DONOSTIA
SAN SEBASTIÁN
DonostiaTIK
Txomin Agirre, 6 | Tel. 010 - 943481800 |
20018 Donostia / San Sebastián

03/2025 Esp

Exp 03/2025

PRESKRIPZIO TEKNIKOEN AGIRIA, ZIBERSEGURTASUNEAN LAGUNTZEKO LAGUNTZA TEKNIKOKO ZERBITZUA ETA ENS, DBEO ETA NIS2 ARLOETAN INDARREAN DAGOEN ARAUDIA KONTRATATZEKO

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE ASISTENCIA TÉCNICA PARA EL APOYO EN CIBERSEGURIDAD y NORMATIVA VIGENTE EN MATERIA DEL ENS, RGPD Y NIS2

1.- KONTRATUAREN XEDEA

Baldintza agiri honen xedea da Zibersegurtasunaren arloan eta Informazioaren Segurtasunari buruzko araudia betetzeko laguntza teknikoko zerbitzua kontratatzea: DBLO, DBEO, ENS, NIS2 zuzentarau berria eta indarrean dauden gainerako araudiak, Donostiako Udalarentzat eta DonostiaTIKentzat.

1.- OBJETO DEL CONTRATO

El objeto del presente pliego de condiciones lo constituye la contratación del servicio de asistencia técnica para el apoyo en materia de Ciberseguridad y en cumplimiento normativo de Seguridad de la Información: LOPD, RGPD, ENS, la nueva directiva NIS2 y demás normativas en vigor, para el Ayuntamiento de Donostia/San Sebastian y DonostiaTIK.

2.- ABIABURUA

Donostiako Udala 17 sail edo arlok osatzen dute, eta, gainera, hiru erakunde autonomo eta zenbait sozietate publiko ditu.

Donostiatik Donostiako Udalaren tokiko erakunde autonomoa da, eta informatikako eta telekomunikazioetako zerbitzu teknologikoak eta ahots- eta datu-zerbitzuen beste edozein zerbitzu zuzenean eta modu deszentralizatuan garatzea du helburu, bai udal-erakundearentzat, bai herritarrentzat.

2016an, Donostiako Udaleko Informazioaren Segurtasunerako Batzordea eratu zen, informazioaren segurtasunaren arloan erabakiak hartzeko organo aholku-emaile eta estrategiko gisa. Besteak beste, datu pertsonalak babesteko arloan (DBLO/DBEO) eta Segurtasun Eskema Nazionalean (SEN) ezarritako betebeharrak betetzeko erabakiak hartzen lagunduko du.

2019ko urtarrilaren 8an egindako Tokiko Gobernu Batzarrak kide anitzeko organoa sortu zuen, Udalean Datuak Babesteko Ordezkariaren eginkizunak bere gain hartzeko.

2.- SITUACIÓN DE PARTIDA

El Ayuntamiento de Donostia-San Sebastian está formado por 17 Departamentos o Áreas, además cuenta con tres Organismos Autónomos y varias Sociedades Públicas.

Donostiatik es un Organismo Autónomo Local del Ayuntamiento de Donostia-San Sebastian cuyo objetivo es desarrollar de forma directa y descentralizada los servicios tecnológicos de informática, de telecomunicaciones, y cualquier otro servicio de voz y datos, tanto a la organización municipal para la prestación de sus servicios, como a la propia ciudadanía.

En 2016 se constituyó el Comité de Seguridad de la Información del Ayuntamiento de Donostia-San Sebastian como órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Entre otras atribuciones, dará soporte en la toma de decisiones para dar cumplimiento en materia de protección de Datos Personales (LOPD/RGPD) y a las obligaciones establecidas en el Esquema Nacional de Seguridad (ENS).

La Junta de Gobierno Local celebrada el 8 de enero de 2019 procedió a la creación del órgano colegiado que asume en el Ayuntamiento las

Bestalde, 2019an, DonostiaTIKek, Udalaren, erakundeen eta sozietate publikoen zerbitzu teknologikoen hornitzaile gisa, Informazioaren Segurtasunerako Batzordea eratu zuen, eta haren segurtasun-politika onartu zuen, betiere Udaleko Informazioaren Segurtasunerako Batzordearen jarraibideak kontuan hartuta.

2019. urtearen amaieran, kategoria ertaineko SEN xedapenekiko adostasun-ziurtagiria lortu zuten, bai DONOSTIAKO UDALAK, honako hauekin:

"Donostiako Udalaren jabetzako informazio-sistemak, DonostiaTIK zerbitzuaren bidez kudeatzen diren Administrazio Elektronikoko zerbitzuei euskarria ematen dietenak, indarrean dagoen Aplikagarritasun Adierazpenaren arabera".

Donostiatik bezala, honako irismen honekin:

"DonostiaTIK sozietateak kudeatzen dituen informazio-sistemak, Donostiako Udalaren Administrazio Elektronikoa eta udal-kudeaketa, posta elektronikoa eta erabiltzaileei, udal-enpresei eta erakunde autonomoei ematen zaien laguntza biltzen dituztenak, indarrean dagoen Aplikagarritasun Adierazpenaren arabera".

funciones del Delegado/a de Protección de Datos.

Por otra parte, en 2019, DonostiaTIK como proveedor de servicios tecnológicos del Ayuntamiento, Organismos y Sociedades Públicas, constituyó su Comité de Seguridad de la Información y aprobó su Política de Seguridad, siempre contemplando las directrices del Comité de Seguridad de la Información del Ayuntamiento.

A finales del año 2019 obtienen y actualmente mantienen, la certificación de conformidad respecto a las disposiciones ENS en categoría MEDIA, tanto el AYUNTAMIENTO DE DONOSTIA-SAN SEBASTIAN con el alcance de:

“Los sistemas de información propiedad del Ayuntamiento de Donostia/San Sebastian, que dan soporte a los servicios de Administración Electrónica gestionados a través de DonostiaTIK, de acuerdo a la Declaración de Aplicabilidad vigente”.

Como DonostiaTIK, con el siguiente alcance:

“Los sistemas de información gestionados por DonostiaTIK que albergan las aplicaciones de Administración Electrónica y gestión municipal, correo electrónico y la asistencia a usuarios del Ayuntamiento de Donostia/San Sebastian, empresas municipales y organismos autónomos, de acuerdo a la Declaración de Aplicabilidad vigente”.

3.- EGIN BEHARREKO ZERBITZUEN DEFINIZIOA

Baldintza-agiri honen xedea da Segurtasun Eskema Nazionala (SEN) arautzen duen 311/2022 Errege Dekretua, maiatzaren 3koa, Datuak Babesteko Erregelamendu Orokorra (DBEO 679/2016), Datuak Babesteko Lege Organikoa (DBLO 3/2018), eta NIS 2 zuzentaraua eta gainerako arau-esparrua betetzen laguntzeko laguntza teknikoko zerbitzuak kontratatzea, bai eta Donostiako Udalean eta haren erakudeen informazioaren segurtasuna kudeatzeko beharrezko segurtasun-neurriak ezartzen laguntzeko laguntza teknikoa kontratatzea ere.

Informazioaren segurtasunaren ikuspegi

3.- DEFINICIÓN DE LOS SERVICIOS A REALIZAR

El objeto del presente pliego de condiciones lo constituye la contratación de los servicios de asistencia técnica de apoyo para el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (ENS), del Reglamento General de Protección de Datos (RGPD 679/2016), de la Ley Orgánica de Protección de Datos (LOPD 3/2018), de la nueva directiva NIS2 y demás marco normativo, así como la asistencia técnica para facilitar la implementación de las medidas de ciberseguridad necesarias para la gestión de la Seguridad de la Información en el Ayuntamiento de Donostia/San Sebastian y DonostiaTIK.

Se requiere de una asistencia técnica con visión

orokorra duen laguntza teknikoa behar da, segurtasuna hobekuntza-ziklotzat hartuta, segurtasun-prozesu, -prozedura eta/edo -instrukzio teknikoak etengabe berrikusiz eta hobetuz. Horiek guztiak garatu eta hobetu behar dira denboran zehar, administrazio elektronikoko zerbitzuen aurrerapenarekin, zerbitzu horiek babesten dituzten azpiegiturekin, bilakaera teknologikoarekin eta ziberespazioan jarduteak dakartzan arriskuekin batera.

Pleguan jasotako lanen ezaugarriak kontuan hartuta, bi urtean egiteko kalkulatu eta planifikatu beharko dira, hurrengo birertifikazioaren data kontuan hartuta, eta SENa Segurtasuna hobetzeko ardatz gisa hartuta.

Egin beharreko zerbitzuek honako puntu hauek izan beharko dituzte:

3.1Adostasuna lortzeko zerbitzuak

1) SEN ezartzeko eta betetzen dela gainbegiratzeko prozesuetan laguntza globala ematea. Donostiako Udalaren eta DonostiaTIKen ENS ziurtagiriaren irismena zabaltzea. Hurrengo birzertifikaziorako prestatzea.

2) Arriskuak aztertzeko ziklo berri bat egitea, datuen babesaren eta SENen ikuspegitik.

3) DBEO/DBLO/DBLO betetzeko lanetan aholkularitza ematea, eta, bereziki, eraginaren ebaluazioari eta DBEOren 35. artikuluarekin bat etortzeari dagokienez, bai eta Datuak Babesteko Euskal Bulegoak edo Estatuko Bulegoak egindako jarduketen eta ikuskapenen aurrean ere.

4) Segurtasuna hobetzeko plana ezartzen laguntzea, bai Udalaren planari, bai DonostiaTIK planari, bai egungoari, bai sortzen ari direnei.

5) Kontratazioaren arloan sartu beharreko informazioaren pribatutasunari eta segurtasunari buruzko klausulei buruzko aholkularitza, bai DonostiaTIKen kontratuetarako, bai Udalaren kontratuetarako.

6) Zibersegurtasunaren arloko barne esparru arauemailearen garapenean laguntza ematea: politikak, protokoloak, jarraibide teknikoak, jardunbide egokiak eta abar sortzea, eguneratzea eta hobetzea.

global de la Seguridad de la Información tomando la Seguridad como un proceso de ciclo de mejora, mediante la revisión y mejora continua de los procesos, procedimientos y/o instrucciones técnicas de seguridad, que se deben desarrollar y perfeccionar a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

Dadas las características de los trabajos incluidos en el pliego, se deberán estimar y planificar para su realización en **dos** años, teniendo en cuenta la fecha de la próxima recertificación, y tomando el ENS como eje de la mejora de la Seguridad.

Los servicios a realizar deberán incluir los puntos siguientes:

3.1 Servicios relativos a conseguir la conformidad normativa

1) Prestación de soporte global en los procesos de implantación y supervisión del cumplimiento ENS. Ampliación del alcance de la certificación ENS del Ayuntamiento de Donostia-San Sebastian y de DonostiaTIK. Preparación para la próxima recertificación.

2) Elaboración de un nuevo ciclo de análisis de riesgos desde la perspectiva de protección de Datos y ENS.

3) Asesoramiento en labores de cumplimiento RGPD/LOPD-GDD y específicamente en lo relativo a la evaluación de impacto y su conformidad con el artículo 35 del RGPD., así como ante actuaciones e inspecciones llevadas a cabo por la Agencia Vasca o Estatal de Protección de Datos.

4) Soporte en la implantación del plan de mejora de la Seguridad tanto al plan del Ayuntamiento como al de DonostiaTIK y tanto actual como los que vayan surgiendo.

5) Asesoría sobre las cláusulas referidas a la privacidad y a la seguridad de la información a incluir en materia de contratación tanto para los contratos de DonostiaTIK como para contratos del Ayuntamiento.

6) Dar soporte en el desarrollo del marco normativo interno en materia de Ciberseguridad: Creación, actualización y mejora de Políticas, Protocolos,

7) SENen barne auditoretza, urteko aldizkakotasunarekin.

3.2 DonostiaTIK Zibersegurtasuneko bulego teknikoaren laguntza zerbitzuak

1) Web aplikazioetan 2 pentesting ariketa egitea. Gainera, sortutako txostenetan, antzemandako ahultasunen deskribapena ez ezik, horiek konpontzeko proposamen egingarri eta zehatzak ere sartzeko eskatzen dizuegu.

2) Kontingentzia eta ziberkrisi planean hobekuntzak egitea, egungo araudien arabera.

3) DonostiaTIKi aholkularitza ematea aplikazioen garapenean eta kodetze seguruko praktiken inplementazioan kontuan hartu beharreko segurtasun alderdiei buruz. Era berean, egungo garapen-metodologia optimizatzera bideratutako hobekuntzak proposatzea eskatzen dizuegu. Esleipendunak DonostiaTIKeko kontratuaren arduradunarekin izango du harremana.

4) Datu pertsonalen tratamenduetan pribatutasunerako hartu behar diren neurri teknikoak aztertzea, berrikustea eta proposatzea.

5) CCNren tresnak hedatzen laguntzea.

6) DonostiaTIKek hala eskatzen duenean, zibersegurtasun arloko tresnak ezartzea aztertzea eta proposatzea.

7) Zibersegurtasuneko adierazleak modu automatizatuan kudeatzea, neurtzea eta gainbegiratzea ahalbidetuko duten tresnak aztertzea.

3.3 Zibersegurtasun Eragiketen Zentroaren Zerbitzua (SOC):

3.3.1 Baldintza orokorrak

Monitorizazio zerbitzuak behar dira zaintza digitalerako, zibersegurtasun ekitaldien alerta

instrucciones técnicas, buenas prácticas etc.

7) Auditorías internas ENS con perioricidad anual.

3.2 Servicios de soporte a la oficina técnica de Ciberseguridad de DonostiaTIK.

1) Realizar 2 ejercicios de pentesting en aplicaciones web. Se requiere, además, que los informes generados incluyan no solo la descripción de las vulnerabilidades detectadas, sino también propuestas factibles y concretas para su remediación.

2) Elaborar mejoras en el plan de contingencias y cibercrisis de acuerdo con normativas actuales.

3) Asesoramiento a DonostiaTIK en los aspectos de seguridad que deben considerarse durante el desarrollo de aplicaciones y en la implementación de prácticas de codificación segura. Asimismo, se requiere la propuesta de mejoras orientadas a optimizar la metodología de desarrollo actual. La empresa adjudicataria estará en contacto con el responsable del contrato de DonostiaTIK.

4) Análisis, revisión y propuesta de las medidas técnicas que se deben adoptar para la privacidad en los tratamientos de los datos personales.

5) Dar soporte al despliegue de herramientas del CCN.

6) Analizar y proponer, cuando DonostiaTIK lo solicite, la implantación de herramientas en materia de Ciberseguridad.

7) Analizar herramientas que permitan gestionar, medir y supervisar indicadores de ciberseguridad de forma automatizada.

3.3 Servicio de Centro de Operaciones de Ciberseguridad (SOC):

3.3.1 Requisitos generales

Se requiere de servicios de monitorización para la

goiztiarra.

Esleipendunak atal honetan segurtasun-gorabeherak detektatzeko eta prebenitzeko jasotzen diren konponbideen mantentze-lanak eta euskarria egingo ditu, kontratuak irauten duen bitartean funtzionatzeko beharrezkoak diren ekipamendu eta lizentzia guztiak barne.

Monitorizazio soluzioa erabilgarritasun handian hedatu beharko da, Cloud formatuan, eta, gutxienez, irismenari eta funtzionaltasunari dagokienez, gaur egun Udalarentzat eta DonostiaTIKentzat dauden KSA zerbitzuak jasoko ditu, bere azpiegituren, komunikazioen eta zerbitzu digitalen segurtasuna bermatzeko, zibersegurtasuneko gertakarien aurrean prebenitzeko, detektatzeko eta erantzuteko gaitasunak hobetuz.

I. eranskinean xehatuta dago egungo soluzioa.

Aurreikusitako konponbideek honako baldintza orokor hauek bete beharko dituzte:

- Erabilitako edozein protokolo eta aplikaziotan intrusioak detektatzea eta prebenitzea.
- Aplikazioen eta zerbitzuen errendimenduaren degradazioan eraginik ez izatea.
- Sortutako informazioa udal segurtasun sistemetan integratzea, bai eta Zibersegurtasun Eragiketen Zentroak monitorizatu beharreko iturriak ere.
- Erakundearen ekitaldiak denbora errealean monitorizatzea 24x7.
- Gertakariak goiz detektatzea eta horiei erantzutea, protokoloak lantzearekin batera.
- *Honeypot*ak izatea sarearen eta erabiltzaileen mailan.
- *Threat Hunting* zerbitzuak ematea gainbegiratutako gertaerei buruz.
- Sinaduretan, portaeretan, logetan, prozesuetan eta IOCetan oinarritutako gertaerak aztertzea.
- Anomaliak detektatzeko AA teknikak izatea.
- Erakundearen berezitasunera egokitutako alerta arauak definitzeko

vigilancia digital, alerta temprana de eventos de ciberseguridad.

El adjudicatario llevará a cabo el mantenimiento y soporte de las soluciones que se incluyen en el presente apartado para la detección y prevención de incidentes de seguridad, incluyendo todo el equipamiento y licencias que sean necesarias para su funcionamiento durante la duración del contrato.

La solución de monitorización se deberá desplegar en alta disponibilidad en formato Cloud e incluirá, al menos, tanto en alcance como en funcionalidad, los servicios de SOC existentes en la actualidad para el Ayuntamiento y DonostiaTIK, a fin de garantizar la seguridad de sus infraestructuras, comunicaciones y servicios digitales, mejorando sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

En Anexo I se encuentra detallada la solución actual.

Las soluciones contempladas deberán cumplir los siguientes requisitos generales:

- Detectar y prevenir intrusiones en cualquier protocolo y aplicación utilizados.
- No repercutir en una degradación del rendimiento de las aplicaciones y servicios.
- Integrar tanto la información generada en los sistemas de seguridad municipales como fuentes a monitorizar por parte del Centro de Operaciones de Ciberseguridad.
- Monitorizar en tiempo real los eventos de la organización 24x7.
- Detección temprana y respuesta ante incidentes, junto con la elaboración protocolos.
- Disponer de *Honeypots* a nivel de red y de usuarios.
- Proporcionar servicios de *Threat Hunting* sobre los eventos supervisados.
- Analizar de eventos basado en firmas, comportamientos, logs, procesos e IOCs.
- Disponer de técnicas de IA para la detección de anomalías.
- Posibilidad de definir reglas de alerta adaptadas a la particularidad de la organización.

aukera.

- Iturri anitzeko gertaerak zentralizatzea, babestea eta korrelatzea.
- Sare-mailako intrusioak detektatzeko sistema izatea.
- Kanpoko zerbitzuak integratzea syslog/api bidez.
- Jakinarazitako gertakarien aurrean euskarri aditua kontuan hartzea.
- Hileroko egoera-txostenak eta -bilerak sortzea, adierazleekin eta haien jarraipenarekin.

Eragiketa Zentroak laguntza-zerbitzu bat eman eta kudeatu beharko du sortutako alerten aurrean. Esleipendunak erakundearen aktiboetan gerta daitezkeen segurtasun eraso edo gorabeherak geldiarazteko edo arintzeko beharrezkoak diren ekintzetan euskarria emango du.

SOC-ak sortutako alerta guztiak aztertu beharko ditu, positibo faltsuak baztertuz, diagnostikoa lehenbailehen transmitituz eta gomendioak modu proaktiboan emanez, erasoa blokeatu ahal izateko, aktiboen edo horiek jasaten dituzten azpiegituren segurtasuna arriskuan jartzen bada.

SOC-aren ustiapenaz arduratzen den enpresak CSIRTesen eta SOC-ren Sare Nazionalaren parte izan beharko du, GOLD kategorian. Informazio hori CCNrekin kontrastatuko da.

Trazabilitate-erregistroak (SIEM) biltzeko eta korrelatzeko gaitasuna, SOC-ak zaintzeko behar duena, CCN-STIC 105 (CPSTIC) katalogoan jasotako produktuen/zerbitzuen bidez egin beharko da. Informazio hori Zentro Kriptologiko Nazionaleko ziurtapen-organismoarekin egiaztatuko da.

Monitorizazio zerbitzua Europan dagoen DataCenter batek eman beharko du, eta Uptime Institutuak gutxienez TIER III ziurtagiria eman beharko dio. Datacenterrak gutxienez segurtasun-ziurtagiri hauek izango ditu: 27001, 27017, 22301 eta ENS kategoria ALTUAN.

3.3.2 SOC-aren zeregin nagusien laburpena

Gorabeheren kudeaketari dagokionez, SOC-ak honako hauek egin beharko ditu:

- Centralizar, salvaguardar y correlacionar eventos multifuente.
- Disponer de Sistema de detección de intrusiones a nivel de red.
- Integración de servicios externos vía syslog/api.
- Contemplar soporte experto ante los incidentes notificados.
- Generar informes y reuniones mensuales de estado con los indicadores y su seguimiento.

Desde el Centro de Operaciones se deberá proveer y gestionar un servicio de soporte ante las alertas generadas. El adjudicatario proporcionará soporte en acciones necesarias para la contención o mitigación de los posibles ataques o incidencias de seguridad en los activos de la entidad.

El SOC deberá analizar todas las alertas generadas, descartando falsos positivos, transmitiendo el diagnóstico cuanto antes y aportando recomendaciones de forma proactiva que permita el bloqueo del ataque en caso de que se ponga en riesgo la seguridad de los activos o las infraestructuras que los soportan.

La empresa encargada de la explotación del SOC deberá formar parte de CSIRT.es y de la Red Nacional de SOC, en categoría GOLD. Esta información será contrastada con el CCN.

La capacidad de recolección y correlación de los registros de trazabilidad (SIEM) necesarios para la vigilancia por parte del SOC deberá realizarse mediante productos/servicios recogidos en el catálogo CCN-STIC 105 (CPSTIC). Esta información será contrastada con el organismo de certificación del Centro Criptológico Nacional.

El servicio de monitorización deberá ser prestado desde un DataCenter ubicado en Europa, certificado al menos en TIER III por el Uptime Institute. El Datacenter contará con al menos las siguientes certificaciones de seguridad: 27001, 27017, 22301 y ENS en Categoría ALTA.

3.3.2 Resumen de las principales tareas del SOC

En cuanto a la gestión de incidencias, el SOC deberá:

- Informazioa iturri kopuru handi batetik jasotzea, bere funtzioak betetzeko beharrezkoak diren guztiak barne, eta jasotako datuak korrelazioan jartzea.

- Informazio-iturri desberdinetako segurtasun-gertaerak biltzea, jatorrizko sistemetan eragin txikiena duten mekanismoen bidez (ahal den guztietan agenteak instalatu beharrik gabe).

- Gailuen, sistemen, aplikazioen eta zerbitzuen egoerari buruzko segurtasun-informazioa monitorizatzea eta denbora errealean kontsultatzea.

- Bildutako gertaerak denbora errealean prozesatzea eta korrelazioan jartzea, eraso baten adierazle izan daitezkeen gertaerak detektatzeko eta alerta egokiak igortzeko.

- Bildutako gertaerak beste informazio-iturri batzuekin korrelazioan jartzea, hala nola ospearen datu-baseekin eta beste ingurune eta sistema batzuetan antzemandako erasoen informazioarekin.

- Erabilgarritasun handia eta berreskuratzeko mekanismoak izatea, osagai nagusietan izan daitezkeen akatsen aurrean zerbitzua emango dela bermatzeko.

- Monitorizazio-prozesuak sortutako alertak sailkatzea eta lehenestea.

- Atzemandako erasoak geldiarazteko edo neutralizatzeko euskarria ematea, automatikoki eusteko tresnen edo eskuz eusteko prozeduren bidez.

- Eskalatzeko eta erabakiak hartzeko prozesuan parte hartzen duten erakundeko solaskideei jakinaraztea, ezarritako kanalen bidez.

- Zibergertakarien Jakinarazpen eta Jarraipenerako Plataforma Nazionalarekin zibergertakariak arin trukatzeko laguntza, CCN-CERTen LUCIA gertakariak kudeatzeko tresnarekin.

- Bildutako gertaerak denbora-tarte zabal batean biltegiratzea eta zaintzea, gutxienez urtebeteko iraupenarekin, behar izanez gero, auzitegiko azterketa bat egiteko eta segurtasun gorabeheren

- Recibir información desde un elevado número de fuentes, incluyendo todas aquellas que sean precisas para cumplir con sus funciones, y correlacionar los datos recogidos.

- Recolectar los eventos de seguridad de diferentes fuentes de información mediante los mecanismos que menos impacten en los sistemas origen (sin necesidad de instalar agentes siempre que sea posible).

- Monitorizar y consultar en tiempo real información de seguridad sobre el estado de los dispositivos, sistemas, aplicaciones y servicios.

- Procesar y correlacionar los eventos recolectados en tiempo real para detectar sucesos que puedan ser indicativos de un ataque y emitir las alertas oportunas.

- Correlacionar los eventos recolectados con otras fuentes de información, tales como bases de datos reputacionales e información de ataques detectados en otros entornos y sistemas.

- Disponer de alta disponibilidad y mecanismos de recuperación que garanticen la prestación del servicio ante potenciales fallos en los principales componentes.

- Clasificar y priorizar las alertas generadas por el proceso de monitorización.

- Dar soporte para contener o neutralizar los ataques detectados a través de herramientas de contención automática o de procedimientos de contención manual.

- Notificar mediante los canales establecidos a los interlocutores de la entidad que formen parte del proceso de escalado y toma de decisiones.

- Soporte al Intercambio fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de ciberincidentes con la herramienta de gestión de incidentes LUCIA del CCN-CERT

- Almacenar y custodiar los eventos recolectados durante un amplio rango de tiempo, con una duración mínima de 1 año para, en caso de necesidad, realizar un análisis forense y obtener datos relativos al origen, destino y traza de los incidentes

jatorriari, helmugari eta trazari buruzko datuak lortzeko.

- Marka eta irudi korporatiboari buruzko Interneteko informazio guztia 24x7 monitorizatzea ahalbidetuko duen Zaintza Digitaleko zerbitzu bat sartzea, babestu beharreko aktiboen edo markaren ospearen gaineko edozein arrisku edo mehatxu aztertzeko, eragin ditzaketen gorabehera edo kalteei aurrea hartzeko. Soluzioak informazioaren segurtasunari, aplikatu beharreko araudiei edo legezko printzipioei eta konfiantza digitalari buruzko alderdiak bete beharko ditu.

3.3.3 SIEM soluzioa

Aipatutako eginkizunak betetzeko, esleipendunak SOC-aren eragiketa ahalbidetuko duen SIEM soluzioa kudeatuko du, agiri honetan eskatutako baldintzetan. SIEM soluzioaren lizentziamendu eta hedapen kostuak barne hartuko ditu, lizentzien eredua eta agiri honetan jasotako baldintzak betetzeko hobekien egokitzen den soluzio mota kontuan hartuta. SIEM soluzio horrek baldintza hauek bete behar ditu:

- Monitorizazio soluzioa erabilgarritasun handian hedatu beharko da, Cloud formatuan.

- Sarean gertatzen diren segurtasun-gertaera guztiak modu zentralizatuan atzemateko eta biltzeko gai izatea, informazioa iturri askotatik jasotzea, bildutako datuak korrelazioan jartzea eta informazio mota ugari paneletan erakustea.

- Segurtasun adierazleak kudeatzeko eta egiteko panelak zabaltzeko gai izatea, panel propioak proposatuz eta DonostiaTIKek eskatuta beste batzuk garatuz, erakundearen segurtasun egoeraren jarraipena egiteko kontsultatu nahi den informazioan oinarrituta.

- Gertaerak korrelaziorako atxikitzeko gaitasuna. Ekitaldiak 12 hilabetez biltegiratuko dira, eta horietatik gutxienez 2 hilabete beroan egin beharko dira. Horrela, KSAk, bere SIEMen eta lotutako gainerako tresnen bidez, beharrezkoak diren iturri guztiak integratu eta monitorizatu beharko ditu, erakundearen testuingurura egokitutako prebentzio-, detekzio- eta erantzun-zerbitzu optimoa emateko. Kontratuaren

de seguridad.

- Incluir un servicio de Vigilancia Digital que permita la monitorización 24x7 de toda la información en Internet relativa a la marca e imagen corporativa, con el objeto de analizar cualquier riesgo o amenaza sobre los activos a proteger o la reputación de la marca, para anticiparse a las incidencias o perjuicios que puedan ocasionar. La solución deberá cubrir aspectos relativos a la seguridad de la información, a las normativas o principios legales de aplicación, y los relativos a la confianza digital.

3.3.3 Solución SIEM

Para realizar las funciones referidas, el adjudicatario gestionará la solución SIEM que permita la operación del SOC en los términos exigidos en el presente pliego. Incluirá los costes de licenciamiento y despliegue de la solución SIEM, atendiendo al modelo de licencias y tipo de solución que mejor se adapte al cumplimiento de los requisitos recogidos en el presente pliego. Dicha solución SIEM debe cumplir los siguientes requisitos:

- La solución de monitorización se deberá desplegar en alta disponibilidad en formato Cloud.

- Ser capaz de capturar y recopilar todos los eventos de seguridad que se producen en la red de forma centralizada, de recibir información desde una gran cantidad de fuentes, de correlacionar los datos recogidos y de mostrar una amplia variedad de información en paneles.

- Ser capaz de ampliar paneles de gestión y elaboración de indicadores de seguridad, proponiendo paneles propios y desarrollando otros bajo demanda de DonostiaTIK en base a la información que se desee poder consultar para hacer seguimiento del estado de seguridad de la organización.

- Capacidad de retención de eventos para su correlación. Se almacenarán eventos durante 12 meses, de los cuales, al menos 2 meses deberán realizarse en caliente. Así, el SOC, a través de su SIEM y resto de herramientas asociadas, deberá integrar y monitorizar todas aquellas fuentes que resulten necesarias para proporcionar un servicio de prevención,

hasieratik integratu beharreko iturriei dagokienez, I. eranskinean zehaztuta daude, eta ezartzeko, pixkanakako ikuspegiari jarraituko zaio.

- SIEM soluzioak gutxienez 5.000 EPS gehitzeko aukera eman beharko du.
- Proposatutako SIEM soluzioari esker, gutxienez 40 iturri mota hartu ahal izango dira.
- SIEM soluzioak direktorio aktiboaren monitorizazio aurreratuko modulu bat izan beharko du, sistema horien gainean izan daitezkeen erasoak identifikatzeko, Mitrerekin eta horrelako erasoetan komunean erabiltzen diren TTP ezagunekin lerrokatuta.
- Proposatutako SIEM soluzioak 6500 arau baino gehiago izango ditu, eta gutxienez 500 arauk aldi berean funtzionatzea ahalbidetu beharko du.
- NIDS zerbitzua, gutxienez 3500 gailutarako.
- Era berean, kontratuan zehar, KSAk, aldez aurretik aldatuta, iturri berriak gehitu ahal izango ditu pixkanaka, Zibersegurtasuneko Bulego Teknikoak egin ditzakeen gomendioei eta/edo erakundeak eskuratzen dituen zibersegurtasuneko soluzio berriei jarraituz.
- Gertaeren analisiaren funtzionaltasunerako, produktuak bildutako datuak zehaztutako arauen arabera aztertzeko gai izan beharko du, erabilera bidegabeak edo jarduera maltzurrak identifikatzeko, eta analisien emaitza erregistratu beharko du.
- Produktuak ez du kredentzial argirik biltegiratuko memoria ez-lurrunkorrean.
- Gertaeren analisiaren eta korrelazioaren funtzionaltasunerako, produktuak biltegiratutako gertaerak baimendu gabeko sarbideetatik, aldaketetatik eta ezabatzeetatik babestu behar ditu, bai eta biltegiratze espazioa betetzeagatik gertaerak galtzea prebenitu ere.

3.3.4 Segurtasun-kopiak

Proposatutako soluzioak hartutako logen multzo osoaren eguneroko babeskopia bat izan

detección y respuesta óptimo y adaptado al contexto de la entidad. En cuanto a las fuentes a integrar desde el inicio del contrato, están especificadas en el Anexo I y para su implantación se seguirá un enfoque gradual.

- La solución SIEM deberá permitir agregar al menos 5.000 EPS
- La solución SIEM propuesta permitirá la ingesta al menos 40 tipos fuentes diferentes.
- La solución SIEM deberá tener un módulo de monitorización avanzada del directorio activo, con el objetivo de identificar posibles ataques sobre estos sistemas, alineados con Mitre y con las TTPs conocidas utilizadas comunmente en este tipo de ataques.
- La solución SIEM propuesta dispondrá de más de 6500 reglas y deberá permitir que al menos 500 reglas funcionen de forma simultánea.
- Servicio NIDS para al menos 3500 dispositivos.
- Asimismo, a lo largo del contrato el SOC, previo modificado, podrá incorporar progresivamente nuevas fuentes, atendiendo a su vez a las recomendaciones que pueda realizar la Oficina Técnica de CiberSeguridad y/o a las nuevas soluciones de ciberseguridad que adquiera la entidad.
- Para la funcionalidad de análisis de eventos, el producto deberá ser capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos o actividades maliciosas, registrando el resultado de los análisis.
- El producto no almacenará ninguna credencial en claro en memoria no volátil.
- Para la funcionalidad de análisis de eventos y correlación, el producto debe proteger los eventos almacenados de accesos, modificaciones y borrados no autorizados, así como prevenir la pérdida de eventos por el llenado del espacio de almacenamiento.

3.3.4 Copias de Seguridad

La solución propuesta deberá contar con una copia de seguridad diario del conjunto total de logs

beharko du, eskuragarri daudela ziurtatzeko eta erregistroak galtzea ekar dezaketen kontingentziak estaltzeko. Backup hori lizitatzaileak emandako kanpoko kokapen batean hartu beharko da, SIEMen tresnaren kokapenaz bestelakoa, eta kokapen horren segurtasuna egiaztatu beharko da. Babeskopiek aukera eman beharko dute logak osorik berreskuratzeko, urtebeteko atxikipen-epearekin, eta gutxienez azken 2 hilabeteetako korrelazioa beroan egin beharko da.

I. eranskina hala eskatzen duten enpresen eskura dago, eskatzailearen datuak erregistratu ondoren, eskatutako konfidentzialtasuna egiaztatzeko. Horretarako, honako hauen bidez jarri beharko dira harremanetan:

donostiatik_kontratazioa@donostia.eus

ingestados para asegurar su disponibilidad y cubrir posibles contingencias que pudieran suponer una pérdida de los registros. Dicho backup deberá ser alojado en una ubicación externa proporcionada por el licitador, diferente a la ubicación de la propia herramienta de SIEM, acreditando la seguridad de dicha ubicación. Las copias de seguridad deberán permitir una recuperación completa de los logs con un plazo de retención de 1 año y al menos la correlación de los 2 últimos meses deberá realizarse en caliente.

El anexo I se encuentra a disposición de las empresas que así lo soliciten previo registro de los datos del solicitante a efectos de acreditar la confidencialidad requerida. Para ello tendrán que ponerse en contacto a través de:

donostiatik_kontratazioa@donostia.eus

4.- INFORMAZIOA ETA DOKUMENTAZIOA ESKUALDATZEA

Esleipendunaren lantalderako proposatutako osaerak gutxienez lau pertsona izan beharko ditu honako eginkizun hauek bere gain har ditzaten:

- Taldearen zuzendaritza/koordinazioa
- Aholkularitza tekniko-antolamenduko-informatikoa SENen eta DBEOren arloan.
- Aholkularitza tekniko-informatikoa IKT segurtasunaren eta zibersegurtasunaren arloan.
- SOC taldea 24x7

Kontratuaren arduradunarekin koordinazio-lanak egingo dituen figura bat proposatu behar dute. Koordinazio-lanak honako hauek izango dira: Kontratuaren arduradunaren jarraibide orokorrak jasotzea, proiektuen gauzatzea koordinatzea, proiektuen kalitate-maila egiaztatzea, proiektuen erantzukizuna hartzea eta egin beharreko lanen plangintza, jarraipena eta kontrola egitea.

Gainera, enpresa esleipendunak orientazio juridikoa duen diziplina anitzeko talde bat izan beharko du, SEN, DBEO, IKT segurtasun eta zibersegurtasunaren arloan antolatzailea.

Diziplina anitzeko talde hori zerbitzua modu eraginkorrean emateko gaitasunak eta indargune indibidualak konbinatzeko moduan proposatu beharko da, eta lanen helburu nagusia zeregin teknikoak, antolamendukoak

4.- CARACTERÍSTICAS Y EQUIPO PARA LA PRESTACIÓN DEL SERVICIO A CONTRATAR

La composición propuesta para el equipo de trabajo del adjudicatario deberá contar mínimamente con 4 personas de los siguientes perfiles:

- Dirección de equipo/Coordinación
- Asesoramiento técnico-organizativo-informático en materia de ENS y RGPD.
- Asesoramiento técnico-informático en materia de Seguridad TIC y Ciberseguridad.
- Equipo del SOC en 24x7

Deben proponer una figura que realice labores de coordinación con el responsable del contrato. Las labores de coordinación consistirán en recibir instrucciones generales por parte del responsable, coordinar la realización de los proyectos, verificar su nivel de calidad, asumir la responsabilidad de los proyectos y se encargará de la planificación, seguimiento y control de los trabajos a realizar.

Además, la empresa adjudicataria deberá contar con un equipo multidisciplinar con orientación jurídica, organizativa en materia de ENS, RGPD, Seguridad TIC y Ciberseguridad.

Este equipo multidisciplinar se deberá proponer de forma tal, que combine capacidades y puntos fuertes individuales, para prestar el servicio de forma eficaz, siendo el principal objeto de los trabajos las tareas técnicas-organizativas-informaticas, con asesoramientos jurídicos.

eta informatikoak izango dira, aholkularitza juridikoarekin.

Proposatutako koordinatzailearen eta kontratuaren arduradunaren arteko ohiko komunikazio bideak hauek izango dira: posta elektroniko bat, telefono finkoaren zenbaki bat eta telefono mugikorraren zenbaki bat, eta bideo-konferentziarako tresna bat, aurrez aurrekoak ez diren bilerak egiteko balio duena.

Los canales de comunicación habituales entre la persona coordinadora propuesta y el responsable del contrato serán: un correo electrónico, un número de teléfono fijo y un número de teléfono móvil, y una herramienta de vídeo-conferencia que sirva para realizar las reuniones que no sean presenciales.

DonostiaTIKek bere SGSI propioa du gaur egun, eta, beraz, lanak egin bitartean sortutako dokumentazio guztia Buletin teknologiako SGSI honetan sartu beharko da, HCL Domino Notes ingurunean, eta dokumentuak PDF eta/edo Libreoffice formatuan edo etorkizunean zehaztuko dena izan beharko dira.

DonostiaTIK tiene actualmente su SGSI propio, por lo que toda la documentación generada durante la realización de los trabajos deberá incluirse en este SGSI de tecnología Boletín en el entorno HCL Domino Notes y los documentos deberán ser en formato PDF y/o Libreoffice o lo que en el futuro se defina.

Kontratua indarrean dagoen bitartean taldearen osaeran egiten den edozein aldaketak ezin izango du aldatu Kaudimen Teknikoan aurkeztutako egiaztapena, eta aldez aurretik DonostiaTIKi jakinarazi beharko zaio eta berariazko baimena izan beharko du.

Cualquier cambio en la composición del equipo durante la vigencia del contrato no podrá variar la acreditación aportada en la Solvencia Técnica, debiendo notificarse previamente a DonostiaTIK y contar con su autorización expresa.

Enpresa esleipenduneko langileen beharrezko ekipoak, lizentziak, komunikazioak eta joan-etorriak enpresa esleipendunaren kontura izango dira.

Los equipos, licencias, comunicaciones y desplazamientos necesarios del personal de la empresa adjudicataria serán a cargo de ésta.

Enpresa esleipendunak lanak egiteko behar diren ezagutzak DonostiaTIKekin partekatzeko duen prestasuna funtsezkotzat jotzen da horien garapen eraginkorrean.

La disponibilidad por parte de la empresa adjudicataria a la hora de compartir con DonostiaTIK los conocimientos necesarios para la realización de los trabajos se considera fundamental en el desarrollo eficaz de los mismos

4.1 Zerbitzu eta dedikazio mailako akordioak

Enpresa esleipendunak kontratazio honen xede diren zerbitzuak egiteko prestasuna izan behar du, bulegoko ordutegian, goizeko 9etatik arratsaldeko 17etara, astelehenetik ostegunera eta ostiraletan, 9: 00etatik 14:00etara. Nolanahi ere, SOC zerbitzuak 24x7 erabilgarri egon behar du kontratuak irauten duen bitartean.

4.1 Acuerdos de nivel de Servicios y dedicaciones

Se requiere que la empresa adjudicataria tenga disponibilidad para la realización de los servicios objeto de esta contratación, en horario de oficina de 9 de la mañana a 17 horas de la tarde, de lunes a jueves y viernes de 9 a 14:00 h. Sin perjuicio de que el servicio SOC requiere de operación de 24x7 durante toda la duración del contrato.

4.1.1 Adostasuna lortzeari buruzko zerbitzuak

Inplementazio planaren bidez, egin beharreko mugarrien arabera hedatuko dira zerbitzuak, aldez aurretik DonostiaTIKekin adostuta, eta bertan ezarriko dira gauzatzeko epeak.

4.1.1 Servicios relativos a conseguir la conformidad

A través del plan de implementación se irán desplegando los servicios según los hitos a realizar, previamente consensuados con DonostiaTIK y en el que quedarán establecidos los diferentes plazos de ejecución.

Planetik kanpoko atazak eskatzeko/kontsultatzeko, enpresa esleipendunak gehienez 24 orduko epean eta gehienez 7 egun balioduneko epean erantzun beharko du lanak egiten hasteko, eskaerak hala eskatzen badu.

Para solicitudes/consultas de tareas fuera del plan, la empresa adjudicataria deberá dar respuesta en un plazo máximo de 24 horas y un plazo máximo de 7 días hábiles para comenzar con los trabajos, en caso de que la solicitud así lo requiriera.

DBEOri buruzko kontsultak egiteko, enpresa

Para consultas en materia de RGPD la empresa

esleipendunak 72 orduko gehieneko epea izango du (24 orduko epea goizeko 9: 00etatik arratsaldeko 17:00etara, astelehenetik ostegunera eta ostiraletan 09:00etatik 14:00etara), gorabehera handia edo kritikoa izan ezean; kasu horretan, epea lanaldiarekiko independentea izango da.

4.1.2 Zibersegurtasuneko bulego teknikoaren laguntza-zerbitzuak

Inplementazio planaren bidez, egin beharreko mugarrien arabera hedatuko dira zerbitzuak, aldez aurretik DonostiaTIKekin adostuta, eta bertan ezarriko dira gauzatzeko epeak.

Planetik kanpoko eskaeretarako/kontsultetarako, enpresa esleipendunak gehienez 24 orduko epean eta gehienez 7 egun balioduneko epean erantzun beharko du lanak egiten hasteko, eskaerak hala eskatzen badu.

4.1.3 Zibersegurtasun Eragiketen Zentroaren Zerbitzua (SOC)

SOC zerbitzuak 24x7 eragiketa behar du kontratuak irauten duen bitartean.

Zerbitzuak, gehienez ere, kontratua sinatzen denetik 90 egun naturaleko epean egon beharko du martxan, eta operatibotzat joko da ezarritako soluzioa kudeatzeko panelen bidez egiaztatzen bada plegu honen 3.3 atalean zehaztutako baldintza guztiak ezarrita daudela.

Erantzuteko eta ebazteko denborei dagokienez, intzidentzia/kontsulta/eskaera tipologia hau hartzen da kontuan:

Ertaina - Baxua: zerbitzuaren operatibarekin zerikusia duen baina zerbitzuaren jarraipenean edo harekin lotutako beste batzuetan eraginik ez duen intzidentzia/kontsulta/eskaera.

Altua: zerbitzuaren operatibarekin zerikusia duen intzidentzia/kontsulta/eskaera, zerbitzuaren prestazioa edo harekin lotutako beste batzuk arriskuan jartzen duena edo are degradatuta dagoena.

Kritikoa: zerbitzua etenda dagoen intzidentzia/kontsulta/eskaera.

Ulertzen da:

Erantzuteko denbora (*): gorabehera/kontsulta/eskaera bat jakinarazten denetik esleipenduna hari zerbitzua emateko prest dagoen arte, hura onartzen dela jakinaraziz.

Ebazteko denbora (*): planteatu den kontsulta/eskaera ebazteko edo gorabehera adjudicataria tendrá un plazo máximo de 72 horas. (se entienden el plazo de 24 horas por una jornada comprendida de 9 de la mañana a 17 horas de la tarde, de lunes a jueves y viernes de 9 a 14:00 h), salvo incidencia alta o crítica, en cuyo caso el plazo será independiente de la jornada.

4.1.2 Servicios de soporte a la oficina técnica de Ciberseguridad

A través del plan de implementación se irán desplegando los servicios según los hitos a realizar, previamente consensuados con DonostiaTIK y en el que quedarán establecidos los diferentes plazos de ejecución.

Para solicitudes/consultas fuera del plan, la empresa adjudicataria deberá dar respuesta en un plazo máximo de 24 horas y un plazo máximo de 7 días hábiles para comenzar con los trabajos, en caso de que la solicitud así lo requiriera.

4.1.3 Servicio de Centro de Operaciones de Ciberseguridad (SOC)

El servicio SOC requiere de operación de 24x7 durante toda la duración del contrato.

El servicio deberá estar operativo como máximo a los 90 días naturales desde la firma de contrato, considerándose operativo, cuando se constate a través de los paneles de gestión de la solución implantada que todos lo requisitos detallados en el apartado 3.3 del presente pliego están implementados.

En relación con los tiempos de respuesta y resolución, se considera la siguiente tipología de incidencia / consulta / petición:

Media - Baja: aquella incidencia / consulta / petición que tiene relación con la operativa del servicio pero que no impacta en la continuidad de este u otros relacionados con él.
Alta: aquella incidencia / consulta / petición que, relacionada con la operativa del servicio, pone en riesgo, o incluso está degradada la prestación o continuidad de este u otros relacionados con él.

Crítica: aquella incidencia / consulta / petición que hay corte de servicio.

Se entiende:
- **Tiempo de respuesta (*):** el periodo de tiempo desde que se comunica una incidencia/consulta/petición hasta que el adjudicatario está disponible para dar servicio a la misma, comunicando su aceptación.
- **Tiempo de resolución (*):** el tiempo necesario para: resolver la consulta/petición que ha sido planteada, ó dar soporte a la resolución de un posible incidencia, una vez ha sido recibida por el

posible baten ebazpenari euskarria emateko behar den denbora, esleipendunak jaso ondoren.

Horrela, erantzuteko eta ebazteko denborak honako hauek izango dira:

LEHENTASUNA	Gehieneko erantzun denbora	Gehieneko euskarri denbora ebazpenean
Ertaina-baxua	24h	72h
Altua	12h	24h
Kritikoa	2h	4h

	Gehieneko denbora
Segurtasun-gorabehera kritikoen jakinarazpena	2h
Arintzeko soluzioen eta kontraneurrien proposamenak egitea gorabehera kritikoak	6h

Maila altuko edo kritikoko segurtasun gertakariei erantzuteko, zerbitzuaren barruan egongo da, kostu gehigarririk gabe, intzidentea koordinatzeko eta kudeatzeko euskarria lehen bi egunetan.

Gainerako jardunaldietarako, SPKL 120. artikuluan oinarritutako larrialdi bidez kontratatuko dira udal zerbitzu guztiak berrezartzeko behar diren zerbitzuak; horretarako, diziplina anitzeko talde baten prezioa/ordua ezarriko da, eta talde horrek analisi forentsea, erantzuna eta errekuperazioa, komunikazioaren kudeaketa eta abar egingo ditu.

adjudicatario.

De esta forma los tiempos de respuesta y resolución serán los siguientes.

PRIORIDAD	Tiempo máximo de respuesta	Tiempo máximo de soporte en la resolución
Media - Baja	24h	72h
Alta	12h	24h
Crítica	2h	4h

	Tiempo máximo
Notificación de incidentes críticos de seguridad	2h
Realización de propuestas de soluciones y contramedidas para mitigar incidentes críticos	6h

Para la respuesta ante incidentes de seguridad de nivel alto o crítico, estará incluido dentro del servicio, sin coste adicional,el soporte para la coordinación y la gestión del incidente durante los dos primeros días.

Para el resto de jornadas, se contratará por vía de emergencia con base en el artículo 120 de la LCSP los servicios necesarios para el restablecimiento de todos los servicios municipales, para ello se establecerá precio/ hora de un equipo multidisciplinar que realice las tareas de análisis forense, respuesta y recuperación, gestión de la comunicación, etc.

5.- LANEN KONTROLA

DonostiaTIK zerbitzuak beretzat gordetzen du egindako lanen kalitatearen kontrola, eta gutxieneko baldintzak betetzen ez dituztenak baztertu ahal izango ditu, plegu tekniko hauetako 3. puntuan eskatutako irizpideen arabera. Hori guztia Donostiatik zerbitzuak atzeratzearen edo kalitate eskasaren ondorioz ezar ditzakeen zigorrak alde batera utzita. Era berean, kontratatutako zerbitzuen atzerapenen edo kalitate eskasaren ondorio ere bada, eta arrazoi bera izango da. Suntsiarazpena justifikatuta.

Ezarritako plana koordinatzeko, gainbegiratzeko eta haren jarraipena egiteko bilerak egingo dira Donostiatik zerbitzuak ezartzen duen aldizkakotasunarekin.

Lanak hasi aurretik, Donostiako Udaleko eta/edo DonostiaTIK erakundeko Informazioaren Segurtasun Batzordeari aurkezpen bat egingo zaio, eta bi hilean behin, edo beharrezkotzat jotzen denean, batzordeei

5.- CONTROL DE LOS TRABAJOS

DonostiaTIK se reserva el control de la calidad de los trabajos realizados, pudiendo rechazar aquellos que no cumplan las condiciones mínimas, de acuerdo con los criterios exigidos en el punto 3 de estos pliegos técnicos, todo ello, con independencia de las penalizaciones que DonostiaTIK pueda imponer como consecuencia de los retrasos o de la baja calidad de los servicios contratados, siendo así mismo causa justificada de resolución contractual.

Se realizarán reuniones de coordinación, supervisión y seguimiento sobre el plan establecido con la periodicidad que establezca DonostiaTIK.

Se realizará una presentación, previa al comienzo de los trabajos, al Comité de Seguridad de la Información del Ayuntamiento de Donostia/San Sebastian y/o al de DonostiaTIK, y cada dos meses, o cuando se estime necesario, se informará a los Comités, del progreso de los

lanen aurrerapenaren berri emango zaie.

6.- TRANSFERENTZIA TEKNOLOGIKOA

Kontratuaren xede diren lanak egiten diren bitartean, enpresa esleipendunak konpromisoa hartzen du DonostiaTIK sozietateari eskatzen dion informazio eta dokumentazio guztia emateko, lanak nola egiten diren, sor daitezkeen arazoak eta horiek konpontzeko teknologiak, metodoak eta tresnak ezagutzeko.

7.- LANEN DOKUMENTAZIOA

Kontratua gauzatu bitartean sortutako dokumentazioa DonostiaTIK enpresaren jabetzakoa izango da soilik, eta enpresa esleipendunak ezingo du dokumentazio hori gorde, ez eta haren kopiarik lortu edo hirugarrenei eman ere, aipatutako erakundearen berariazko baimenik gabe.

Esleipendunak dokumentazioaren bertsio berriak eman beharko dizkio DonostiaTIK erakundeari, hala badagokio.

trabajos.

6.- TRANSFERENCIA TECNOLÓGICA

Durante la ejecución de los trabajos objeto del contrato la empresa adjudicataria se compromete a facilitar a DonostiaTIK la información y documentación que solicite a efectos de conocer las circunstancias en que se desarrollan los trabajos así como los problemas que puedan plantearse y las tecnologías, métodos y herramientas para resolverlos.

7.- DOCUMENTACIÓN DE LOS TRABAJOS

La documentación generada durante la ejecución del contrato será propiedad exclusiva de DonostiaTIK sin que la empresa adjudicataria pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de la citada organización.

El adjudicatario deberá suministrar, en su caso, a DonostiaTIK las nuevas versiones de la documentación.

Donostian, sinaduraren egunean

Kontratuaren Arduraduna

Sin/Fdo: Lourdes Apeztegia Alzola