpresei eta gizarte-erakundeei emandako zerbitzuetan lortutako digitalizazio-mailagatik.

Udal Sarearen zabaltasuna eta sakabanatzeak, kanpoko sistemekin gero eta konektagarritasun eta elkarreragingarritasun handiagoa izateak, dagoeneko ezarrita dauden zerbitzuei buruz aztertu beharreko datuen bolumenak eta alerta moduan iragazteko eta azkar erantzuteko beharrak gaur egun guztiz bideraezina egiten dute zibersegurtasun-azterketa eskuz egitea. Hori dela eta, 2022an, EU Next Generation laguntza-programak Administrazioari eskaintzen zion Europako finantzaketaren aukera aprobetxatuz, kontratazio bat abiarazi zen (2022ZAUN0093 espediente), prozesuak automatizatzeko eta segurtasun-kudeaketa zentralizatzeko proiektu bat garatzeko helburuarekin,

'on premise' en los sistemas del Ayuntamiento, adecuándolo a las crecientes necesidades de protección del Sistema de Información Municipal de acuerdo con las prescripciones establecidas por este Pliego, manteniendo su actual integración en la Red Nacional de Centros de Operaciones de Ciberseguridad, y evolucionando esta integración conforme a las nuevas directrices que el CCN-CERT pueda establecer.

- **VARIANTE B: Nueva solución SOC:** Implantación de un SIEM alternativo según las características indicada en el apartado 2.3.2 B.1), admitiéndose tanto su implantación on-premise como en modalidad cloud.

(Cada empresa solamente podrá presentar una única propuesta, de la VARIANTE A o de la VARIANTE B, no ambas).

2. CARACTERÍSTICAS TÉCNICAS Y ALCANCE DEL PROYECTO

2.1. ÁMBITO DE ACTUACIÓN.

Como toda la Administración Pública, como cualquier entidad en general en esta sociedad conectada, el Ayuntamiento de Irun debe hacer frente al creciente volumen y sofisticación de las ciberamenazas, en entornos de TI de complejidad creciente y de cada vez mayor criticidad por el grado de digitalización alcanzado por la Institución en su funcionamiento interno y en sus servicios a la ciudadanía, empresas y entes sociales.

La amplitud y dispersión de la Red Municipal, la creciente conectividad e interoperabilidad con sistemas externos, el volumen de datos a analizar de los servicios ya implantados, y la necesidad de filtrado y rápida respuesta en forma de alertas, hace hoy día del todo inviable la realización de un análisis de ciberseguridad de forma manual. Por ello, en 2022, aprovechando las posibilidades de la financiación europea que ofrecía a la Administración el programa de ayudas EU Next Generation, se lanzó una contratación (expediente 2022ZAUN0093) con el objetivo de desarrollar un proyecto para automatizar los procesos y centralizar la gestión de seguridad mediante instrumentos que ayudasen a simplificar la

gordetzen eta kudeatzen den informazioa eta ematen diren zerbitzu elektronikoak babesteko lan zaila sinplifikatzen lagunduko zuten tresnen bidez.

Kontratazioak, dirulaguntzen programa horren 5. linearen (Zibersegurtasuna) jarraibideei jarraituz, CCN-CERT katalogoko tresnetan oinarritutako soluzio teknologiko bat hedatzea izan zuen helburu, segurtasun-intzidentek monitorizatu, detektatu eta kudeatzeko.

Hala, inplementatutako SOCa izan da, 2023ko lehen hiruhilekoan abian jarri zenetik, Udala-sareko jardueraren, zerbitzarien, datu-baseen, aplikazioen, webguneen eta beste udal-sistema batzuen jarraipena eta analisia etengabe egiteaz arduratu den sistema, segurtasun-mehatxu baten adierazle izan daitezkeen ezohiko jarduerak bilatuz, informazio hori neurri zuzentzaileak aplikatzeko helburuarekin jaso dadin, dagozkion jakinarazpenak sortuz.

Aurreko kontratazio horren ondorioz hedatutako SOCa Zibersegurtasuneko Operazio Zentroen Sare Nazionalaren (RNS) parte da gaur egun, eta Sare horren koordinazioa Ziberintzidenteen Jakinarazpenerako eta Jarraipenerako Plataforma Nazionalaren bidez egiten da, Informazio-sare eta -sistemen segurtasunari buruzko irailaren 7ko 12/2018 Errege Lege Dekretua garatzen duen urtarrilaren 26ko 43/2021 Errege Dekretuaren 11. artikuluan aurreikusitakoaren arabera.

Orain, kontratazio berri honen helburua da Irungo Udalaren SOCAren egungo azpiegitura mantentzea eta, ahal bada, hobetzea, dela egungo konfigurazioari eutsita, MonICA SIEMn oinarrituta, dela CCN-CERTek homologatutako SIEM soluzioa sartzen dela, dela sistemetan modu lokalean ezarritako on premise soluzio gisa mantenduta, dela enpresa esleipendunak emandako hodeiko zerbitzu gisa.

Gainera, kontratu honek irauten duen bitartean, enpresa esleipenduna arduratuko da azpiegitura horren beharrezko egokitzapenak ezartzeaz, Irungo Udaleko SOC Zibersegurtasuneko Operazio Zentroen Sare Nazionalan erabat integratuta mantentzeko.

difícil tarea de proteger la información que se alberga y gestiona, así como los servicios electrónicos que se prestan.

La contratación, siguiendo las directrices de la Línea 5 (Ciberseguridad) de dicho programa de subvenciones, se centró en el despliegue de una solución tecnológica basada en herramientas del catálogo del CCN-CERT orientadas a la monitorización, detección y gestión de incidentes de seguridad.

Así, el SOC implementado ha sido, desde su puesta en marcha en el primer trimestre de 2023, el sistema encargado de realizar de forma permanente el seguimiento y análisis de la actividad en la Red Municipal, servidores, bases de datos, aplicaciones, sitios web y otros sistemas municipales, buscando actividades anómalas que puedan ser indicativas de una amenaza de seguridad, de modo que dicha información sea recogida con el fin de aplicar medidas correctivas, generando las correspondientes notificaciones.

El SOC desplegado en virtud de esa contratación precedente forma parte hoy de la Red Nacional de Centros de Operaciones de Ciberseguridad (RNS), cuya coordinación se lleva a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, prevista en el artículo 11 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Ahora, el objetivo de esta nueva contratación es mantener, y perfeccionar si cabe, la actual infraestructura de SOC del Ayuntamiento de Irun, ya sea manteniendo su actual configuración, basada en el SIEM MonICA o entra solución SIEM homologada por el CCN-CERT, y ya sea manteniéndola como solución on premise implantada en modo local en los sistemas, o como servicio en la nube prestado por la empresa adjudicataria.

Además, a lo largo de la duración del presente contrato, la empresa adjudicataria se encargará de implantar las necesarias adecuaciones de esta infraestructura que sean precisas para mantener al SOC del Ayuntamiento de Irun plenamente integrado en la Red Nacional de Centros de Operaciones de Ciberseguridad.

2.2 GARUR EGUN EZARRITA DAGOEN SISTEMAREN OSAGAIK

Aurreko kontratazioak honako hauek biltzen zituen:

1. SOCaren berezko tresnak hornitzea, ezartzea eta abiaraztea. Hori, funtsean, Estatuko CCN-CERTek homologatutako software-tresnekin egin behar da. Estatuko CCN-CERTek doan ematen zion lizentzia Espainiako Administrazioari.
2. Ezarritako azpiegitura (eguneratzeak eta hobekuntzak) kontratuaren bizitza osoan mantentzea.
3. SOCaren monitorizazioa, talde aditu batek kanpora ateratakoa (CyberSOC urrunekoa), etengabe eta modu iraunkorrean mailegatua, eguneko 24 orduetan x asteko 7 egunetan. Funtzio hori, funtsean, zerbitzu automatizatu bat ematean zetzan, sor zitezkeen alerten, zibererasoen, gure sistemetan detektatutako kalteberatasun berrien edo Udal-Sareko erabiltzaileek kudeatutako datu eta zerbitzuentzat arriskutsua izan zitezkeen ezohiko edozein jardueraren aurrean adituak ziren pertsonen esku-hartzearekin. Horretarako, gorabeherak jakinarazteko eta kudeatzeko hainbat tresna eta sistematika eratu behar ziren, kanpoko monitorizazio-lana eta Udaleko sistema-teknikariek hartu beharreko erremediatze-neurriak hartzeko lana koordinatzeko.

Gaur egun ezarrita dagoen konponbideak, aurretiko kontratu horren arabera, bere funtzioa behar bezala betetzen baitu, osagai hauek ditu:

2.2.A. Software tresnak

1. **SIEM gisa, MonICA NGSIEM tresna**, informazioa eta segurtasun-ekitaldiak kudeatzeko CCN-CERTen soluzio gisa (produktu ziurtatua bere segurtasun-funtzionaltasunetan, GOI mailako ENS gisa sailkatua). Funtsean, hauek dira funtzionalitate garrantzitsuenak:

2.2. COMPONENTES DEL SISTEMA ACTUALMENTE IMPLANTADO

La contratación precedente comprendía:

1. El aprovisionamiento, implantación y puesta en marcha de las herramientas propias del SOC, debiendo realizarse esto básicamente con herramientas software homologadas por el CCN-CERT estatal, cuyo licenciamiento se facilitaba de forma gratuita por éste a la Administración española.
2. El mantenimiento de la infraestructura implantada (actualizaciones y mejoras) a lo largo de toda la vida del contrato.
3. La monitorización del SOC, realizada de forma externalizada por un equipo experto (CyberSOC remoto), prestado de forma permanente e ininterrumpida, 24 horas al día x 7 días a la semana. Esta función consistía básicamente en la prestación de un servicio automatizado, con intervención humana experta ante las alertas que pudieran surgir, de detección de ciberataques, de nuevas vulnerabilidades detectadas en nuestros sistemas, o de cualquier actuación anómala por parte de los usuarios de la Red Municipal que pudiera constituir un riesgo para los datos y servicios por ésta gestionados. Para ello, se debían constituir una serie de herramientas y de sistemáticas de notificación y gestión de incidencias que coordinase el trabajo externo de monitorización con el trabajo de adopción de medidas resolutorias de remediación a adoptar por los Técnicos de Sistemas del Ayuntamiento.

La solución actualmente implantada, en virtud de dicho contrato previo, que viene cumpliendo su función de forma adecuada, consta de los siguientes componentes:

2.2.A. Herramientas software

1. **Como SIEM, la herramienta MonICA NGSIEM**, como solución del CCN-CERT para la gestión de información y eventos de seguridad (producto certificado en sus funcionalidades de seguridad, clasificado como ENS de nivel ALTO). Básicamente, sus funcionalidades más relevantes

- Gertaerak denbora errealean kudeatzea eta korrelatzea.
- Mehatxuak hautematea eta korrelatzea denbora errealean, korrelazio-motorraren bidez.
- Gertakari garrantzitsuak lehenestea eta ikertzea, erabilera pertsonalizatuko kasuen bidez.
- Erabiltzailearen portaera aztertzea.
- Mehatxuen ziberinteligentzia, MISPEkin integratuta (CCN-CERTeko REYES tresnarekin integratuta).
- CCN-CERTeko beste tresna batzuekin integratzea (LUCIA, SAT-INET).
- Kontrol sekurizatuko eta biltegitratze zentralizatuko puntu bakarra, gertaeren biltegitratze mugagabearekin.

Irungo Udalak, gaur egun, MonICA NGSIEMen Standalone lizentzia du, eta 17 monitore-lizentzia. Honako iturri hauek ditu:

1. Domeinu-kontrolatzaileak.
2. FW Palo Alto.
3. Ms/Exchange zerbitzaria.
4. SQL Server zerbitzariak.
5. Aplikazio-zerbitzariak (IIS, NGINXm Apache Tomcat eta Jboss).
6. CORTEX Endpoint antibirusa.
7. CCN-CERTeko SAT-INET zunda.

Gainera, 5 kontsulta-erabiltzaile daude tresna maneiatu eta kudeatzeko.

OHARRA: MonICA NGSIEM ez da Gertaerak Segundikorik (EPS) lizentziatu, ez erabiltzaile konkurrenteengatik, ezta erabilitako informazioagatik eta bolumetriagatik ere. MONICA NGSIEM log formatu desberdineko lizentzia da.

2. **LUCIA-Nube, CCN-CERTek garatutako tresna, gertaerak kudeatzeko eta komunikatzeko, Plataforma Nazionalarekin modu federatuan lan eginez, eta MonICako gure instalazioan integratuta.**
3. **REYES, CCN-CERTek ere emandako tresna, ziberintzidentek aztertzeko eta zibermehatxuei buruzko informazioa partekatzeko (MISP).**

son:

- Gestión y correlación de eventos en tiempo real.
- Detección y correlación de amenazas en tiempo real mediante su motor de correlación.
- Priorizar e investigar incidentes relevantes mediante casos de uso personalizables.
- Analizar el comportamiento del usuario.
- Ciberinteligencia de amenazas mediante la integración con MISP (integrado con la herramienta REYES del CCN-CERT).
- Integración con otras herramientas del CCN-CERT (LUCIA, SAT-INET).
- Punto único de control securizado y almacenamiento centralizado, con almacenamiento ilimitado de eventos.

El Ayuntamiento de Irun cuenta actualmente con una licencia Standalone de MonICA NGSIEM, y con 17 licencias de monitor, con las que integra las siguientes fuentes:

1. Controladores de dominio.
2. FW Palo Alto.
3. Servidor Ms/Exchange.
4. Servidores SQL Server.
5. Servidores de aplicaciones (IIS, NGINXm Apache Tomcat y Jboss).
6. Antivirus CORTEX Endpoint.
7. Sonda SAT-INET del CCN-CERT.

Además, se disponen de 5 usuarios de consulta para el manejo y gestión de la herramienta.

NOTA: MonICA NGSIEM no se licencia por Eventos por Segundo (EPS), ni por usuarios concurrentes, ni por información manejada y volumetría. MONICA NGSIEM se licencia por formato de log diferente.

2. **LUCIA-Nube, herramienta desarrollada por el CCN-CERT, para la gestión y comunicación de incidentes, operando de modo federado con la Plataforma Nacional, e integrada en nuestra instalación de MonICA.**
3. **REYES, herramienta también facilitada por el CCN-CERT, para el de análisis de ciberincidentes y compartir información de ciberamenazas (MISP).**

4. **SAT-INET zunda, CCN-CERT Alerta Goiztiarreko Sistemarekin (SAT) integratzeko.**

5. **NeuShield softwarea, Udal-Sareko erabiltzaile-postu guztietan hedatua, ransomware bidezko infekzioak prebenitzeko, bezeroei eta zerbitzariei txertoak inokulatuz.**

4. **Sonda SAT-INET, para la integración con el Sistema de Alerta Temprana (SAT) del CCN-CERT.**

5. **Software NeuShield, desplegado en todos los puestos de usuario de la Red Municipal, para la prevención de infecciones por ransomware mediante la inoculación de vacunas en clientes y servidores.**

2.2.B. Instalatutako hardwarea

Udaleko sistema informatikoan instalatutako KSaren hardware-euskarriak 2 makina ditu, gaur egun 2 urteko bizitza operatiboarekin:

- SIEM MonICaren euskarria SYS-5029P-WTR modeloko Supermikro ekipo bat da, eta ezaugarri hauek ditu:
 - o 2U
 - o CPU: 24 core 2,4 Ghz
 - o RAM: 128Gb RAM DDR4
 - o EDUKIERA:
 - 2 TB sistemarentzat, RAID 1
 - 10 TB datu primarioak RAID 5ean biltegitzeko.
 - o KONEKTIBITATEA:
 - Kudeaketa eta ekoizpena: 10G (kudeaketa) - 10G (ekoizpena)
 - Base-T 10/100/1000 ataka bat kudeaketarako.
 - o Elikatze-iturri bikoitza.
- SYS-1019P-WTR modeloko Supermikro ekipo batek eusten dio SAT-INET zundari:
 - o 1U
 - o INTEL XEON CASCADE LAKE-SP 4216 16C/32T 2.1G 9.6GT 2UPI 22M
 - o 16GB DDR4-2933 2Rx8 ECC REG DIMM
 - o 1 AOC-S3108L-H8IR-16DD 8P INT(hautazko 16ra. arte) LP 12Gb
 - o 2 MINI SAS HD,INT,60CM,30AWG
 - o 2.5" SSD SATA3 SAMSUNG PM883 240GB 6GB/S V4 TLC MZ7LH240HAHQ05 VNAND 7mm (1.3 DWPD) 2 diska
 - o GIGABIT 2P PCI-E RJ45 LP i350 Sareko adap.
 - o IN SITU bermea 3 LANURTE.

2.2.B. Hardware instalado

El soporte hardware del SOC instalado en el Sistema Informático municipal consta de 2 máquinas, actualmente con 2 años de vida operativa:

- El SIEM MonICA se soporta sobre un equipo Supermicro modelo SYS-5029P-WTR, con las siguientes características:
 - o 2U
 - o CPU: 24 cores 2,4 Ghz
 - o RAM: 128Gb RAM DDR4
 - o ALMACENAMIENTO:
 - 2 TB para sistema en RAID 1
 - 10 TB para almacenamiento de datos primarios en RAID 5.
 - o CONECTIVIDAD:
 - Gestión y producción: 10G (gestión) - 10G (producción)
 - un puerto Base-T 10/100/1000 para gestión
 - o Doble fuente de alimentación
- La sonda SAT-INET está soportada por un equipo Supermicro modelo SYS-1019P-WTR:
 - o 1U
 - o INTEL XEON CASCADE LAKE-SP 4216 16C/32T 2.1G 9.6GT 2UPI 22M
 - o 16GB DDR4-2933 2Rx8 ECC REG DIMM
 - o 1 AOC-S3108L-H8IR-16DD 8P INT(opc.hasta 16) LP 12Gb
 - o 2 MINI SAS HD,INT,60CM,30AWG
 - o 2 discos 2.5" SSD SATA3 SAMSUNG PM883 240GB 6GB/S V4 TLC MZ7LH240HAHQ05 VNAND 7mm (1.3 DWPD)
 - o T.RED GIGABIT 2P PCI-E RJ45 LP i350
 - o Garantía IN SITU 3 AÑOS laborables.

2.3. BEHARREZKO SOLUZIOA

2.3.1. PLATAFORMA MANTENTZEA

2.3.1 a. A Aldaera

Gaur egun Udalaren sistemetan on-premise ezarrita dagoen SOC azpiegitura mantenimendua eta CCN-CERTekin integrazioa.

Konponbide honen planteamendua guztiz jarraitua da, hau da, kontratu osoan zehar, on-premise bidez ezarritako egungo konponbideari mantentzea (SIEM MonICA eta REYES, LUCIA-hodeia eta SAT-INET tresnak). Orain arte, irtenbide hori eraginkorra izanez, enpresa esleipendunak bere gain hartuko ditu eguneraketak gauzatzea, CCN-CERTek adierazitako lehendik dauden tresnen edozein up-grade, bai eta CCN-CERTek adieraz dezakeen edozein tresna berri ezartzea ere, Irungo Udala RNSn erabat integratuta mantentzeko.

Enpresa esleipendunak SIEMek analisisian eta prozesamenduan sartu beharreko iturrien edo sistemen egungo zerrenda zabaltzea proposatzen duen proposamen teknikoaren barruan baloratuko da, betiere dokumentu honen 2.2.A.1 puntuan adierazitako iturrien egungo zerrenda oinarritzat hartuta.

Tresna osagarriak erabiltzea ere baloratuko da, betiere CCN-CERTek Udalarentzat doako lizentzia duten ziurtatutako produktuen esparruan. Tresna horiek funtzionalitate osagarriak emango dituzte mehatxu iraunkor aurreratuak (APT) detektatzeko eta/edo babesteko, sentsoreen bidez malware konplexua detektatzeko, etab.

Nolanahi ere, SIEMen logs guztiak enpresa esleipendunaren sistemetan atxikiko dira monitorizazio-zerbitzuak eta CyberSOC zerbitzuak emateko, gutxienez hilabete bat berotan (online sistemetan), eta, aldi berean, mekanismo sinple eta erabat automatizatu bat egon beharko da, gertaera guztiak Udalaren edo esleipendunaren azpiegituran gordetzeko, gutxienez urtebetez.

2.3. SOLUCIÓN REQUERIDA

2.3.1. MANTENIMIENTO DE LA PLATAFORMA

2.3.1.a. Variante A:

Mantenimiento de la infraestructura SOC actualmente implantada on-premise en los sistemas del Ayuntamiento, y de su integración con el CCN-CERT.

El planteamiento de esta solución es completamente continuista, consistiendo en el mantenimiento, a lo largo de todo el contrato, de la actual solución implantada on-premise (SIEM MonICA y herramientas REYES, LUCIA-nube y SAT-INET), que se ha manifestado hasta ahora efectiva, asumiendo la materialización de sus actualizaciones, cualquier up-grade de las herramientas preexistentes que sea indicado por el CCN-CERT, así como la implantación de cualquier nueva herramienta que pueda indicar el CCN-CERT para mantener al Ayuntamiento de Irun plenamente integrado en la RNS.

Se valorará dentro de la propuesta técnica que la empresa adjudicataria proponga ampliar la relación actual de fuentes o sistemas a incluir en el análisis y procesamiento por el SIEM, siempre tomando como base la lista actual de fuentes, indicada en el punto 2.2.A.1 de este documento.

Se valorará también la incorporación de herramientas adicionales, siempre en el marco de los productos certificados por el CCN-CERT con licenciamiento gratuito para el Ayuntamiento, que faciliten funcionalidades suplementarias para la detección y/o protección ante amenazas persistentes avanzadas (APT), para la detección de malware complejo mediante sensores, etc.

En todo caso, todos los logs del SIEM serán retenidos en los sistemas de la empresa adjudicataria en la prestación de servicios de monitorización y CyberSOC, durante un mínimo de un mes en caliente (en los sistemas online), al tiempo que deberá existir un mecanismo simple y totalmente automatizado para que todos los eventos sean igualmente guardados en infraestructura del Ayuntamiento o del adjudicatario durante al menos 1 año.

2.3.1.b. B Aldaera: SOC KSA soluzio berria (Gaur egun Udalean ezarrita dagoen SOCaren bilakaera, tresna edo itrenbide multzo berri baterantz).

Aldaera hori SIEM alternatibo batean oinarritutako proposamen bat aurkeztean datza, eta online eta cloud modalitateetan ezartzea onartuko da, betiere honako baldintza hauek betez:

- Proposatutako soluzioak SIEM MonICaren egungo ezarpenaren gainean dituen abantailei buruzko informazioa aurkeztu behar da, erreferentzia objektibo eta kontrastagarrii buruzkoa.
- CCN-CERTek homologatu behar du proposatutako SIEMa, eta "Informazioaren eta Komunikazioaren Teknologien Segurtasuneko Produktu eta Zerbitzuen Katalogoaren" (CCN-STIC 105 gida) azken edizioan agertu behar du.
- SAT-INET zundarako, egokiena da lehendik dagoen instalazioa mantentzea, bai softwarearen konfigurazioan, bai hura eusten duen hardwarearen aprobetxamenduan.
- Proposatutako SOCa CCN-CERTeko Red Nacional de SOC's (RNS)-en integratuko dela bermatu beharko da, bere plataformen, LUCIAren, REYESen eta SAT-INETen bidez, edo horiek ordeztzen dituzten beste batzuen bidez. Enpresa esleipenduna arduratuko da proposatutako SIEMa SOCen Sare Nazionalarekin koordinatzeko tresnekin integratzeko beharrezkoak diren lan teknikoez eta udal-teknikarien esku geratuko dira alderdi formalak (eskaerak, baimenak, etab.) CCN-CERTekin.
- **Migrazio-plan bat aurkeztuko da**, honako hauek jasoko dituenak:
 - SIEM ordezkatzeko prozesuaren planifikazioa, eta CCN-CERTekin integratzeko tresna guztiak (LUCIA, REYES eta SAT-INET) migratzeko sistematika.
 - Zenbat denboraz mantenduko

2.3.1.b. Variante B: Nueva solución SOC (Evolución del SOC actualmente implantado en el Ayuntamiento hacia un nuevo conjunto de herramientas o soluciones).

Esta variante consiste en la presentación de una propuesta basada en un SIEM alternativo, admitiéndose tanto su implantación on-premise como en modalidad cloud, cumpliendo en todo caso los siguientes requisitos:

- Debe presentarse información que documente, sobre referencias objetivas y contrastables, las ventajas que la solución propuesta presenta sobre la actual implantación del SIEM MonICA.
- EL SIEM propuesto debe estar homologado por el CCN-CERT y figurar en la última edición de su "Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación" (Guía CCN-STIC 105).
- Para la sonda SAT-INET lo apropiado es mantener la instalación pre-existente, tanto en la configuración del software como en el aprovechamiento del hardware que lo soporta.
- Deberá garantizarse la integración del SOC propuesto en la Red Nacional de SOC's del CCN-CERT por medio de sus plataformas, LUCIA, REYES y SAT-INET, u otras que las sustituyan en el futuro. La empresa adjudicataria deberá responsabilizarse de los trabajos técnicos necesarios para la integración del SIEM propuesto con las herramientas de coordinación con la Red Nacional de SOC's, quedando para los técnicos municipales los aspectos formales (peticiones, autorizaciones, etc.) con el CCN-CERT.
- Se presentará un **Plan de Migración** en el que se referencie:
 - La planificación del proceso de sustitución del SIEM, y la sistemática de migración de todas las herramientas de integración con el CCN-CERT (LUCIA, REYES y SAT-INET).
 - Durante cuánto tiempo se

/existituko den MoniCA SIEM berriarekin eta zein funtzionamendu-planteamendurekin. Prozesu horretarako gehieneko denbora 10 egun naturalekoa izango da.

- Migrazio-prozesuak zerbitzuaren galeraren edo gelditzearen bat ekarri beharko duen, eta, beraz, aldaketa-prozesuan zibermehatxuren bat gertatuz gero, arriskuak hartu behar diren.

- Proposatutako SIEMa informazio-iturri multzo bati aplikatuko zaio. Informazio-iturri horiek, gutxienez, gaur egungoak izan beharko dute:

- Domeinu-kontrolatzaileen logak eta gertaerak.
- Firewallaren logak eta gertaerak (Palo Alto).
- Udal Informazio Sistemako SQL Server zerbitzarien logak eta gertaerak.
- Exchange plataformaren logak eta gertaerak.
- Aplikazio-zerbitzarien logak eta gertaerak (IIS, NGINX, Apache Tomcat y Jboss).
- Birusen aurkako motorren logak eta gertaerak (Cortex Endpoint).

Hala ere, enpresa esleipendunak sartu beharreko iturri edo sistemen zerrenda zabaltzea proposatzea baloratuko da, betiere aurreko zerrenda oinarritzat hartuta. Nolanahi ere, sare publikoen eraginpean dauden sistemen gertaerei emango zaie lehentasuna.

- Proposatutako konponbideek CCN-CERTek Espainiako Administrazioarako emandako doako lizentziamenduaren mende egon behar dute. Babes-tresna osagarriak planteatzen badira, CCN-CERTek Administrazioari eskaintzen dizkion tresnen katalogotik kanpo, kostu hori lizitatzailerak hartuko du bere gain, kontratazio honen marjina ekonomikoen barruan.
- Proposatutako SOCak nazioarteko SOC sare baten parte izan behar du, eta segurtasunaren arloko ziurtagiriak izan behar ditu (gutxienez ENS GOI-MAILAKOAK eta ISO 27001).

mantendrá/coexistirá MoniCA con el nuevo SIEM y con qué planteamiento de funcionamiento. El tiempo máximo para este proceso será de 10 días naturales.

- Si el proceso de migración deberá suponer alguna pérdida o detención de servicio, y por lo tanto la asunción de riesgos ante una eventual ciberamenaza durante dicho proceso.

- El SIEM propuesto se aplicará sobre un conjunto de fuentes de información, que cuando menos deberán ser las actuales:

- Logs y eventos de los controladores de dominio.
- Logs y eventos del firewall (Palo Alto).
- Logs y eventos de los servidores SQL Server del Sistema de Información Municipal.
- Logs y eventos de la plataforma Exchange.
- Logs y eventos de los diferentes servidores de aplicaciones (IIS, NGINX, Apache Tomcat y Jboss).
- Logs y eventos de los motores antivirus (Cortex Endpoint).

No obstante, se valorará que la empresa adjudicataria proponga ampliar la relación de fuentes o sistemas a incluir, siempre tomando como base la lista anterior.

En cualquier caso, se priorizarán los eventos de los sistemas expuestos a redes públicas.

- Las soluciones propuestas deben estar sujetas a licenciamiento gratuito facilitado por el CCN-CERT para la Administración española. Si se plantean herramientas de protección complementarias, fuera del catálogo de las ofrecidas por el CCN-CERT a la Administración, este coste estará asumido por el licitador dentro de los márgenes económicos de la presente contratación.
- El SOC propuesto debe formar parte de una red de SOC de ámbito internacional, y debe contar con certificaciones en el ámbito de la seguridad (al menos ENS de nivel ALTO e ISO 27001).

- Proposatutako plataformak ez ditu handituko eraso bat kudeatzaren kostuak (tiketekin eta alertekin lotutako bolumetriarik gabe, irenste-bolumenagatik soilik, kontratu osoan zehar kostu egonkorra mantenduz).
- SIEMek mehatxu potentzialei buruz dagoen informazio guztia ere bilduko du, eta erasoen aurrean erreakzionatzea ez ezik, horiek prebenitzea ere ahalbidetuko du, gerta daitezkeenari aurrea hartzen saiatuz.
- SIEMen log guztiak enpresa esleipendunaren sistemetan atxikiko dira monitorizazio-zerbitzuak eta CyberSOC zerbitzuak emateko, gutxienez hilabete berotan (online sistemetan), eta, aldi berean, mekanismo sinple eta erabat automatizatu bat egon beharko da gertaera guztiak Udalaren azpiegituran gordetzeko, gutxienez urtebetez.
- Proposatutako plataformak inbentarioa egiteko eta aktiboak katalogatzeko mekanismo bat izango du. Log-ak ez dira zuzenean sistemetatik bidaliko; aitzitik, elementu kolektoreak erabiliko dira, enpresa esleipendunak emandakoak eta Udalaren azpiegituran instalatutakoak, eta gateway gisa jardungo dute esleipendunaren jarraipen-plataformara. SIEMen datuak korrelazioen bidez edo eraso-patroiak identifikatzea ahalbidetzen duten beste teknika batzuen bidez tratatuko dira.
- Plataforma kontrolatzeko eta kudeatzeko emandako kontsola edo kontsolak web formatuan izango dira, eta edozein inguruetan exekutatu ahal izango dira, fabrikatzailearen sistema jabetzen beharrik gabe.
- Nolanahi ere, garrantzi handikoa izango da proposatutako tresnen integrazio- eta osagarritasun-maila, bai eta tresna horien konfigurazioa eta administrazioa zentralizatzeko gaitasuna ere.
- La plataforma propuesta no incrementará los costes por la gestión de un ataque (sin volúmenes relacionados con tickets ni alertas, únicamente por volumen de ingesta, manteniendo un coste estable a lo largo de todo el contrato).
- El SIEM recogerá también toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques sino también prevenirlos, intentando anticiparse a que sucedan.
- Todos los logs del SIEM serán retenidos en los sistemas de la empresa adjudicataria en la prestación de servicios de monitorización y CyberSOC, durante un mínimo de un mes en caliente (en los sistemas online), al tiempo que deberá existir un mecanismo simple y totalmente automatizado para que todos los eventos sean igualmente guardados en infraestructura del Ayuntamiento durante al menos 1 año.
- La plataforma propuesta dispondrá de un mecanismo de inventario y catalogación de activos. Los logs no se enviarán directamente desde los sistemas, sino que se utilizarán elementos colectores, proporcionados por la empresa adjudicataria e instalados en la infraestructura del Ayuntamiento, que actúen como gateway hacia la plataforma de seguimiento de la adjudicataria. En el SIEM se realizará el tratamiento de los datos mediante correlaciones u otras técnicas que permitan la identificación de patrones de ataque.
- La consola o consolas facilitada/s para el control y gestión de la plataforma, lo será/n en formato web, permitiendo su ejecución en cualquier entorno, sin necesidad de sistemas propietarios del fabricante.
- En cualquier caso, será de capital importancia el grado de integración y complementariedad de las herramientas propuestas, así como la capacidad de centralización de su configuración y administración.

2.3.2. Urrutiko CyberSOC zerbitzuak ematea.

Kontratuan zehar, enpresa esleipendunak hartutako SIEMek detektatutako arrisku-egoera posible guztiak monitorizatu eta kudeatu beharko ditu, bai proposatutako irtenbidea egungo MonICA NGESIEM soluzioa mantentzea bada, bai SIEM alternatibo bat aukeratzen bada, on premise edo cloud bertsioan instalatuta.

Garatu beharreko zerbitzuen gutxienezko ezaugarriak, GUTXIENEZ, honako hauek izan behar dira nahitaez:

- Gertakizunen kudeaketa.

- Enpresa esleipenduna arduratuko da SIEM plataformaren arauak, korrelazio-estrategiak eta optimizazioa sortzeaz, adierazitako sistemak babesteko, SIEMen jarduera inplementatuko den informazio-iturrien multzotik abiatuta.
- Esleipendunaren ardura izango da sortutako alerten eraginkortasuna berrikustea, alertak etengabe hobetzeko, bai eta SIEM eta monitorizatutako gailuak sintonizatzea ere, detekzio-prozesua optimizatzeko.
- Plataformak, halaber, kalteberatasunak identifikatzeko zerbitzu bat izan behar du, bai azpiegiturei dagokienez bai aplikazioei dagokienez, kalteberatasunen inbentarioa egin ahal izateko, segurtasun-arrakala horien bilakaera egiaztatzearen. Halaber, zibersegurtasuneko gertaeren zerrendekin (IOC) elikatuko da sistema, ahalik eta eguneratze-mailarik handienarekin.
- Hasierako ekitaldien bolumena (gutxienez jasan beharrekoa) segundoko 1.500 ekitaldi izango dela kalkulatu da, urtean %20ko hazkunde posiblearekin.
- Enpresa esleipenduneko segurtasun teknikari batek 24x7an berrikusi beharko ditu SIEM motorrak sortzen dituen alertak, Irungo Udaleko Informatika Zerbitzuko teknikariei bidali aurretik eman beharreko urrats gisa. Gertakariak identifikatzean positibo faltsuak ezabatzen

2.3.2. Prestación de los servicios de CyberSOC remoto.

A lo largo del contrato, la empresa adjudicataria deberá realizar la monitorización y gestión de todas las situaciones de posible riesgo detectadas por el SIEM adoptado, tanto si la solución propuesta consiste en el mantenimiento de la actual solución MonICA NGESIEM, como si se opta por un SIEM alternativo, instalado ya sea on premise o en versión cloud.

Las características mínimas de los servicios a desarrollar deben ser, obligatoriamente, **AL MENOS**, las siguientes:

- Gestión de los eventos.

- La empresa adjudicataria será responsable de la creación de reglas, estrategias de correlación y optimización de la plataforma SIEM para proteger los sistemas indicados, a partir del conjunto de fuentes de información sobre las que se habrá implementado la actuación del SIEM.
- Será responsabilidad de la adjudicataria revisar la efectividad de las alertas generadas para la mejora continua de éstas, así como la sintonización del SIEM y de los dispositivos monitoreados con el fin de optimizar el proceso de detección.
- La plataforma debe incluir asimismo un servicio de identificación de vulnerabilidades, tanto a nivel de infraestructura como de aplicaciones, que permita mantener un inventario de vulnerabilidades que permita contrastar la evolución de dichas brechas de seguridad. Igualmente, se alimentará el sistema con listas de incidentes de ciberseguridad (IOCs) con el mayor nivel de actualización posible.
- Se estima un volumen de eventos inicial (mínimo a soportar) de 1.500 eventos por segundo con un posible crecimiento de un 20% anual.
- Las alertas generadas por el motor SIEM serán revisadas en 24x7 por un técnico de seguridad de la empresa adjudicataria, como paso previo a su envío a los técnicos del Servicio de Informática del Ayuntamiento de Irun. Esto deberá permitir mayor nivel de acierto en la

hobeto asmatzea ahalbidetu beharko du horrek. Bildutako informazio guztia, sor daitezkeen alertak eta sistemaren osasun egoera orokorra, baita elementu bakoitzarena ere, kontsola zentralizatu baten bidez eskuratu ahal izango da, kudeaketa arina ahalbidetzeko.

eliminación de falsos positivos durante la identificación de incidentes. Toda la información recolectada, junto a las posibles alertas generadas, y el estado de salud global del sistema, así como el de cada uno de los elementos, deberá ser accesible mediante una consola central que permita una gestión ágil.

- Logak eta gertaeren transmisioa.

- Deskribatutako zerbitzu guztiak enpresa esleipendunaren azpiegituratik emango dira, eta SOC plataformari esleitu beharreko goi-mailako ENS eskakizuna betetzeko, tunel seguru bat egongo da bi sareen artean, informazio guztia zifratzeko baldintza egokietan bidaiatzeko. Horretarako, tunela ahalik eta segurtasun-maila handienarekin ezarri beharko da, protokoloei eta araudiari dagokienez.

- Transmisión de logs y eventos.

- Todos los servicios descritos serán prestados desde la infraestructura de la empresa adjudicataria y, para dar cumplimiento a la exigencia de ENS de nivel alto que se requiere a la plataforma SOC a adjudicar, existirá un túnel seguro entre ambas redes de forma que toda la información viaje en condiciones de cifrado adecuadas. Para ello se requerirá que el túnel sea establecido con los máximos niveles de seguridad en cuanto a protocolos y normativa.

- Udal Sarearen dimentsionamendua.

Erreferentzia gisa, ondorengo datuak ematen dira:

Zerbitzariak (fisikoak eta birtualak)	68
Lanpostuak	650
Logen gutxienezko erretentzioa	Urte 1
Ekitaldiak: Arrunta/pikoa/urteko hazk.	1.500 / 2.000 / %20

- Dimensionamiento de La Red Municipal.

Como referencia, se facilitan los siguientes datos:

Servidores (físicos y virtuales)	68
Puestos de trabajo	650
Retención mínima de logs	1 año
Eventos: Ordinario / pico / incr. Anual	1.500 / 2.000 / 20%

2.3.2.4. Urruneko monitorizazio zerbitzua. Gertakarien aurrean erantzuteko ekipoa.

- Urruneko CyberSOC zerbitzuaren ordutegia 24x7x365 erregimenean izango da erasoen patroioak aztertu, detektatu eta identifikatzeko ondorioetarako.
- Ondorengo prozedura jarraituz emango da zerbitzua:
 - a. Enpresa esleipendunak Irungo Udalaren esku jarriko ditu plataformaren funtzionamenduari eta gorabeheren tratamenduari buruzko eskaerak eta/edo kontsultak egiteko mekanismo arin eta seguruak (gutxienez posta-kontu orokor bat eta telefono bat).

- Servicio de monitorización remota. Equipo de respuesta ante incidentes.

- El horario del servicio de CyberSOC remoto será en régimen 24x7x365 a efectos de análisis, detección e identificación de patrones de ataque.
- El servicio se prestará siguiendo el siguiente procedimiento:
 - a. La empresa adjudicataria pondrá a disposición del Ayuntamiento de Irun mecanismos ágiles y seguros para realizar peticiones y/o consultas (como mínimo una cuenta de correo genérica y un teléfono) en relación con el funcionamiento de la plataforma y con el tratamiento de las incidencias.

- b. Enpresa esleipendunaren talde teknikoak hura kudeatzeko formatu/tresna egoki batean erregistratuko ditu gertaerak eta garatzen diren ekintza guztiak, Udalarentzat kostu gehigarririk gabe. Lehentasunezko eta presazko jakinarazpen-kanal bat egongo da garrantzi bereziko gertaeretarako.
 - c. Era berean, ekintza horien jarraipena egingo du gertaera kudeatu ahala, eta itxiera erregistratuko du Irungo Udalak ebazpena onartu eta itxi ondoren.
 - d. Antzemandako gertaerak Irungo Udalar jakinaraziko zaizkio, haiek arintzeko gomendioekin batera. Hortik abiatuta, erantzuteko dagokion jarduera zehaztuko da, enpresa esleipendunak eskaintako esku-hartze mailaren arabera, oinarrizkoa edo udalaren sistemen administrazio aurreratuagoa duena erabiliz, eta larritasuna kontuan hartuz eta Udaleko Sistemen Sekzioaren eta urruneko CyberSOC zerbitzua ematen duen enpresaren arteko protokolozko harreman dinamikaren arabera egingo da.
Aldez aurretik prozedura eginda eta Udalarekin adostuta dauden kasuetan, urruneko CyberSOC zerbitzuak prozedura horien arabera jardungo du, eta Udalar jarduera horren berri emango dio.
 - e. Aldizkako jarraipen-bilerak egingo dira (gutxienez hamabostean behin) zerbitzua kudeatzen duten enpresa esleipenduneko teknikarien eta Udal Informatika Zerbitzuko Sistemen Unitateko teknikarien artean.
 - b. El equipo técnico de la empresa adjudicataria registrará las incidencias y todas las acciones que se vayan desarrollando para su resolución en un formato/herramienta adecuado para su gestión, sin coste adicional para el Ayuntamiento. Existirá un canal de notificación prioritaria y urgente para aquellas incidencias de especial relevancia.
 - c. Asimismo, realizará un seguimiento de dichas acciones a medida que la incidencia se vaya gestionando y registrará el cierre una vez que el Ayuntamiento de Irun dé la aceptación de su resolución y cierre.
 - d. Las incidencias detectadas serán comunicadas al Ayuntamiento de Irun, junto con las recomendaciones de mitigación. A partir de ello, se determinará la actuación de respuesta correspondiente, en función del grado de intervención ofertado por la empresa adjudicataria, básica o con administración más avanzada de los sistemas del Ayuntamiento, y de acuerdo con la gravedad y con la dinámica de interrelación protocolizada entre la Unidad de Sistemas del Ayuntamiento y la empresa prestadora del servicio de CyberSOC remoto.
En los casos previamente procedimentados y consensuados con el Ayuntamiento, el servicio CyberSOC remoto actuará siguiendo dichos procedimientos y notificando al Ayuntamiento de dicha actuación.
 - e. Se realizarán reuniones de seguimiento periódicas (mínimo quincenalmente) entre los técnicos de la empresa adjudicataria que gestionen el servicio y los técnicos de la Unidad de Sistemas del Servicio de Informática Municipal.
- Enpresa esleipendunak Zerbitzu-mailari buruzko Akordio (ANS) baterako konpromisoa hartuko du eta, gutxienez, honako maila hauek izango ditu:
 - La empresa adjudicataria se comprometerá a un Acuerdo de Nivel de Servicio (ANS) que, como mínimo, tendrá los siguientes niveles:

<i>Zerbitzua / Servicio</i>	<i>Lehentasuna / Prioridad</i>	<i>Harrera denbora * (minutuak) / Tiempo de Recepción * (minutos)</i>	<i>Erantzuteko denbora (urrutiko euskarria) (minutuak) / Tiempo de Respuesta ** (Soporte en remoto) (minutos)</i>	<i>Konpontzeko denbora garbia *** / Tiempo neto resolución *** (orduak/horas)</i>
Euskarri zerbitzua / Servicio de soporte	Kritikoa / Crítica	10	30	4
	Handia / Alta	10	60	12
	Ertaina / Media	10	240	24
	Txikia / Baja	10	600	72

alegia,

- Harrera denbora = zerbitzua ematen duen enpresa esleipendunak gertaera jaso duela baieztatu arte igarotako denbora,
- Erantzuteko denbora = dagokion intzidentzia teknikari arduradun bati esleitu eta horretan lanean hasi arteko denbora.
- Konpontzeko denbora garbia = konpontzeko denbora guztira, bezeroaren erantzunaren itxaronaldia kenduta. Hori zenbatzen da erantzun-ekipoaren orduak kontsumitzen diren kasuan.

donde:

- Tiempo de recepción = tiempo transcurrido hasta la confirmación de la recepción de la incidencia por parte de la empresa adjudicataria, prestadora del servicio,
- Tiempo de respuesta = tiempo hasta que la incidencia es asignada a un técnico responsable y se empieza a trabajar en ella,
- Tiempo neto de resolución = tiempo total de resolución descontando el tiempo de espera de respuesta cliente. Esto se computa en caso de consumir horas del equipo de respuesta.

eta lehentasunak zehazten dira ondorengo taularen arabera:

Lehentasuna	Deskribapena
Kritikoa	Zerbitzu guztiak erabat geldituta aurkitzen direnean, sistemaren funtzionalitatea arriskuan eta funtsezko prozesuak gauzatu ezinik.
Altua	Arazo bat gertatzen denean hardware edo software zerbitzu edo azpiegituraren edozein elementu indibidualetan; soluzio partzial bat egon badago, baina funtsezko prozesuei eusteko gaitasuna degradatuta dago.
Ertaina	Modu indibidualean lokalizatu daitezkeen akatsak. Soluzio partzial bat dago, baina sistema mantentzeko gaitasuna zertxobait degradatu da.
Baxua	Funtzio edo konfigurazio partikularrei buruzko kontsultak. Dokumentazio edo informazio eskaerak.

y las prioridades se determinan de acuerdo con la siguiente tabla:

Prioridad	Descripción
Crítica	Cuando todos los servicios se ven afectados por un paro total, estando la funcionalidad del sistema comprometida y no pudiendo ejecutarse los procesos esenciales.
Alta	Cuando se produce un problema en cualquier elemento individual del servicio o infraestructura hardware o software, existiendo una solución parcial, pero la capacidad de mantener los procesos esenciales está degradada.
Media	Fallos que pueden ser localizados de manera individual. Existe una solución parcial, pero la capacidad de mantener el sistema se ha degradado ligeramente.
Baja	Consultas sobre las funciones o configuraciones particulares. Solicitudes de documentación o información.

- Monitorizazio zerbitzuak SOC erredundante bat eduki beharko du eta SOC nagusia eroriz gero soilik (Europar Batasunaren esparruan kokatuta egon beharko du) zerbitzuak bigarren mailakora edo mailakoetara konmutatuko lirakeke, era horretan zerbitzuaren maila berberak bermatuz.

- El servicio de monitorización deberá disponer de un SOC redundado, de tal manera que solo en caso de caída del SOC principal (que deberá residir en suelo de la Unión Europea) se conmuten los servicios al secundario o secundarios, garantizándose los mismos niveles de servicio.

2.3.4 Errekerimendu gehigarriak

- Horrez gain, ondorengo baldintza orokorren zerrenda ematen da, izaera orokorra dute, enpresa esleipendunak proiektua ezartzearekin eta kontratazio honetan sartutako zerbitzuak ematearekin zerikusia dutenak:

- Kontratazio honetan sartutako software eta hardware oro mantenimenduan eta bermatuta egongo da, zerbitzuak emateko

2.3.4. Requerimientos adicionales.

- Adicionalmente, se relacionan los siguientes requisitos adicionales, de carácter general, en relación con la empresa adjudicataria, y con la prestación de los servicios incluidos en esta contratación:

- Todo el software y el hardware que se incorpore a esta contratación por el adjudicatario estará en mantenimiento y

epealdiaren amaiera arte. Lizentziamendu osoak produktuen funtzionaltasun osoa ahalbidetzen duten lizentziak izango ditu, produktu horiek garatu ziren funtzioaren arabera, betiere proiektuaren indarraldian.

- Esleipendunak CSIRT.es sarearen partaide izan beharko du eta CERT bezala akreditatuta egon. Era berean, SOC Sare Nazionaleko partaide izango beharko du.
- Proiektu honek segurtasun alorrean daukan sentsibilitate berezia kontuan hartuta, enpresa esleipendunak ENS ziurtagiriaren maila altua ziurtatu beharko du.
- Udal Informazio Sistemaren zibersegurtasunaren arloko gertakarien log eta erregistroak enpresa esleipendunaren (edo enpresa azpikontratistaren, CyberSOC zerbitzuaren prestazioa azpikontratatzeko asmoa badute) sistemetan atxikiko direnez, lizitatuzaileek beren eskaintzan adierazi beharko dituzte segurtasun-baldintzak, titulartasuna eta datu horiek zainduko dituzten zerbitzariak zein herrialdetan dauden (nahitaez EBren barruan).
- SISTEMAREN ADMINISTRATZAILE-ENTZAKO PRESTAKUNTZA.
CyberSOC zerbitzua ematen hastean prestakuntza-saioak (gutxienez 2 jardunaldi) antolatuko zaizkie Udal Informatika Zerbitzuko Sistemen ataleko sistemako administratzaileei, SIEMen kudeaketaren arloan eta hedatutako tresna guztien erabileran dituzten ezagutzak indartzeko, baita kanpoko CyberSOC zerbitzuarekin koordinatzeko mekanika eta tresnetan ere.

garantía hasta el final del periodo de prestación de servicios. Todo el licenciamiento será con licencias que permitan una funcionalidad completa de los productos de acuerdo a la función para la que fueron desplegados, siempre durante el periodo de vigencia del proyecto.

- El adjudicatario deberá formar parte de la red CSIRT.es y estar acreditado como CERT. Asimismo deberá pertenecer a la Red Nacional de SOC.
- Dada la especial sensibilidad de este proyecto con respecto a la seguridad, la empresa adjudicataria deberá acreditar la certificación ENS a nivel alto.
- Dado que los log y registros de eventos en materia de ciberseguridad del Sistema de Información Municipal serán retenidos en los sistemas de la empresa adjudicataria (o de la empresa subcontratista, en el caso de que tengan previsto subcontratar la prestación del servicio de CyberSOC), los licitadores deberán indicar en su oferta, las condiciones de seguridad, la titularidad y el país (obligatoriamente dentro de la UE) en el que se sitúen los servidores que custodiarán estos datos.
- FORMACIÓN DESTINADA A ADMINISTRADORES DEL SISTEMA.
Al comienzo de la prestación del servicio de CyberSOC se organizarán sesiones (mínimo 2 jornadas) de formación a los administradores del sistema de la sección de Sistemas del Servicio de Informática Municipal para reforzar sus conocimientos en materia de gestión del SIEM, y en el manejo de todas las herramientas desplegadas, así como en las mecánicas e instrumentos de coordinación con el servicio de CyberSOC externo.

3. TALDE TEKNIKO KUDEATZAILEA

Erreferente gisa, Irungo Udalaren aldetik, honako hauek agertuko dira:

- Sareko administratzailea (ARDURADUNA),
- Udaleko Informatika Zerbitzuko burua,
- Sistemetako teknikaria,
- Sistemetako teknikari laguntzailea.

3. EQUIPO TÉCNICO GESTOR

Como referentes, por parte del Ayuntamiento de Irun, figurarán:

- el Administrador de Red (RESPONSABLE),
- el Jefe del Servicio de Informática Municipal,
- el Técnico de Sistemas,
- el Técnico Auxiliar de Sistemas.

Eta enpresak **zerbitzuaren koordinatzaile bat** izendatu beharko du **udalaren aurrean**, enpresa esleipendunaren funtsezko solaskide eta erreferente gisa. Gainera, kontratazio honetan parte hartzen duten enpresek profilak aurkeztu beharko dituzte (Informatika-sistemen administrazioko goi-mailako teknikariak, segurtasun-analistak), eta haien gaitasun-eta esperientzia-maila adierazi beharko dute. Profil horiek egonkor mantendu beharko dira kontratu osoan zehar, gutxienez egitura eta profil profesionaletan.

Udal Informatika Zerbitzuko Sistemen Unitateak kontrolatuko du adostutako baldintzak betetzen diren, bai eta espediente honen xede den zerbitzuaren kalitatea eta egokitasuna ere, emandako zerbitzuen baldintzak eta kalitatea osatzeari dagokionez.

Irunen, sinaduraren egunean.

SAREKO ADMINISTRATZAILEA
Eusebio Hernández-ek izpta.

y por parte de la empresa, ésta deberá designar un **Coordinador del Servicio ante el Ayuntamiento**, como interlocutor fundamental y referente de la empresa adjudicataria. Además, las empresas que concurren a esta contratación deberán presentar los perfiles (técnicos superiores en Administración de Sistemas Informáticos, analistas de seguridad), indicando su grado de capacitación y experiencia, que deberá mantenerse estable a lo largo de todo del contrato, al menos en estructura y perfiles profesionales.

La Unidad de Sistemas del Servicio de Informática Municipal controlará el cumplimiento de los términos acordados, así como la calidad y adecuación del servicio objeto de este expediente, en cuanto hace referencia a completar los términos y la calidad de los servicios facilitados.

Irun, a fecha de la firma.

EL ADMINISTRADOR DE RED
Fdo. Eusebio Hernández