ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA · MINISTERIO DE POLITICA TERRITORIAL · Plan de Recuperación, Transformación y Resiliencia · Financiado por la Unión Europea NextGenerationEU

PLIEGO DE PRESCRIPCIONES TECNICAS

Centro de Operaciones de Ciberseguridad

Expediente 202201336

INDICE:

Objeto y alcance del contrato 4
Plazo de ejecución 5
Facturación 5
Presentación de la Oferta Técnica (proyecto técnico) 5
Gestor Técnico 6
Requisitos mínimos 6
Requisitos comunes a los capítulos objeto del contrato 7
Criterios valorables por formula 8
PROTECCIÓN DE DATOS 8
CONDICIONES ESPECIALES DE EJECUCIÓN 8
CAPITULO I: Suministro, licenciamiento y servicios de garantía de la plataforma especificada 10
Concepto I.1 Cortafuegos - Firewall 10
Descripción de los suministros 10
Objetivos 10
Requisitos 10
A tener en cuenta y valorar 12
Actualización, renovación y soporte licencias 12
Servicios de soporte y/o mantenimiento 12
Trabajos complementarios de instalación avanzados 12

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

Concepto I.2 Antivirus y EDR 14
Descripción de los suministros 14
Objetivos 14
Requisitos 14
A tener en cuenta y valorar 17
Actualización, renovación y soporte licencias 20
Servicios de soporte y/o mantenimiento 20
Trabajos complementarios de instalación avanzados 20
Concepto I.3 NAC Network Access Control 23
Descripción de los suministros 23
Objetivos 23
Requisitos 23
A tener en cuenta y valorar 25
Actualización, renovación y soporte licencias 25
Servicios de soporte y/o mantenimiento 25
Trabajos complementarios de instalación avanzados 26
Concepto I.4 SIEM Security Information and Event Managemet 28
Descripción de los suministros 28
Objetivos 28
Requisitos 28
A tener en cuenta y valorar 31
Actualización, renovación y soporte licencias 32
Servicios de soporte y/o mantenimiento 32
Trabajos complementarios de instalación avanzados 32

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

Entregables 33
Documento que garantice la compatibilidad con las funciones existentes 34
Concepto I.5 Garantía del SOC 35
Descripción de los suministros 35
Objetivos 35
Requisitos 35
A tener en cuenta y valorar 37
Entregables 37
Concepto I.6 Herramientas del CCN-CERT 38
Concepto I.6.1 Implantación LUCIA 38
Concepto I.6.2 Implantación MICROCLAUIDIA 38
Concepto I.6.3 Implantación de sonde SAT-INET 38
Concepto I.6.4 Implantación de REYES/MISP 38
CAPITULO II: Mantenimiento por dos (2) años de la plataforma implantada 39
Objetivos y alcance 39
Requisitos 39
Condiciones de ejecución del servicio del SOC 24x7 40
Niveles de servicio 41

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Objeto y alcance del contrato

Implantar un Centro de Operaciones de Ciberseguridad (vSOC), para lo que habrá que suministrar los componentes necesarios y así como su explotación.

El vSOC será el sistema encargado de realizar un seguimiento y analizar la actividad en redes, 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 para tratar de aplicar medidas correctivas e informar a la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

A través de este proyecto de ciberseguridad se podrá:

✓ Garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales que presta el Ayuntamiento y mejorar su capacidad de prevención, detección y respuesta ante ataques o incidentes de seguridad.

✓ Contar con un sistema de seguimiento que permita la monitorización de los sistemas.

✓ Compartir con otras administraciones públicas integradas en la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes toda la información relativa a incidentes de seguridad que pueda ayudar a prevenir y evitar ataques.

✓ Mejorar la protección de la información tratada y almacenada en el conjunto de sistemas de información del Ayuntamiento.

✓ Proteger la continuidad de los servicios digitales que se prestan a la ciudadanía desde el Ayuntamiento.

✓ Proteger y garantizar la normal actividad municipal.

✓ Capacitar a los técnicos informáticos en materia de ciberseguridad, en particular para corregir fallos de configuración, prevenir y/o subsanar incidentes.

✓ Aumentar el parque tecnológico actual del Ayuntamiento que permita incrementar los flujos y elementos que serán analizados por el vSOC.

Objetivos adicionales:

✓ Sensibilizar al resto de la organización, no implicada directamente en el proyecto vSOC, acerca de la vulnerabilidad de la información tratada en el ayuntamiento y de la necesidad de proteger los sistemas.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

✓ Formar a todos los empleados en los riesgos y medidas proactivas a tomar para evitar los ciberataques.

Objetivos, todos ellos, alineados con las especificaciones, directrices, exigidas y recomendadas por el CCN Centro Criptológico Nacional.

A continuación se especifican las prescripciones que han de cumplir las soluciones ofertadas en los siguientes capítulos de forma conjunta.

CAPITULO I: Suministro, licenciamiento y servicios de garantía de la plataforma especificada

CAPITULO II: Mantenimiento por dos (2) años de la plataforma implantada

Plazo de ejecución

El plazo de instalación y puesta en funcionamiento del suministro correspondiente al Capítulo I, se establece en tres (3) meses desde la firma del contrato. Los Técnicos municipales verificarán su correcta instalación y funcionamiento, recepcionando las prestaciones de dicho Capítulo I, por tratarse del gasto subvencionable de este contrato en el marco del PRTR, facilitando así la trazabilidad de esta actuación con vistas a su adecuada y precisa justificación.

El plazo de ejecución para las prestaciones del Capítulo II será de dos años desde el fin de la garantía del objeto del Capítulo I.

Se valorará como mejora (MEJ.0) la reducción del plazo de ejecución de Capítulo I.

Facturación

El importe adjudicado total para el Capítulo I se facturará con el acta de recepción de dicho objeto.

El importe adjudicado para el Capítulo II se facturará en periodos mensuales vencidos hasta el fin del contrato, dos (2) años desde el fin de la garantía del objeto de los componentes del Capítulo I.

Presentación de la Oferta Técnica (proyecto técnico)

Deberá seguir la estructura del presente pliego.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Deberá especificar todos y cada uno de los requisitos (REQ.x) que se indican en los Capítulos y Conceptos del presente pliego en el orden indicado en el mismo, con indicación y justificación de que la solución propuesta lo cumple, justificación suficiente para su valoración.

De forma análoga para los conceptos a valorar (VAL.x) que se indican en los Capítulos y Conceptos del presente pliego en el caso que la solución presentada las cumpla se deberá indicar y justificar convenientemente para su valoración.

Disponiendo por cada Capítulo y Concepto la posibilidad de incluir mejoras, bondades o cuanto se quiera presentar técnicamente para su valoración.

Gestor Técnico

La oferta debe incluir la figura de un gestor técnico que ejerce de responsable del contrato por parte del adjudicatario y de interlocutor con el Ayuntamiento de Barakaldo.

Requisitos mínimos

Los licitadores deberán acreditar la existencia de un sistema adecuado de gestión de calidad a tales efectos deberán contar con las siguientes certificaciones o equivalentes:

- (REQ.1) Certificación conforme a ENS de nivel Medio para Servicios de instalación, operación, asistencia técnica y soporte a infraestructuras de Tecnologías de la Información y las Comunicaciones.
- (REQ.2) ISO 9001: Sistema de Gestión de la Calidad.
- (REQ.3) ISO 14001: Sistema de Gestión Medioambiental.
- (REQ.4) ISO 20000: Sistema de Gestión de Servicios de TI
- (REQ.5) ISO 27001: Sistema de Gestión de Seguridad de la Información

Se valorará disponer de:

- (MEJ.1) Certificación conforme a ENS de nivel Alto para Servicios de instalación, operación, asistencia técnica y soporte a infraestructuras de Tecnologías de la Información y las Comunicaciones
- (MEJ.2) ISO 15504: Modelo de madurez de la Ingeniería del Software.
- (MEJ.3) ISO 22301: Sistema de Gestión de Continuidad del Negocio.
- (MEJ.4) ISO 27017: Controles de Seguridad para Servicios Cloud.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (MEJ.5) ISO 27018: Protección de la Información de Identidad Personal PII) en Cloud.

Requisitos comunes a los capítulos objeto del contrato

a) En el caso que la solución propuesta para los componentes contemplen servicios en la nube. Dado que la aplicación del servicio así como lo base de datos asociada se alojará en servidores externos a los servidores municipales del Ayuntamiento, tienen que cumplir las condiciones siguientes:
   - Los datos y el servicio tendrán que estar alojados en servidores ubicados dentro del Espacio Económico Europeo.
   - Servidores dimensionados para garantizar el correcto funcionamiento de la aplicación de acuerdo con las necesidades indicadas iniciales y las que la evolución propia del proyecto requiera en cada momento.
   - Monitorización 24x7x365 de los servidores, parta prevenir y responder a cualquier incidencia que impida el acceso y la correcta ejecución de la aplicación así como de posibles ataques o intentos de intrusión no autorizados.
   - El prestador del servicio "cloud" (sea el propio licitador o un tercero) deberá acreditar la posesión de las diferentes certificaciones relativas a la prestación del servicio:
     - Datacenter certificado TIER III o superior
     - Certificación ISO 27001
     - Certificación ENS nivel ALTO en prestación de servicios CloudSe considera el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en lo indicados en los artículos 2, 16 y 19 y concretamente en la disposición transitoria única de adecuación de sistemas que establece un plazo de veinticuatro meses para alcanzar su plena adecuación al ENS. Por lo que el prestador tiene hasta el 05/05/2024 para certificarse.
   - Como medidas técnicas de seguridad, deberá contar con las siguientes:
     - Doble barrera redundante de seguridad perimetral UTM, de dos fabricantes diferentes.
     - Barrera perimetral redundante y propósito específico anti DDoS (denegación de servicio)
   - Se realizarán los servicios necesarios para realizar copias de seguridad y recuperación de la base de datos y aplicaciones instaladas. El Ayuntamiento, en cualquier momento, podrá solicitar copia del sistema para su salvaguarda o migrar a otro cloud privado o propio.
   - El almacenamiento de las copias de seguridad deberá ser en datacenter independiente del datacenter principal.

b) El presente contrato contempla el suministro de las licencias y servicios necesarios para conseguir los objetivos de los diferentes Capítulos y sus Componentes contenidos, así como el mantenimiento correctivo, adaptativo y evolutivo durante la ejecución del contrato.

c) En caso de que la solución requiera uso de tecnología de virtualización de servidores, dada la capacitación que dispone la Sección de Sistemas del Servicio O.S.IT., deberá ser VMware 7.x.

d) Para el Plan de Contingencia y Recuperación de la Plataforma de Ciberseguridad resultante de la ejecución de este contrato, el Ayuntamiento pone a disposición del adjudicatario el Sistema de Backup Municipal Veritas Backup Exec que actualmente dispone o que disponga en su momento.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

Siendo necesaria la colaboración del adjudicatario con la Sección de Sistemas para su configuración y validación.

e) Perfiles profesionales, se debe proporcionar los perfiles profesionales que el adjudicatario utilizará en la ejecución de este contrato.

f) El adjudicatario podrá subcontratar tareas con otros especialistas, siendo de aplicación los requisitos del adjudicatario a los subcontratados.

Criterios valorables por formula

Se valorarán positivamente si el licitador presenta los siguientes criterios:

(MEJ.1) Realización de una auditoria externa del estado de ciberseguridad a la finalización de los compromisos expresado en el Capítulo I del presente pliego.

(MEJ.2) Que la propuesta proponga componentes del mismo fabricante.

(MEJ.3) Mejorar el plazo de implantación del Capítulo I de requerimientos.

(MEJ.4) Acceso a plataformas de formación y concienciación en materia de seguridad informática.

PROTECCIÓN DE DATOS

De conformidad con la Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, Reglamento General de Protección de Datos (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento, mediante la suscripción del correspondiente contrato de encargo de tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD.

CONDICIONES ESPECIALES DE EJECUCIÓN

En cumplimiento de lo prescrito en el art. 202 de la LCSP, se establece como condición especial de ejecución de este contrato, el mantenimiento o mejora de los valores medioambientales que puedan verse afectados por la ejecución del mismo, con condiciones como es el evitar el uso de papel en las comunicaciones que se deban realizar en su ejecución, con el consiguiente ahorro energético y de agua, además, los elementos disponen de funciones de ahorro de energía y cumplen los requisitos de consumo energético, lo que

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

favorece el ahorro energético durante su uso, o que el proveedor suministrará conjuntamente los elementos objeto del contrato, con la finalidad de reducir las emisiones de gases de efecto invernadero que conllevaría la realización del suministro por partes, contribuyéndose con estas condiciones a dar cumplimiento al objetivo que establece el art. 88 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

Al finalizar la ejecución del contrato, el adjudicatario presentará una declaración responsable en la que manifieste el cumplimiento de estas condiciones.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

CAPITULO I: Suministro, licenciamiento y servicios de garantía de la plataforma especificada

Concepto I.1 Cortafuegos - Firewall

Descripción de los suministros

Un firewall constituye uno de los principales elementos de seguridad en una organización como el Ayuntamiento de Barakaldo, al ser el elemento que recibe todo el tráfico que viene de internet, de forma que debe ser capaz de detectar intrusiones, inspeccionar paquetes, analizar tráfico incluyendo el https, realizar filtrado antispam y de contenidos, etc.

Objetivos

El alcance de este servicio incluye el suministro, instalación y puesta en servicio de dos firewalls físicos montados y configurados como una granja en alta disponibilidad, así como el soporte técnico prestado por el propio fabricante, la garantía y los servicios de seguridad.

La garantía será como mínimo de un (1) año desde la el acta de recepción de este concepto o componente.

El suministro deberá contemplar todas las licencias (propias y de terceros) y su mantenimiento necesarias durante el plazo de garantía no suponiendo coste para el Ayuntamiento.

Requisitos

El equipamiento deberá cumplir los siguientes requisitos mínimos:

- (REQ.1) Los equipos ofertados deberán aparecer como certificados en categoría ALTA en la Guía de Seguridad de las TIC CCN-STIC-105 del CCN CERT (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion.html) en el apartado de productos cualificados, fijando como fecha de referencia para el cumplimiento de este requisito el último día del plazo de presentación de ofertas del presente concurso.
- (REQ.2) Actualmente el Ayuntamiento de Barakaldo dispone de una barrera de firewall en alta disponibilidad (HA) del fabricante Fortinet y de una barrera de firewall de aplicación web (WAF) en HA. Es por ello y para dar cumplimiento a los requisitos del ENS el suministro que se contempla en este concepto que debe ser de un fabricante diferente al que actualmente dispone el Ayuntamiento.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.3) El formato del suministro es appliance on-premise, para ello el Ayuntamiento proporcionará el espacio necesario para ellos en sus racks disponibles en su CPD.
- (REQ.4) Las características hardware mínimas de cada equipo deben ser las siguientes:
  - Rendimiento de firewall igual o mayor que 1 Gbps.
  - Rendimiento de IPS igual o superior a 1,4 Gbps
  - Rendimiento de antimalware igual o superior con todos los elementos de seguridad activados a 1,5 Gbps
  - Conexiones concurrentes: 1M
  - Nuevas conexiones por segundo: 14.000
  - Interfaces de red:
    - 2 puertos 2,5GbE SFP+
    - 2 puertos 2,5GbE RJ45
    - 8 puertos 1GbE RJ45
    - 1 puerto MGMT
  - 2 puertos USB
- (REQ.5) Motor AV sin límites en el tamaño de ficheros a analizar.
- (REQ.6) Capacidad para detectar virus en más de 6 protocolos TCP diferentes
- (REQ.7) Motor DPI que realiza el análisis de los paquetes “al vuelo” (sin necesidad de reensamblaje).
- (REQ.8) Arquitectura de procesadores Multi-Core.
- (REQ.9) Solución de Sandboxing en la nube con múltiples motores.
- (REQ.10) Al usar el servicio de Sandboxing, posibilidad de bloquear la descarga hasta que haya un veredicto.
- (REQ.11) Visualización de tráfico (aplicaciones, usuarios, etc.) en tiempo real.
- (REQ.12) Posibilidad de configurar simultáneamente múltiples modos/topologías (p.ej.: NAT, L2 Bridge Mode, Transparent Mode, etc.)
- (REQ.13) Soporte para NetFlow e IPFix.
- (REQ.14) Inspección de tráfico cifrado con SSL (DPI-SSL y SSH) en puertos diferentes al 443/TCP.
- (REQ.15) Posibilidad de configurar Inclusiones/Exclusiones basadas en categorías de Content Filtering (CFS) para el servicio DPI-SSL.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.16) Posibilidad de configurar Inclusiones/Exclusiones basadas en dominio para el servicio DPI-SSL.
- (REQ.17) En el servicio de Filtrado Web (CFS), posibilidad de configurar múltiples páginas de bloqueo personalizadas.
- (REQ.18) Posibilidad de compartir licencias en entornos de HA.

A tener en cuenta y valorar

La solución propuesta para este concepto, en el caso que se contemplen, serán valoradas.

- (VAL.1) El motor antivirus que utilicen estos firewall deberá estar certificado por ICSA Labs (International Computer Security Association).

Actualización, renovación y soporte licencias

Incluidos durante el periodo de garantía del suministro.

Servicios de soporte y/o mantenimiento

Incluidos durante el periodo de garantía del suministro.

Trabajos complementarios de instalación avanzados

Trabajos de instalación

Trabajos que permitan verificar que se cuenta con una instalación plenamente funcional e integrada en el Ayuntamiento, como los siguientes:

- Instalación de la solución en el CPD Municipal
- La correcta integración con las herramientas de monitorización de seguridad del Ayuntamiento (EDR, SIEM, etc.), en la forma que especifique el Ayuntamiento. Estos trabajos deben contar con la verificación del Servicio de Organización, Sistemas e Innovación Tecnológica (O.S.IT) del Ayuntamiento para darse por satisfactoriamente realizado.

Estimación de jornadas profesionales

Para la realización de los trabajos necesarios, se deberá indicar en la oferta técnica el mínimo de jornadas profesionales de arquitectos y consultores expertos en la solución ofertada para conseguir el objetivo y los requerimientos de este concepto.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Condiciones de ejecución de los trabajos

Si la naturaleza de los trabajos lo requiere, éstos tendrán que ser realizados en las instalaciones del Ayuntamiento de Barakaldo en los horarios marcados por el Servicio O.S.IT.

Es posible la ejecución de tareas-trabajos en formato remoto cuando técnicamente sea viable, en este caso, serán por cuenta del adjudicatario las licencias de terceros necesarias para el control remoto securizado a nuestra infraestructura.

Entregables

El adjudicatario deberá proporcionar, al menos, los siguientes entregables en el ámbito de la instalación avanzada, que deberán ser validados por el Servicio O.S.IT. del Ayuntamiento para su aceptación:

- Elaboración de un Plan de Trabajo detallado.
- Documento de análisis y diseño incluyendo esquemas de arquitectura lógica y física.
- Documentación de instalación, parametrización y configuración
- Planes de pruebas realizadas y sus resultados.
- Plan de contingencia, detallando las actuaciones para llevarlo a cabo
- Manuales y otro material relacionado con la transferencia de conocimientos
- Informes periódicos de las actuaciones realizadas

La documentación se deberá mantener actualizada en el periodo de ejecución del objeto de este apartado, en todo caso estarán sujetas a las condiciones de planificación del proyecto indicadas por el Servicio de O.S.IT. del Ayuntamiento.

Documento que garantice la compatibilidad con las funciones existentes

La solución deberá mantenerse la integridad, compatibilidad con el resto de componentes de la Plataforma de Ciberseguridad que tiene por objeto general el presente pliego.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Concepto I.2 Antivirus y EDR

Descripción de los suministros

El Ayuntamiento de Barakaldo dispone actualmente de un antivirus del fabricante SYMANTEC, sin funcionalidades avanzadas de EDR.

Las nuevas amenazas del ciberespacio, tales como el ransomware, hacen necesaria la incorporación de nuevos elementos de detección y respuesta (EDR) que complementen la protección clásica de los antivirus basados en firmas.

Se define el término de "endpoint" como cualquier dispositivo con posibilidad de conexión a la infraestructura de comunicaciones del Ayuntamiento, centrándose en puestos de trabajo y servidores de proceso.

Objetivos

Suministro de las licencias de tipología EDR (Endpoint Detection & Response) para la infraestructura del Ayuntamiento de Barakaldo que en la actualidad está compuesta por 700 elementos (puestos de trabajo y servidores).

La garantía será como mínimo de un (1) año desde la el acta de recepción de este concepto o componente.

El suministro deberá contemplar todas las licencias (propias y de terceros) y su mantenimiento necesarias durante el plazo de garantía no suponiendo coste para el Ayuntamiento.

Despliegue de la solución en 100 elementos de la infraestructura indicados por el Servicio de O.S.IT. del Ayuntamiento.

Requisitos

Se propone modernizar la seguridad de puesto con una solución que cumpla los siguientes requisitos mínimos:

- (REQ.1) Los equipos ofertados deberán aparecer como certificados en categoría ALTA en la Guía de Seguridad de las TIC CCN-STIC-105 del CCN CERT (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion.html) en el apartado de productos cualificados, fijando como fecha de referencia para el cumplimiento de este requisito el último día del plazo de presentación de ofertas del presente concurso.
- (REQ.2) La existencia de un único agente para EPP y EDR, sin necesidad de agentes adicionales

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.3) Para minimizar el consumo de recursos, el producto debe permitir la instalación de módulos personalizada (por ejemplo, instalación del módulo de antimalware sin el módulo de firewall).
- (REQ.4) Para ofrecer una mejor protección contra Ransomware la solución debe incluir “archivos cebo” o “decoy files” en las estaciones de trabajo y los servidores y actuará como una capa de bloqueo contra el proceso de cifrado. El “ransomware vaccine” será actualizada por el proveedor utilizando el mismo proceso de actualización que está siendo desarrollado por el modulo antimalware.
- (REQ.5) La solución deberá poder proteger específicamente los endpoints contra los ataques ransomware bloqueándolos antes de que puedan dañar los sistemas. En el caso de un nuevo ransomware (Zero Day) que no pudo bloquearse de forma proactiva, también debería implementar algunas operaciones/técnicas de copia de seguridad automática, basadas en la tecnología Windows Shadow Copy.
- (REQ.6) La solución debería poder bloquear los ataques basados en Ransomware tanto de forma local a los endpoints como de forma remota haciendo una clasificación total de todos los ejecutables provenientes del exterior, tanto de dispositivos de almacenamiento externos como de Internet o redes externas
- (REQ.7) La solución incluirá algoritmos Machine Learning utilizados contra ataques Zero-Day o Advanced Exploit (directional).
- (REQ.8) La solución incluirá un módulo de gestión del riesgo (Gestión de Riesgo del Endpoint) capaz de identificar y proporcionar remediación para una gran categoría de indicadores de riesgo y configuraciones erróneas que pueden afectar a la funcionalidad y comprometer la seguridad del endpoint
- (REQ.9) El módulo de gestión de riesgo debe proporcionar un Dashboard con el estado de riesgo del ayuntamiento.
- (REQ.10) El módulo de gestión de riesgo debe proporcionar una separación entre configuraciones incorrectas, vulnerabilidades de aplicaciones y comportamiento humano
- (REQ.11) La solución debe incluir tecnología de firmas, tanto local como en cloud, heurísticos, filtrado de URL y categorización que ayuden a la detección de ataques avanzados en la fase de pre-ejecución
- (REQ.12) Esta tecnología también será utilizada para detectar APTs (Advanced Persistent Threats), archivos o tráfico de red sospechoso con la capacidad de establecer al menos 3 umbrales de protección para cada tipo de actividad/archivo sospechoso: permisivo, normal o agresivo.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.13) La tecnología deberá ser capaz de reportar, bloquear, desinfectar, eliminar o enviar a cuarentena cada uno de los archivos sospechosos y dar la opción al administrador de la solución de bloquear o reportar cada categoría (incluyendo la capacidad de reportar actividad/archivos que deberían haber sido bloqueados en un umbral más alto que el actualmente en uso)
- (REQ.14) La solución deberá incluir un módulo de clasificación 100% de ejecutables o procesos ejecutándose en el cloud público del proveedor.
- (REQ.15) El módulo Sandbox deberá ser capaz de enviar automáticamente (o manualmente) varios archivos para su “detonación”
- (REQ.16) El módulo de clasificación tendrá la capacidad de bloquear o monitorizar los archivos actualmente enviados para analizar. En el modo monitorización, el archivo enviado deberá ser accesible en el endpoint durante la detonación mientras que el modo bloqueo el acceso al archivo enviado será bloqueado hasta que la clasificación se haya completado y se realice una acción específica en el archivo enviado
- (REQ.17) La solución deberá de proveer de un servicio de antivirus para navegación web y control de acceso a páginas web
- (REQ.18) La solución incluirá un módulo para conocer si las amenazas se han llegado a ejecutar y qué acciones han llevado a cabo: si se han tenido acceso a datos o han establecido conexiones externas al equipo.
- (REQ.19) Este módulo utiliza la recopilación de datos (incluyendo eventos hardware y software grabados en el puesto de trabajo/endpoint) y tiene la capacidad de dibujar un detallado mapa del incidente, tanto como proporcionar las acciones de remediación para cada fase del ataque
- (REQ.20) El módulo EDR tendrá la capacidad de filtrar incidentes desde la consola de administración utilizando varios criterios: tipo de infección (malware o PUP), si el binario ha sido ejecutado, fecha, acción, si se ha tenido acceso a datos o ha habido conexiones externas, etc…
- (REQ.21) En caso de Indicador de Ataque, el módulo EDR tendrá la capacidad de evaluar la actividad típica del endpoint (baseline) de acuerdo con las técnicas MITRE
- (REQ.22) El módulo EDR permite la visualización con gran detalle de cada incidente incluyendo detalles específicos de cada endpoint afectado, proceso especifico, cronología y también actuar en cada paso del incidente con un conjunto de acciones que se pueden utilizar para investigar más a fondo (Sandbox, Virus Total, Google search) o simplemente matar el proceso, aislar el equipo,

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

realizar una conexión remota con el equipo, instalar parches o añadir una excepción de URL (dependiendo del tipo de amenaza evaluada en cada paso del incidente).

- (REQ.23) El módulo EDR puede bloquear archivos y/o procesos basados en los valores hash (MD5/SHA256) directamente desde la consola de gestión
- (REQ.24) El módulo EDR puede añadir excepciones para archivos no maliciosos para parar cualquier investigación en ellos o puede añadir a una lista negra un conjunto de archivos maliciosos conocidos para prevenir movimientos laterales.
- (REQ.25) El módulo EDR permitirá conexión remota al endpoint potencialmente comprometido para hacer posible una rápida investigación y remediación directamente en el endpoint desde la consola. Un conjunto específico de comandos a nivel de kernel están disponibles para minimizar el tiempo de remediación o recoger datos adicionales.
- (REQ.26) La solución deberá incluir un módulo Host IPS capaz de bloquear varias amenazas en la capa de red incluyendo la prevención de movimientos laterales para varias categorías de malware.
- (REQ.27) El módulo Host IPS deberá estar integrado con el módulo EDR y este puede incluir información específica desde el módulo de Host IPS en los detalles del incidente.
- (REQ.28) La solución EDR trabajará con la solución EPP para crear incidentes de seguridad para todo el malware detectado en los endpoints.
- (REQ.29) La solución EDR deberá integrase con una solución Patch Management para instalar los parches faltantes como una acción de respuesta.
- (REQ.30) La solución propuesta deberá constar con soporte para sistemas Legacy como: Windows XP, Windows 7, Windows 7, Windows 2000, Windows 2003 o Windows 2008.
- (REQ.31) Consumo de recursos muy limitado, máximo 5% con todos los componentes

A tener en cuenta y valorar

La solución propuesta para este concepto, en el caso que se contemplen, serán valoradas.

- (VAL.1) La solución debe incluir tecnología “Tuneable Machine Learning” utilizada para detectar ataques avanzados en la fase de pre-ejecución.
- (VAL.2) El módulo Sandbox deberá ser capaz de enviar automáticamente (o manualmente) varios archivos para su “detonación”

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (VAL.3) El módulo Sandbox tendrá la capacidad de bloquear o monitorizar los archivos actualmente enviados para analizar. En el modo monitorización, el archivo enviado deberá ser accesible en el endpoint durante la detonación mientras que el modo bloqueo el acceso al archivo enviado será bloqueado hasta que la detonación se haya completado y se decide realice una acción específica en el archivo enviado.

- (VAL.4) La detonación manual es controlada por el administrador (el administrador de la consola de administración puede enviar archivos manualmente al Sandbox, uno o más archivos al mismo tiempo y especificar si los archivos serán detonados simultánea o individualmente).

- (VAL.5) El módulo Sandbox puede "detonar" los siguientes tipos de archivos: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

- (VAL.6) Los archivos soportados mencionados en el punto anterior pueden ser detonados incluso si están dentro de un archivo con el siguiente formato: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. – los archivos que están utilizando una contraseña pueden ser detonados solamente si se proporciona la contraseña antes de la detonación.

- (VAL.7) La solución Sandbox debe ser capaz de analizar URLs.

- (VAL.8) La solución Sandbox debe ser capaz de analizar archivos protegidos por contraseña.

- (VAL.9) La solución incluirá un módulo Endpoint Detection and Response, capaz de identificar ataques avanzados que se están llevando a cabo en tiempo real (fase de ejecución).

- (VAL.10) Este módulo utiliza la recopilación de datos (incluyendo eventos hardware y software grabados en el puesto de trabajo/endpoint) y tiene la capacidad de dibujar un detallado mapa del incidente, tanto como proporcionar las acciones de remediación para cada fase del ataque (incluyendo integración con los algoritmos ajustables de Machine Learning, presentados anteriormente que pueden bloquear varios tipos de ataques en la fase de pre-ejecución, módulo Sandbox, etc.). Desde una perspectiva puramente funcional, el módulo EDR consta de dos componentes distintos: uno que recopila y procesa los datos relacionados con eventos de seguridad y el componente forense que interpreta los datos y los correspondientes indicadores de compromiso.

- (VAL.11) El módulo EDR tendrá a capacidad de filtrar incidentes desde la consola de administración utilizando varios criterios: puntuación, fecha, estado, ID de la alerta, nombre del endpoint, tipo de

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

ataque, número de alertas, técnicas ATT&CK, IP del endpoint, MD5, SHA256, nombre del nodo, nombre de usuario

- (VAL.12) El módulo EDR tendrá la capacidad de evaluar la actividad típica del endpoint (baseline) de acuerdo con las técnicas MITRE y reportar cualquier desviación de la actividad típica mediante la generación de un nuevo incidente en la sección Incidentes en la consola de administración.
- (VAL.13) La solución deberá incluir un módulo de firewall personal del endpoint capaz de bloquear varias amenazas en la capa de red incluyendo la prevención de intrusiones como SYN flood, escaneo de puertos TCP y DUP, Smart ARP, Smart DNS, ICMP attack, entre otros.
- (VAL.14) La solución deberá incluir un módulo Host IPS capaz de bloquear varias amenazas en la capa de red incluyendo la prevención de movimientos laterales para varias categorías de malware.
- (VAL.15) La solución ofertada deberá ser capaz de incluir capacidades de XDR (Extended Detection and Response), bien sea en el momento de la adjudicación del contrato o de forma gradual e iterativa, durante la vigencia del periodo total de contratación. Por tanto, cada licitador deberá especificar qué tipo de capacidades XDR presenta la solución propuesta en tiempo de contratación o a futuro (definidas en el roadmap del producto). Se entiende por capacidades XDR la posibilidad de unificar y correlacionar la información proveniente de diferentes tecnologías (agentes en PC y servidores, tráfico de red, información de dispositivos de terceros como firewall de otros fabricantes, etc.), para facilitar la tarea de prevención, detección y análisis, y respuesta, evitando tener que desplegar y operar todas esas tecnologías por separado, con el esfuerzo en tiempo y coste que conlleva.
- (VAL.16) Soporte para Linux, Mac, Android e iOS.
- (VAL.17) Consola en castellano
- (VAL.18) Capacidad de aislamiento de los equipos con posibilidad de autorizar la conexión de algunas aplicaciones.
- (VAL.19) Posibilidad de importación masiva de reglas Yara o IoCs a través de formatos.
- (VAL.20) Servicio gestionado de clasificación 100% de las aplicaciones, ejecutables y librerías de los equipos de forma externa sin usar recursos locales de la máquina y sin necesidad de intervención del usuario con 3 modos de configuración: Audit, Hardening y Lock.
- (VAL.21) Trazabilidad de la actividad de amenazas detectadas hasta 365 días.
- (VAL.22) Soporte técnico de nivel 1, 2 y 3 (R&D) en castellano.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (VAL.23) Soporte de laboratorio en castellano
- (VAL.24) Centro de desarrollo en territorio nacional
- (VAL.25) Sistema de reducción de superficie de ataque con granularidad para auditar o bloquear herramientas involucradas en ataque de tipo living-off-the-land.
- (VAL.26) Servicio de validación e inclusión de indicadores de ataque de alta confianza.

Actualización, renovación y soporte licencias

Incluidos durante el periodo de garantía del suministro.

Servicios de soporte y/o mantenimiento

Incluidos durante el periodo de garantía del suministro.

Trabajos complementarios de instalación avanzados

Trabajos de instalación

Trabajos que permitan verificar que se cuenta con una instalación plenamente funcional e integrada en el Ayuntamiento, como los siguientes:

- La instalación de la solución EDR/XDR en un conjunto de servidores y dispositivos (endpoints) indicados por el Servicio O.S.IT., que permita verificar su correcto funcionamiento inicial. Si la solución propuesta lo oferta y se autoriza que parte de la solución se desplegué en la nube, estas tareas incluirán la correcta configuración de los componentes en la nube.
- La correcta integración con las herramientas de monitorización de seguridad del Ayuntamiento (SIEM, etc.), en la forma que especifique el Ayuntamiento. Estos trabajos deben contar con la verificación del Servicio de Organización, Sistemas e Innovación Tecnológica (O.S.IT) del Ayuntamiento para darse por satisfactoriamente realizado.
- Tareas de diseño, despliegue e integración de la solución contratada en el Ayuntamiento, tareas que comprenden la realización de una configuración personalizada para optimizar la detección de eventos, incluyendo las relativas a la integración de la solución con las herramientas existentes en el Ayuntamiento y aquellas relativas al CCN-CERT.
- Ajuste fino (“Fine Tuning”) de las herramientas instaladas para su correcta adaptación al ciclo actualizado del estado de la seguridad.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- Configuración y pruebas del adecuado reporte de la información y eventos relevantes desde el punto de vista de seguridad a los sistemas de monitorización de seguridad del Ayuntamiento de Barakaldo (SIEM, etc.).
- Transferencia de conocimiento a los Técnicos Municipales del Servicio de O.S.IT. relacionada con el proceso de instalación y configuración en el Ayuntamiento.
- (VAL.27) Despliegue de más elementos de los objeto indicados en este concepto.
- Las actuaciones realizadas deben asegurar la no interrupción del servicio operativo, por lo que las intervenciones se realizarán en las fechas y horarios autorizados, lo que podría incluir fines de semana y festivos.

Estimación de jornadas profesionales

Para la realización de los trabajos necesarios, se deberá indicar en la oferta técnica el mínimo de jornadas profesionales de arquitectos y consultores expertos en la solución ofertada para conseguir el objetivo y los requerimientos de este concepto.

Adicionalmente, el adjudicatario asignará al Ayuntamiento uno o varios técnicos de seguridad en horario 24x7 durante la garantía del suministro e implantación que tiene por objeto este concepto.

Al menos trimestralmente, el adjudicatario entregará un informe sobre trabajos ejecutados.

Condiciones de ejecución de los trabajos

Si la naturaleza de los trabajos lo requiere, éstos tendrán que ser realizados en las instalaciones del Ayuntamiento de Barakaldo en los horarios marcados por el Servicio O.S.IT.

Es posible la ejecución de tareas-trabajos en formato remoto cuando técnicamente sea viable, en este caso, serán por cuenta del adjudicatario las licencias de terceros necesarias para el control remoto securizado a nuestra infraestructura.

Entregables

El adjudicatario deberá proporcionar, al menos, los siguientes entregables en el ámbito de la instalación avanzada, que deberán ser validados por el Servicio O.S.IT. del Ayuntamiento para su aceptación:

- Elaboración de un Plan de Trabajo detallado.
- Documento de análisis y diseño incluyendo esquemas de arquitectura lógica y física.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- Documentación de instalación, parametrización y configuración
- Planes de pruebas realizadas y sus resultados.
- Plan de contingencia, detallando las actuaciones para llevarlo a cabo
- Manuales y otro material relacionado con la transferencia de conocimientos
- Informes periódicos de las actuaciones realizadas

La documentación se deberá mantener actualizada en el periodo de ejecución del objeto de este apartado, en todo caso estarán sujetas a las condiciones de planificación del proyecto indicadas por el Servicio de O.S.IT. del Ayuntamiento.

Documento que garantice la compatibilidad con las funciones existentes

La solución deberá mantenerse la integridad, compatibilidad con el resto de componentes de la Plataforma de Ciberseguridad que tiene por objeto general el presente pliego.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Concepto I.3 NAC Network Access Control

Descripción de los suministros

Para una mejora del control de la superficie de exposición del Ayuntamiento se requiere el suministro e implantación de una solución de control de acceso a la red (NAC) para garantizar el uso de dispositivos corporativos y prevenir la conexión de equipos no autorizados que puedan poner en riesgo la seguridad del Ayuntamiento. El sistema permitirá identificar el tipo de dispositivo que se quiere conectar a la red del Ayuntamiento y evaluar si cumple con los requisitos definidos para determinar si debe tener acceso a la red local o debe ser ubicado en una red provisional de remedio o únicamente de salida a Internet.

Objetivos

El suministro e implantación del NAC con licencia para el control de 650 dispositivos.

La garantía será como mínimo de un (1) año desde la el acta de recepción de este concepto o componente.

El suministro deberá contemplar todas las licencias (propias y de terceros) y su mantenimiento necesarias durante el plazo de garantía no suponiendo coste para el Ayuntamiento.

Requisitos

La solución propuesta para el NAC deberá contemplar los siguientes requisitos mínimos:

- (REQ.1) Los equipos ofertados deberán aparecer como certificados en categoría ALTA en la Guía de Seguridad de las TIC CCN-STIC-105 del CCN CERT (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion.html) en el apartado de productos cualificados, fijando como fecha de referencia para el cumplimiento de este requisito el último día del plazo de presentación de ofertas del presente concurso.
- (REQ.2) El sistema quedará completamente configurado, instalado y en pleno funcionamiento, en modalidad “Llave en mano”.
- (REQ.3) Suministro del hardware necesario para el funcionamiento de la solución, no en alta disponibilidad, para garantizar la continuidad de la misma, pero garantizando la continuidad del servicio ante la caída del servidor NAC. Sin necesidad de utilizar recursos del Ayuntamiento.
- (REQ.4) Permitirá flexibilidad en el despliegue mediante el uso de virtualización, será adaptable a las necesidades y requisitos del organismo y fácilmente escalable.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REG.5) El coste de la solución no debe verse afectado por la arquitectura final a implantar, sea cual sea el número de servidores virtuales requeridos finalmente en la implantación escogida.
- (REG.6) El soporte del fabricante deberá ser en castellano hasta el nivel 3 del mismo.
- (REG.7) La gestión de la plataforma debe ser a través de la interfaz gráfica 100% Web.
- (REG.8) Toda la comunicación entre la consola y el resto de nodos debe estar cifrada.
- (REG.9) Debe tener la posibilidad de desplegar cualquier arquitectura en HA (Alta Disponibilidad) sobre un número de servidores ilimitados, en cualquier arquitectura, físico, virtual o nube, o mezcla de ellas, sin ningún coste adicional.
- (REG.10) Se integrará con cualquier electrónica que soporte el estándar de autenticación 802.1x con capacidad para asignar VLANs dinámicamente (RFC3580).
- (REG.11) Deberá ser agnóstica a la electrónica de red actual o futura, para evitar ser forzados a usar proveedores de infraestructura específicos, permitiendo la integración de varios proveedores.
- (REG.12) La solución tendrá integración al menos con Directorio Activo (AD), Protocolo Ligero de Acceso a Directorios (LDAP), con cualquier servidor Radius estándar del mercado, y Doble Factor de Autenticación, autenticación con certificados, SSO mediante SAMLv2 actuando como IDP o SP, NGFW, SDWAN, MDMs o sistemas SIEM.
- (REG.13) Debe tener una integración nativa con las guías publicadas de bastionado de electrónica de red del CCN, basada en las reglas de la solución ROCIO del CCN-CERT
- (REG.14) Debe contar con un Procedimiento de empleo seguro publicado como guía del CCN-CERT y vigente.

Requerimientos funcionales y tecnológicos:

- (REQ.15) El descubrimiento de dispositivos (cuantificación de activos) se realizará a través de mecanismos pasivos (port mirroring / port span).
- (REQ.16) Se visibilizarán activos a través del modo denominado sensor, teniendo como fuente las capas 2 a 7 y realizando una inspección profunda de paquetes (DPI) de tráfico de red conectado a los puertos span y con visibilidad a los protocolos DNS, DHCP, FTP, HTTP, IRC, SMTP, SSH, SSL, etc.
- (REQ.17) Dispondrá de sensores que permitan la inspección y clasificación del tráfico de red que llega al nivel de aplicación (capa 7) y proveer de visibilidad sobre segmentos de red que no son administrados por el control de acceso.
- (REQ.18) Permitirá perfilamiento y clasificación de dispositivos conectados a la red (cualificación de activos).
- (REQ.19) El perfilado automático podrá ser extensible mediante la creación de atributos / características de los activos de manera manual (definidos por parte del administrador) y de manera dinámica.
- (REQ.20) El perfilado se realizará íntegramente sobre la misma solución, sin realizar peticiones a plataformas externas a la infraestructura del organismo.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.21) Capacidad de descubrimiento, perfilado y control hasta los dispositivos indicados.
- (REQ.22) Deberá permitir las agrupaciones lógicas de dispositivos (por ejemplo agrupación de dispositivos en función de la sede desde que acceden, agrupación de dispositivos en función de su criticidad,…).
- (REQ.23) Deberá permitir visibilidad del comportamiento de la red:
  - Flujos de comunicación.
  - Protocolos de red utilizados.
  - Estadísticas de comportamiento.
- (REQ.24) Deberá disponer de una CMDB de los activos de la red centralizado y extensible.
- (REQ.25) Permitirá la elaboración de informes y dashboards personalizables, alimentados por la CMDB y automatizables.
- (REQ.26) Deberá permitir visibilidad en tiempo real de todos los dispositivos conectados a la red de manera activa y/o pasiva.
- (REQ.27) Permitirá la integración de otras fuentes de información sobre los activos para enriquecer el CMDBs.
- (REQ.28) Incluirá el concepto CPE (Common Platform Enumeration) del estándar NIST.
- (REQ.29) Tendrá una base de tipos de dispositivos predeterminado.
- (REQ.30) Permitirá la creación de nuevos tipos de dispositivos.
- (REQ.31) Permitirá la creación de dashboards, sin límites, para visualizar la comunicación entre activos.
- (REQ.32) Permitirá crear agrupaciones, sin límites, de los activos en función de la lógica del Ayuntamiento.

A tener en cuenta y valorar

La solución propuesta para este concepto, en el caso que se contemplen, serán valoradas.

- (VAL.1) Integración o complemento con sistemas existentes en el Ayuntamiento, por ejemplo, Gestión de Activos PROACTIVANET
- (VAL.2) Propuesta de HA (alta disponibilidad) para este componente.
- (VAL.3) El escalado y crecimiento debe ser de forma horizontal de tal forma que para aumentar la capacidad global solo hagan falta añadir nodos adicionales.
- (VAL.4) Debe existir un único nodo de configuración del sistema y deberá sincronizar la configuración con el resto.

Actualización, renovación y soporte licencias

Incluidos durante el periodo de garantía del suministro.

Servicios de soporte y/o mantenimiento

Incluidos durante el periodo de garantía del suministro.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Trabajos complementarios de instalación avanzados

Trabajos de instalación

Trabajos que permitan verificar que se cuenta con una instalación plenamente funcional e integrada en el Ayuntamiento, como los siguientes:

- La instalación de la solución NAC, que permita verificar su correcto funcionamiento inicial. Si la solución propuesta lo oferta y se autoriza que parte de la solución se desplegué en la nube, estas tareas incluirán la correcta configuración de los componentes en la nube.
- La correcta integración con las herramientas de monitorización de seguridad del Ayuntamiento (SIEM, etc.), en la forma que especifique el Ayuntamiento. Estos trabajos deben contar con la verificación del Servicio de Organización, Sistemas e Innovación Tecnológica (O.S.IT) del Ayuntamiento para darse por satisfactoriamente realizado.
- Tareas de diseño, despliegue e integración de la solución contratada en el Ayuntamiento, tareas que comprenden la realización de una configuración personalizada para optimizar la detección de eventos, incluyendo las relativas a la integración de la solución con las herramientas existentes en el Ayuntamiento y aquellas relativas al CCN-CERT.
- Ajuste fino (“Fine Tuning”) de las herramientas instaladas para su correcta adaptación al ciclo actualizado del estado de la seguridad.
- Configuración y pruebas del adecuado reporte de la información y eventos relevantes desde el punto de vista de seguridad a los sistemas de monitorización de seguridad del Ayuntamiento de Barakaldo (SIEM, etc.).
- Transferencia de conocimiento a los Técnicos Municipales del Servicio de O.S.IT. relacionada con el proceso de instalación y configuración en el Ayuntamiento.
- Las actuaciones realizadas deben asegurar la no interrupción del servicio operativo, por lo que las intervenciones se realizarán en las fechas y horarios autorizados, lo que podría incluir fines de semana y festivos.

Estimación de jornadas profesionales

Para la realización de los trabajos necesarios, se deberá indicar en la oferta técnica el mínimo de jornadas profesionales de arquitectos y consultores expertos en la solución ofertada para conseguir el objetivo y los requerimientos de este concepto.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Condiciones de ejecución de los trabajos

Si la naturaleza de los trabajos lo requiere, éstos tendrán que ser realizados en las instalaciones del Ayuntamiento de Barakaldo en los horarios marcados por el Servicio O.S.IT.

Es posible la ejecución de tareas-trabajos en formato remoto cuando técnicamente sea viable, en este caso, serán por cuenta del adjudicatario las licencias de terceros necesarias para el control remoto securizado a nuestra infraestructura.

Entregables

El adjudicatario deberá proporcionar, al menos, los siguientes entregables en el ámbito de la instalación avanzada, que deberán ser validados por el Servicio O.S.IT. del Ayuntamiento para su aceptación:

- Elaboración de un Plan de Trabajo detallado.
- Documento de análisis y diseño incluyendo esquemas de arquitectura lógica y física.
- Documentación de instalación, parametrización y configuración
- Planes de pruebas realizadas y sus resultados.
- Plan de contingencia, detallando las actuaciones para llevarlo a cabo
- Manuales y otro material relacionado con la transferencia de conocimientos
- Informes periódicos de las actuaciones realizadas

La documentación se deberá mantener actualizada en el periodo de ejecución del objeto de este apartado, en todo caso estarán sujetas a las condiciones de planificación del proyecto indicadas por el Servicio de O.S.IT. del Ayuntamiento.

Documento que garantice la compatibilidad con las funciones existentes

La solución deberá mantenerse la integridad, compatibilidad con el resto de componentes de la Plataforma de Ciberseguridad que tiene por objeto general el presente pliego.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Concepto I.4 SIEM Security Information and Event Managemet

Descripción de los suministros

El adjudicatario deberá gestionar, administrar y procesa cualquier evento de seguridad relacionado con los productos a implementar dentro del presente contrato. Para realizar las funciones referidas, el adjudicatario deberá implementar una solución SIEM que permita la operación del SOC en los términos exigidos. Así, el contrato 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

Objetivos

El suministro e instalación de todas las licencias necesarias para implantar y gestionar una solución SIEM para el Ayuntamiento de Barakaldo.

La garantía será como mínimo de un (1) año desde la el acta de recepción de este concepto o componente.

El suministro deberá contemplar todas las licencias (propias y de terceros) y su mantenimiento necesarias durante el plazo de garantía no suponiendo coste para el Ayuntamiento.

Requisitos

La solución propuesta para el SIEM debe cumplir los siguientes requisitos mínimos:

- (REQ.1) Los equipos ofertados deberán aparecer como certificados en categoría MED IA en la Guía de Seguridad de las TIC CCN-STIC-105 del CCN CERT (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion.html) en el apartado de productos cualificados, fijando como fecha de referencia para el cumplimiento de este requisito el último día del plazo de presentación de ofertas del presente concurso.
- (REQ.2) Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma Common Criteria: *(Perfiles de protecc6n Common Criteria – CCn STIC 140 Anexo B.6 pt 4.1)*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices[1]	2.2e	27/03/2020	CCDB
Collaborative Protection Profile for Network Devices[2]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[3]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.4	1.0	27/02/2015	CCDB

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

- (REQ.3) La solución deberá atender a un numero de 5 fuentes (FW, Antivirus-EDR, Directorio Activo, DHCP/DNS y NAC)
- (REQ.4) La solución SIEM deberá permitir la ingesta de al menos 1000 EPS (eventos por segundo), permitiendo su ampliación hasta 5.000 EPS sin necesidad de cambios de equipamiento.
- (REQ.5) Herramienta dimensionada para la ingesta de la infraestructura mínima de seguridad municipal, pudiendo soportar picos puntuales de ingesta de mayor magnitud sin pérdida de servicio.
- (REQ.6) Soporte del fabricante en 8x5 y niveles 1, 2 y 3 en castellano.
- (REQ.7) Debe permitir la asistencia insitu de lunes a viernes de personal de nivel 3 del fabricante en España para resolución de incidencias graves en la herramienta.
- (REQ.8) Arquitectura robusta y escalable que permita el crecimiento según se necesite.
- (REQ.9) Disposición de un conjunto suficiente de conectores, reglas de correlación y alertas para integrar, al menos los siguientes sistemas:
    - Firewall, WAF, IPS, antivirus/EDR, proxy, NAC, controladores de dominio, puestos de usuario, servidores críticos, etc. La solución SIEM propuesta permitirá la ingesta de al menos 15 tipos de fuentes diferentes si fuese necesario.
- (REQ.10) 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 (para poder revisar la publicación de IOC en los 2 meses anteriores y saber si el Ayuntamiento se ha visto afectado). 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, detección y respuesta óptimo y adaptado al contexto del Ayuntamiento. En cuanto a las fuentes a integrar desde el inicio del contrato, estas se determinarán durante la fase de implantación tras la realización de un análisis inicial y se seguirá un enfoque gradual.
- (REQ.11) La solución SIEM propuesta dispondrá de más de 6.000 reglas y deberá permitir que al menos 300 de estas reglas funcionen de forma simultánea. Se deberá acreditar al arranque del proyecto el número de reglas activas.
- (REQ.12) 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.
- (REQ.13) La solución deberá contar con una integración nativa con la solución NAC propuesta.
- (REQ.14) El producto no almacenará ninguna credencial en claro en memoria no volátil.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.15) 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.
- (REQ.16) La solución propuesta deberá contar con una copia de seguridad diaria del conjunto total de logs ingestados para asegurar su disponibilidad y cubrir posibles contingencias que pudieran suponer una pérdida de los registros. Dicho backup 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.
- (REQ.17) Solución específica orientada a proteger las infraestructuras de directorio activo de los clientes. Aporta visión desde un punto de vista proactivo, reactivo y como herramienta forense todo incluido en una única licencia y en una consola única.
- (REQ.18) Solución no intrusiva en la medida que no necesita desplegar cuentas privilegiadas con lo cual no se aumenta el riesgo por desplegar la solución ni tiene ningún impacto en la infraestructura ni en su rendimiento.
- (REQ.19) Herramienta de monitorización en tiempo real frente a la visión tradicional de las auditorias. En la medida que el directorio activo está en continuo cambio la única manera de garantizar una seguridad continua es monitorizar y analizar en tiempo real todos los cambios que se producen en el AD.
- (REQ.20) La solución incluirá un motor de detección de ataques en tiempo real a través de los Indicadores de Ataque (IoA) y siguiendo la estructura (framework) de Mitre. Se indicará la fuente, desde qué máquina se ha hecho el ataque, con qué cuenta y contra qué Controlador de Dominio.
- (REQ.21) Herramienta forense que permita almacenar todos los cambios que se han producido en el AD y correlacionar la información para las fases de investigación y respuesta ante ataques.
- (REQ.22) KPIs y cuadros de mando (dashboards) claros y fáciles de configurar para mostrar el nivel de riesgo del AD y como va evolucionando su seguridad y refuerzo en el tiempo.
- (REQ.23) La herramienta debe contar con capacidad ilimitada del número de usuarios de operación sin que afecte en coste a la licencia suministrada.
- (REQ.24) El fabricante proporcionará actualizaciones periódicas que incluirán nuevas reglas de correlación, casos de uso, informes y alertas predefinidos y documentados por fabricante.
- (REQ.25) La herramienta debe ser capaz de agrupar incidentes relacionados en un único incidente, aunque los eventos estén separados en el tiempo por horas o días.
- (REQ.26) La herramienta debe detectar y reconocer automáticamente las fuentes syslog más comunes.
- (REQ.27) La herramienta debe contar con capacidad ilimitada del número de usuarios de operación sin que afecte en coste a la licencia suministrada.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.28) Para su integración en la Red Nacional de SOC, la solución dispondrá de una API para la federación con el CCN, con el fin de poder monitorizar las alertas de seguridad de peligrosidad Alta, Muy Alta y Critica, según la norma CCN-STIC 817 de Gestión de Incidentes.

A tener en cuenta y valorar

La solución propuesta para este concepto, en el caso que se contemplen, serán valoradas.

- (VAL.1) Integración o complemento con sistemas existentes en el Ayuntamiento, por ejemplo, Gestión de Activos PROACTIVANET. Sistema integrado de alerta temprana de vulnerabilidades con capacidad emitir alertas por correo electrónico y de generación de eventos en tiempo real en el SIEM para cada vulnerabilidad descubierta en los activos inventariados en el módulo de gestión de activos.
- (VAL.2) Consola web en formato HML5 que permita su ejecución en cualquier plataforma compatible, sin necesidad de sistemas propietarios del fabricante.
- (VAL.3) Que la licencia del fabricante permita crecer en EPS, o usuarios que utilicen la consola sin coste adicional, de manera que la ciberseguridad del Ayuntamiento no se vea comprometida.
- (VAL.4) Se valorará la integración de la información en tiempo real y forense de manera nativa y no requiera de add ons adicionales o componentes separados, que perjudiquen la interacción de los usuarios respecto a la información en tiempo real y forense.
- (VAL.5) Capacidad de desarrollos a medida del Ayuntamiento para integración con aplicativos propietarios, herramientas de ticketing y soluciones EDR.
- (VAL.6) Deberá permitir el almacenamiento configurable de datos históricos que permita fijar el volumen o la antigüedad de los datos histórico en función de las necesidades del Ayuntamiento de Barakaldo.
- (VAL.7) La herramienta debe ofrecer casos de uso predefinidos mantenidos y documentados por el fabricante.
- (VAL.8) La herramienta debe ofrecer informes predefinidos mantenidos y documentados por el fabricante.
- (VAL.9) El fabricante proporcionará actualizaciones periódicas que incluirán nuevas reglas de correlación, casos de uso, informes y alertas predefinidos y documentados por fabricante.
- (VAL.10) La herramienta debe ser personalizable, permitiendo crear, como mínimo, vistas, gráficos, filtros y cuadros de mando personalizados.
- (VAL.11) La herramienta debe permitir analizar el comportamiento del usuario (UEBA).
- (VAL.12) La herramienta debe permitir realizar consultas avanzadas mediante combos o lenguaje tipo SQL.
- (VAL.13) La herramienta debe incorporar de manera nativa y sin soluciones terceras adicionales de capacidades de análisis de comportamiento (behavioural analytics).

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

- (VAL.14) La herramienta debe incorporar de manera nativa y sin soluciones terceras adicionales de capacidades de detección de anomalías y funcionalidades XDR.
- (VAL.15) La herramienta debe permitir incorporar LUCIA como plataforma de gestión de tickets bidireccional con el CCN-CERT.
- (VAL.16) La herramienta debe permitir incorporar REYES como plataforma de feeds de inteligencia con datos sobre amenazas de seguridad que utilice posteriormente en sus correlaciones y búsquedas de eventos de seguridad.
- (VAL.17)La herramienta debe permitir la recolección de logs utilizando diferentes protocolos (a modo de ejemplo, syslog, TLS Syslog, Syslog mixtilínea, SNMPv3, SMB, SCP/SFTP, WMI, MSRPC, API…).
- (VAL.18) La herramienta debe contar con capacidad ilimitada de crecimiento de EPS o ingesta de volumen de logs diarios sin que afecte en coste a la licencia suministrada.
- (VAL.19) La herramienta debe contar con capacidad de compartir información de forma federada con instancias jerárquicas superiores, de acuerdo a la estrategia de federación del CCN para la RNS, incluido en la licencia.
- (VAL.20) La plataforma debe incluir un servicio de alerta temprana de vulnerabilidades, tanto a nivel de infraestructura como de aplicaciones, que permita mantener un inventario de vulnerabilidades con actualización, como mínimo, diaria que permita contrastar la evolución de dichas brechas de seguridad.

Actualización, renovación y soporte licencias

Incluidos durante el periodo de garantía del suministro.

Servicios de soporte y/o mantenimiento

Incluidos durante el periodo de garantía del suministro.

Trabajos complementarios de instalación avanzados

Trabajos de instalación

Trabajos que permitan verificar que se cuenta con una instalación inicial plenamente funcional e integrada en el Ayuntamiento, como los siguientes:

- La instalación de la solución SIEM en el conjunto de servidores indicados, que permita verificar su correcto funcionamiento inicial. Si la solución propone despliegue en la nube de algún componente, estas tareas incluirán la correcta configuración de los componentes en la nube.
- La correcta integración con las herramientas de monitorización de seguridad de3l resto del proyecto (EDR, SIEM, etc.). Estos trabajos deberán contar con la verificación del Servicio O.S.IT. para darse por satisfactoriamente realizados.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

- Tareas de diseño, despliegue e integración de la solución contratada en el Ayuntamiento, tareas que comprenden la realización de una configuración personalizada para optimizar la detección de eventos, incluyendo las relativas a la integración de la solución con las herramientas existentes en el Ayuntamiento y aquellas relativas al CCN-CERT.
- Ajuste fino ("Fine Tuning") de las herramientas instaladas para su correcta adaptación al ciclo actualizado del estado de la seguridad.
- Configuración y pruebas del adecuado reporte de la información y eventos relevantes desde el punto de vista de seguridad a los sistemas de monitorización de seguridad del Ayuntamiento de Barakaldo (EDR, SIEM, etc.).
- Transferencia de conocimiento a los Técnicos Municipales del Servicio de O.S.IT. relacionada con el proceso de instalación y configuración en el Ayuntamiento.
- Las actuaciones realizadas deben asegurar la no interrupción del servicio operativo, por lo que las intervenciones se realizarán en las fechas y horarios autorizados, lo que podría incluir fines de semana y festivos.

Estimación de jornadas profesionales

Para la realización de los trabajos necesarios, se deberá indicar en la oferta técnica el mínimo de jornadas profesionales de arquitectos y consultores expertos en la solución ofertada para conseguir el objetivo y los requerimientos de este concepto.

Al menos mensualmente el adjudicatario entregará un informe sobre trabajos ejecutados.

Condiciones de ejecución de los trabajos

Si la naturaleza de los trabajos lo requiere, éstos tendrán que ser realizados en las instalaciones del Ayuntamiento de Barakaldo en los horarios marcados por el Servicio O.S.IT.

Es posible la ejecución de tareas-trabajos en formato remoto cuando técnicamente sea viable, en este caso, serán por cuenta del adjudicatario las licencias de terceros necesarias para el control remoto securizado a nuestra infraestructura.

Entregables

El adjudicatario deberá proporcionar, al menos, los siguientes entregables en el ámbito de la instalación avanzada, que deberán ser validados por el Servicio O.S.IT. del Ayuntamiento para su aceptación:

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- Elaboración de un Plan de Trabajo detallado.
- Documento de análisis y diseño incluyendo esquemas de arquitectura lógica y física.
- Documentación de instalación, parametrización y configuración
- Planes de pruebas realizadas y sus resultados.
- Plan de contingencia, detallando las actuaciones para llevarlo a cabo
- Manuales y otro material relacionado con la transferencia de conocimientos
- Informes periódicos de las actuaciones realizadas

La documentación se deberá mantener actualizada en el periodo de ejecución del objeto de este apartado, en todo caso estarán sujetas a las condiciones de planificación del proyecto indicadas por el Servicio de O.S.IT. del Ayuntamiento.

Documento que garantice la compatibilidad con las funciones existentes

La solución deberá mantenerse la integridad, compatibilidad con el resto de componentes de la Plataforma de Ciberseguridad que tiene por objeto general el presente pliego.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Concepto I.5 Garantía del SOC

Descripción de los suministros

El adjudicatario pondrá en marcha, operará y llevará a cabo el mantenimiento y soporte de las soluciones que se incluyen en el presente Capítulo I para la detección y prevención de incidentes de seguridad mediante un Centro de Operaciones de Seguridad (SOC), incluyendo todas las licencias y costes que sean necesarias para su funcionamiento.

Objetivos

Ejecución de la garantía que será como mínimo de un (1) año desde la el acta de recepción del suministro que tiene por objeto los componentes desarrollados en el Capítulo I.

Requisitos

La solución propuesta debe cumplir los siguientes requisitos mínimos:

- (REQ.1) Detectar y prevenir intrusiones en cualquier protocolo y aplicación utilizados.
- (REQ.2) No repercutir en una degradación del rendimiento de las aplicaciones y servicios.
- (REQ.3) Integrar su información generada como fuentes a monitorizar por parte del Centro de Operaciones de Ciberseguridad.
- (REQ.4) Monitorización en tiempo real de los eventos de la organización 24x7. El servicio se dará con cobertura 24x7, con al menos 3 niveles de escalado técnico.
- (REQ.5) Detección temprana y respuesta ante incidentes.
- (REQ.6) Ciberinteligencia para la detección de indicadores de ataques (IoA) e indicadores de compromiso (IoC).
- (REQ.8) Contará con una única consola centralizada, incluyendo paneles personalizables y con acceso por parte del Ayuntamiento.
- (REQ.9) Proporcionará respuesta ante incidentes, incluyendo análisis de causa raíz, gestión con terceros, comunicados, remediación y verificación de seguridad tras restablecimiento
- (REQ.10) Los sistemas de información que permiten la prestación de los servicios deberán disponer de la conformidad con el Esquema Nacional de Seguridad en categoría ALTA. La conformidad deberá de mantenerse vigente durante todo el ciclo de vida del proyecto. En caso de adscribir por medios externos, el Centro de Operaciones de Seguridad deberá de disponer de la misma categoría (ALTA).
- (REQ.11) Proporcionar servicios de Caza de amenazas o Threat Hunting.
- (REQ.12) Integración con la solución de EDR. Detección de anomalías en puesto de usuario.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.13) Análisis de eventos basado en firmas, comportamientos, logs, procesos e IOCs.
- (REQ.14) Técnicas de Inteligencia Artificial (IA) para la detección de anomalías mediante el uso de Machine Learning.
- (REQ.15) Desarrollo de reglas de alerta adaptadas a la particularidad del Ayuntamiento.
- (REQ.16) Centralización, salvaguarda y correlación de eventos multifuente.
- (REQ.17) Sistema de detección de intrusiones a nivel de red.
- (REQ.18) Integración de eventos de seguridad de servicios externos vía syslog/api.
- (REQ.19) La empresa encargada de la explotación del SOC deberá formar parte de la comunidad CSIRT.es y estar integrada dentro de la Red Nacional de Centros de Operaciones de Ciberseguridad -Red Nacional de SOC (RNS GOLD), estableciendo para ello el licitador los contactos correspondientes con el resto de SOCs integrantes.
- (REQ.20) El Centro de Operaciones de Ciberseguridad estará ubicado y operado desde España. La empresa beneficiaria de la explotación de éste deberá formar parte de la comunidad CSIRT.ES y de la Red Nacional de SOC. Esta información se contrastará con el Centro Criptológico Nacional (CCN).
- (REQ.21) Desde el Centro de Operaciones se deberá proveer y gestionar un servicio de soporte ante las alertas generadas por los diferentes sistemas de seguridad y por los usuarios de la red corporativa. El adjudicatario realizará la contención o mitigación de los posibles ataques o incidencias de seguridad en los activos del Ayuntamiento.
- (REQ.22) El SOC deberá analizar todas las alertas generadas, descartando falsos positivos, transmitiendo al Ayuntamiento el diagnóstico cuanto antes y bloqueando el ataque de forma proactiva en caso de que se ponga en riesgo la seguridad de los activos o las infraestructuras que los soportan.
- (REQ.23) Asimismo, actuará como punto de contacto con el Ayuntamiento para la operación de los servicios incluidos en el presente pliego, supervisará el estado de los activos y generará las alertas correspondientes en caso de eventos que puedan afectar a la seguridad de la información.
- (REQ.24) Reunión mensual de seguimiento del servicio, análisis de eventos, definición de nuevas reglas de alerta, nuevos casos de uso, etc.
- (REQ.25) La empresa encargada de la explotación del SOC deberá formar parte de la comunidad CSIRT.es y estar integrada dentro de la Red Nacional de Centros de Operaciones de Ciberseguridad (Red Nacional de SOC), estableciendo para ello el licitador los contactos correspondientes El adjudicatario del contrato deberá proporcionar, mantener y operar una solución de protección del dominio que permita la gestión de los mecanismos de defensa (prevención, detección y reacción) ante ataques dirigidos o que puedan afectar al directorio activo. La solución deberá cumplir con los siguientes requisitos mínimos.
- (REQ.26) Monitorización continua del directorio activo frente ataques como escalado de privilegios, suplantación de identidad, fuerza bruta, DCShadow, Password Spraying y DCSync entre otras.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- (REQ.27) Recopilación de las evidencias que puedan servir de base para un análisis forense tras la materialización de una amenaza que haya impactado contra el directorio activo.

A tener en cuenta y valorar

- (VAL.1) A lo largo del contrato el SOC deberá incorporar progresivamente nuevas fuentes de posibles soluciones de ciberseguridad que adquiera el Ayuntamiento

Entregables

El adjudicatario deberá presentar Informe mensual de estado con indicadores.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Concepto I.6 Herramientas del CCN-CERT

Dado que el enfoque del proyecto está alineado con la Estrategia Nacional de Ciberseguridad, el aspecto más sostenible es la implantación de soluciones propias del CCN contribuyendo a la reutilización de herramientas comunes como:

Concepto I.6.1 Implantación LUCIA

Implantación de la herramienta de gestión de incidentes LUCIA del CCN-CERT, operando de modo federado con la plataforma estatal, y su integración con las aplicaciones internas de gestión de incidentes del área informática del Ayuntamiento.

Concepto I.6.2 Implantación MICROCLAUIDIA

Implantación de la herramienta microCLAUDIA del CCN-CERT en todos los puestos del Ayuntamiento (650).

El adjudicatario deberá proporcionar procedimiento de despliegue automatizado y asistir técnicamente a la Sección de Sistemas del Servicio de O.S.IT. para la ejecución y actualización de la herramienta cuando sea necesario durante la ejecución del contrato.

Concepto I.6.3 Implantación de sonde SAT-INET

Implantación de la sonda SAT-INET (sistema de alerta temprana) del CCN-CERT para la vigilancia del perímetro.

Concepto I.6.4 Implantación de REYES/MISP

Implantación de la plataforma MISP y/o REYES para el intercambio de información de amenazas y ciber inteligencia y su integración con las plataformas de seguridad del Ayuntamiento.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

CAPITULO II: Mantenimiento por dos (2) años de la plataforma implantada

Objetivos y alcance

El objetivo incluye todos los servicios de asistencia, monitorización y gestión de los suministros e instalaciones correspondientes al Capítulo I de este pliego. Durante el plazo de dos (2) años más una posible prórroga de un (1) año o hasta nueva adjudicación del servicio.

Servicios que comenzarán a ejecutarse a la finalización de la garantía de los componentes detallados en el Capítulo I.

El objetivo de este Capítulo II es que el Ayuntamiento de Barakaldo alcance unos niveles de seguridad suficientes para prevención, detección y gestión de amenazas de manera eficiente.

El servicio de ciberseguridad (SOC) gestionará los eventos de seguridad mediante el uso de la información generada por las herramientas instaladas en el Capítulo I así como otras ya disponibles del Ayuntamiento.

Durante toda la duración del contrato, el adjudicatario, de acuerdo con el personal del Ayuntamiento, realizará un proceso de ajuste y mejora continua de las herramientas y procesos de monitorización y gestión de la seguridad para adaptarse a las cambiantes situaciones en el campo de la ciberseguridad.

El adjudicatario se hará cargo durante la ejecución del contrato de gestionar las licencias y garantías de todos los componentes que conforman la plataforma de ciberseguridad resultante de la implantación que tiene objeto el Capítulo I del pliego.

El adjudicatario asignará al Ayuntamiento uno o varios operadores y analistas de seguridad. Dichos técnicos se encargarán de procurar las tareas que el Ayuntamiento demande en esta fase, como servicios de soporte y mantenimiento de las distintas plataformas y herramientas, la preparación de informes personalizados, investigaciones avanzadas y análisis de situaciones y el contexto de amenazas sobre los trabajos ejecutados, monitorización 24x7 de la seguridad de los sistemas, respuesta a incidentes de seguridad, etc.

Estos servicios se requieren en moda y forma “compartida”, es decir, que no se requiere exclusividad del servicio para el Ayuntamiento de Barakaldo si no al contrario, compartirlo con otras entidades con el mismo objetivo con el fin de aprovechar sinergias.

Requisitos

Se encuentran incluidos las siguientes tareas:

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

- (REQ.1) Configuración y pruebas del adecuad o reporte de información y eventos relevantes desde el punto de vista de seguridad a los sistemas de seguridad del Ayuntamiento (SIEM, EDR/XDR, NDR, NAC, etc.).

- (REQ.2) Ajuste fino ("fine tuning") de las herramientas instaladas para su correcta adaptación al ciclo actualizado del estado de seguridad.

- (REQ.3) Notificación y revisión de las alertas generadas por los motores del SIEM, EDR/XDR, etc. Por un/una analista de seguridad de la adjudicataria, como paso previo al envio al ayuntamiento. Esto permitirá, dentro de lo posible, con un importante nivel de acierto, la eliminación de falsos positivos en la identificación de incidentes y permitirá comprobar el correcto funcionamiento de las distintas plataformas a lo largo de la duración de este contrato.

- (REQ.4) En general, las tareas de monitorización, administración y soporte, basada en la operación remota delegada de los dispositivos y soluciones de seguridad del Ayuntamiento de Barakaldo incluidos en esrte proyecto. Esta administración delegada se hará desde un Centro de Operaciones de Ciberseguridad (SOC).

- (REQ.5) Realización de las actividades de capacitación y concienciación en ciberseguridad.

Condiciones de ejecución del servicio del SOC 24x7

Si la naturaleza de los trabajos lo requiere, estos se harán en las instalaciones del Ayuntamiento.

Las actuaciones realizadas aseguraran la no interrupción de los servicios del Ayuntamiento, por lo que las intervenciones se harán en fechas y horarios autorizados, lo que puede incluir fines de semana y festivos.

Los registros de logs no se enviarán directamente desde los sistemas, si no que se emplearán elementos intermedios (colectores) proporcionados por la adjudicataria e instalados en la infraestructura propuesta en el Capítulo I de este pliego.

Los datos o meta datos de los usuarios o de los sistemas de información del ayuntamiento recogidos y almacenados por las plataformas y soluciones propuestas deberán mantenerse dentro del ámbito geográfico y legal de la UE, así como la ejecución de los servicios sobre los mismos deben realizarse en el marco de la UE, para de este modo, garantizar el cumplimiento con la legislación y garantizar la confidencialidad de los datos de los usuarios y cualquier otra información del ayuntamiento.

Cuanto menos, de forma trimestral, el gestor técnico designado por el adjudicatario entregará un informe sobre los trabajos ejecutados.

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Niveles de servicio

Es necesario especificar los siguientes acuerdos de nivel de servicio (ANS-SLA). Los ANS permiten obtener indicadores para evaluar el grado de cumplimiento del servicio. El cálculo el ANS tendrá que hacerse por parte de la empresa adjudicataria.

Indicadores de Servicio

Se definen indicadores para cada una de las actividades del servicio objeto:

- Servicio de gestión de incidentes
- Servicio de atención a consultas y soporte técnico de aplicaciones
- Servicio de mantenimiento correctivo (problemas)
- Servicio de mantenimiento evolutivo/adaptivo y nuevo desarrollo

Para cada indicador se detallan una serie de campos:

- **Catalogación caso / Tipo mantenimiento**: atributo que identifica el indicador
- **Tiempos objetivo**: límite temporal para el cumplimiento del indicador entendiendo por:
    - **Tiempo de resolución**: tiempo transcurrido desde la petición de una consulta o soporte técnico hasta que se entrega la respuesta definitiva que cierra el caso
    - **Tiempo de primera respuesta**: Tiempo transcurrido desde el alta de la petición hasta que esta ésta se acepta.
      El tiempo de primera respuesta de una petición tiene como objetivo:
        - confirmar la recepción de la petición
        - realizar un análisis preliminar
        - comunicar una primera valoración y planificación con fecha de resolución
    - **Desviación sobre planificación:** Tiempo transcurrido desde la fecha estimada de entrega hasta que ésta se resuelve satisfactoriamente (fecha real de entrega)
- **Periodicidad**: Frecuencia de cálculo del indicador
- **Objetivo**: Valor fijado como objetivo para el indicador. El cálculo del valor objetivo se aplicará sobre el total de peticiones dadas de alta en el periodo.

Un atributo de catalogación importante es la urgencia o criticidad (prioridad), que influye sobre los tiempos de resolución requeridos y los indicadores de nivel de servicio asociados.

Sus valores son:

- **Bloqueante**: toda aquella incidencia que bloquea el trabajo del usuario impactando gravemente sobre el negocio o la imagen del Ayuntamiento de Barakaldo. Requiere de una intervención inmediata e interrumpida hasta su resolución definitiva y debe ser solucionada en el momento.
- **Critica**: toda aquella incidencia que no bloquea el trabajo del usuario en el momento en el que se produce, pero que requiera una resolución rápida, ya que puede suponer una parada en el flujo de trabajo posterior, y que además impacta sobre la imagen del Ayuntamiento.

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

- **Importante**: toda aquella incidencia que no bloquea el trabajo del usuario en el momento en el que se produce, que no impacta sobre el negocio o la imagen del ayuntamiento., pero que impiden la ejecución normal de una o más partes de la aplicación objeto del Servicio o de otras con las que se relaciona.
- **Normal**: incidencias que no impactan sobre el negocio o la imagen del Ayuntamiento y no impiden el funcionamiento normal de la aplicación

La prioridad de las incidencias podrá ser modificada por el Servicio de Organización, Sistemas e Innovación Tecnológica del Ayuntamiento de Barakaldo tras su revisión.

Los niveles de servicio indicados serán objeto de penalización en el caso de incumplimiento durante la ejecución, se especifican en las siguientes tablas.

Servicio de gestión de incidentes.

Catalogación uso	Tiempo máximo resolución (máximo)	Periodicidad	Objetivo
Todos	Al momento	Mensual	>= 99 %

Atención a consultas y soporte técnico de aplicaciones

Catalogación uso	Tiempo máximo resolución (máximo)	Periodicidad	Objetivo
Importante	4 horas	Mensual	>= 95 %
Normal	16 horas	Mensual	>= 95 %

Mantenimiento correctivo (problemas)

Catalogación uso	Tiempo máximo resolución (máximo)	Periodicidad	Objetivo
Bloqueante	2 horas	Mensual	>= 95 %
Critica	4 horas	Mensual	>= 95 %

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H

ZKIA./NÚM. 2023/001653
DATA/FECHA 20/02/2023
ALKATEAREN DEKRETU LIBURUA
LIBRO DE DECRETOS DE ALCALDIA

GOBIERNO DE ESPAÑA MINISTERIO DE POLITICA TERRITORIAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

Importante	8 horas	Mensual	>= 95 %
Normal	16 horas	Mensual	>= 95 %

Mantenimiento evolutivo / adaptativo y nuevo desarrollo

Catalogación uso	Tiempo máximo resolución (máximo)	Periodicidad	Objetivo
Critica	4 horas	Mensual	>= 95 %
Importante	16 horas	Mensual	>= 90 %
Normal	24 horas	Mensual	>= 90 %

Tipo mantenimiento	Desviación sobre planificación	Periodicidad	Objetivo
Evolutivo / adaptativo	Máximo 15 %	Mensual	>= 90 %
Nuevo desarrollo	Máximo 15 %	Trimestral	>= 90 %

Para la obtención de estos indicadores se requiere un mínimo de 5 casos de lo contrario, se acumularan durante los meses que será necesario hasta alcanzar ese mínimo, procediéndose a aplicar el resultado final a todo el periodo contabilizado.

En Barakaldo,

EL JEFE DE ORGANIZACIÓN, SISTEMAS E INNOVACIÓN TECNOLOGICA en funciones.

Luis Alberto Méndez de Andrés

[Firmado electrónicamente]

Fecha: 2023.02.15 08:26:19 +01'00'

Herriko Plaza, 1 • 48901 BARAKALDO • Tel.: 944789100 • e-mail: ayuntamiento@barakaldo.eus • http://www.barakaldo.eus • F.I.K./C.I.F. P - 48 - 01700 - H