# PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS DE CIBERSEGURIDAD Y LA ADQUISICIÓN DE UN CORTAFUEGOS PARA EL ORGANISMO DE GESTIÓN TRIBUTARIA DE LA DIPUTACIÓN DE BARCELONA.

Expediente núm.: ORGT/2025/0035517

## CONTINGUT

## 1. OBJECTO.

El Organismo de Gestión Tributaria de la Diputación de Barcelona (ORGT) es un organismo autónomo local de la Diputación de Barcelona, dotado de personalidad jurídica propia, que tiene como finalidad principal el ejercicio de las funciones y potestades de gestión, inspección y recaudación de tributos y otros ingresos de derecho público por delegación o encargo de gestión de las administraciones públicas de Cataluña y de los entes públicos que dependen de ellas.

Uno de los objetivos de ORGT es alcanzar un buen nivel de ciberseguridad, que maximice la disponibilidad de sus servicios y la autenticidad, confidencialidad, integridad y trazabilidad de la información que almacena, procesa y transmite. Para lograrlo, es necesario mejorar el nivel actual de ciberseguridad de ORGT ampliando la monitorización de la ciberseguridad, la detección temprana de incidentes, el análisis de las amenazas y vulnerabilidades, y optimizando la capacidad de detección, contención, erradicación y recuperación ante cualquier posible incidente.

El objeto de esta licitación es:

- Contratar un servicio de Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés *Security Operations Center*) con capacidades de Equipo de Respuesta a Incidentes (CSIRT, por sus siglas en inglés *Computer Security Incident Response Team*) que proporcione servicios de seguridad gestionada al ORGT.
- Actualizar la solución actual de detección y respuesta a incidentes (EDR, por sus siglas en inglés *Endpoint Detection and Response*), denominada Cortex XDR, hacia la solución de gestión, monitorización y automatización de procesos de Ciberseguridad, denominada Cortex XSIAM.
- Implantar un servicio de cortafuegos de aplicaciones web (WAF, por sus siglas en inglés *Web Application Firewall*), para proteger la sede electrónica del ORGT.
- Implantar un servicio de gestión de accesos privilegiados (PAM, por sus siglas en inglés *Privileged Access Management*).
- Implantar un servicio de concienciación en ciberseguridad para los empleados del ORGT.
- Renovar el cortafuegos perimetral PA3220 a la nueva versión comercial PA3410.

## 2. SITUACIÓN ACTUAL.

Para llevar a cabo sus funciones, el ORGT dispone de una infraestructura informática y de comunicaciones redundante, alojada en los dos centros de procesamiento de datos (CPD) situados en la ciudad de Barcelona y que trabajan en modo activo-pasivo.

El ORGT da servicio a 1.000 empleados distribuidos en una red de unas 100 oficinas interconectadas con los dos Centros de Procesamiento de Datos (CPD) mediante líneas de comunicaciones de alta velocidad, a 4.000 usuarios de los ayuntamientos (400 de ellos simultáneos) que acceden a través de internet a la aplicación de gestión tributaria, y a los contribuyentes de los municipios de la provincia de Barcelona que acceden a la sede electrónica del ORGT.

Todas las comunicaciones están protegidas por un doble cortafuegos de nueva generación de diferentes fabricantes. El cortafuegos interno es un clúster de 2 nodos PA3220 (con nombre FWORGT), del fabricante Palo Alto Networks, que está alojado en los CPD del ORGT, y el externo es un clúster de 2 nodos Fortigate FG6301F del fabricante FortiNet (con nombre FWVDF), alojado en la nube y gestionado por el operador de comunicaciones.

El ORGT comparte con la Diputación de Barcelona (DiBa) un sistema para evitar ataques de denegación de servicio (antiDDoS, por sus siglas en inglés *Distributed Denial of Service*), que también se encuentra alojado en la nube del operador de comunicaciones.

El cortafuegos interno FWORGT interconecta 11 redes mediante un agrupamiento de 2 interfaces de 10Gbps. Su política de seguridad está formada por 600 reglas de seguridad, 200 reglas de traducción de direcciones y 6 túneles IPSEC.

El cortafuegos FWORGT dispone de las siguientes suscripciones, que finalizan su vigencia el 28/09/26:

- Advanced URL Filtering
- Advanced DNS Security
- GlobalProtect
- Advanced Threat Prevention
- Advanced Wildfire

Los servicios del ORGT se ofrecen desde 150 servidores virtualizados con sistema operativo Windows Server 2012R2 o superior, que se ejecutan en hipervisores

VmWare Vsphere ESXi 8.0 U3. Los servidores están protegidos contra software malicioso mediante el EDR Cortex XDR, del fabricante Palo Alto Networks.

Los puestos de trabajo del ORGT son 1.000 portátiles que se conectan a una de las 2.000 sesiones de escritorios virtuales (VD, por sus siglas en inglés *Virtual Desktop*) que se ejecutan en hipervisores VmWare Vsphere ESXi 8.0 U3. Mil sesiones se ejecutan en el CPD activo y las otras mil están en reposo en el CPD pasivo, esperando dar servicio en caso de contingencia. Los VD son no persistentes y tienen instalado el EDR Cortex XDR.

El ORGT dispone de dos sondas de red que permiten detectar actividad maliciosa en el tráfico de datos de la red de área local (LAN, por sus siglas en inglés *Local Area Network*) de servidores y en la red LAN de la zona desmilitarizada (DMZ, por sus siglas en inglés *Demilitarized Zone*).

El ORGT tiene contratado un SOC que realiza las siguientes tareas:

- Monitorización de la ciberseguridad, detección y análisis de incidentes y amenazas.
- Detección, análisis y gestión de vulnerabilidades.
- Administración, gestión, mantenimiento y monitorización de la infraestructura de ciberseguridad.
- Gestión y respuesta a incidentes de ciberseguridad.

El SOC actual se apoya en un SIEM (por sus siglas en inglés, *Security Information and Event Management*) del modelo QRadar del fabricante IBM, que correlaciona los eventos de varias fuentes de información, como son el cortafuegos, las sondas de red, algunos servidores y los EDR, lo que permite la detección de posibles actividades maliciosas.

La gestión de la infraestructura en la nube (FWVDF y sistema antiDDoS) la lleva a cabo el operador de comunicaciones.

## 3. ALCANCE I DESCRIPCIÓN DEL SERVICIO.

El alcance del servicio es la contratación de un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés *Security Operations Center*) con capacidades de Equipo de Respuesta a Incidentes (CSIRT, por sus siglas en inglés *Computer Security*

*Incident Response Team*) que proporcione servicios de seguridad gestionada al ORGT.

Los servicios que el SOC llevará a cabo son los siguientes:

- Monitorización de la ciberseguridad, detección y análisis de incidentes y amenazas.
- Detección, análisis y gestión de vulnerabilidades.
- Administración, gestión, mantenimiento y monitorización de la infraestructura de ciberseguridad.
- Gestión y respuesta a incidentes de ciberseguridad.

El SOC deberá estar fundamentado en el uso de la solución Cortex XSIAM, que es una solución de gestión, monitorización y automatización de procesos de ciberseguridad, especificada en el apartado 4.2.

El SOC solicitado tiene la particularidad de que uno de sus integrantes, al que denominamos Referente Técnico, estará dedicado de manera exclusiva al ORGT. Con esta medida, el SOC dispondrá de un mejor conocimiento de la infraestructura y necesidades del ORGT y así podrá aportar un mejor y más àgil servicio. El detalle de las tareas que llevará a cabo el Referente Técnico se encuentra recogido en el apartado 5.6 del presente Pliego.

Además del servicio de SOC, el ORGT quiere mejorar las medidas preventivas de ciberseguridad que tiene implantadas. Para ello renovará el cortafuegos perimetral, dispositivo que realiza el filtrado de las comunicaciones de entrada y salida en el ORGT, implantará un servicio de cortafuegos de aplicaciones web, WAF (por sus siglas en inglés *Web Application Firewall*), y implantará una solución de gestión de accesos privilegiados (PAM, por sus siglas en inglés *Privileged Access Management*). Estas mejoras están detalladas en los apartados 6, 7 y 8 respectivamente.

El elemento más importante de la cadena de seguridad y que puede evitar más incidentes es el usuario final, por ello el contratista deberá implantar un servicio de concienciación en ciberseguridad para los empleados del ORGT, detallado en el apartado 9.

# 4. SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC).

## 4.1. PRINCIPIOS DEL SERVICIO.

El contratista se responsabiliza de la ciberseguridad del ORGT, por lo tanto deberá aportar proactividad y proponer de manera continua mejoras en la ciberseguridad de los sistemas de información y servicios del ORGT.

Los sistemas de información del ORGT están categorizados de categoría media en el Esquema Nacional de Seguridad (ENS).

El contratista llevará a cabo el servicio de SOC siguiendo las normas, instrucciones, guías y procedimientos elaborados por el CCN-CERT (Centro Criptológico Nacional – *Computer Emergency Response Team*).

Los desplazamientos, dietas y cualquier otro gasto asociado estarán incluidos en el servicio y no supondrán mayor coste para el ORGT.

Los técnicos de la DSI tendrán acceso a las consolas de gestión de los servicios suministrados en el presente contrato.

## 4.2. SOLUCIÓN DE GESTIÓN, MONITORIZACIÓN Y AUTOMATIZACIÓN DE PROCESOS DE CIBERSEGURIDAD.

El ORGT actualizará la solución EDR denominada Cortex XDR y el servicio de SIEM ofrecido en una plataforma Qradar, a la evolución comercial denominada CORTEX XSIAM (código PAN-XSIAM-BASE-ENT-PLUS), que es una solución de gestión, monitorización y automatización de procesos de ciberseguridad.

El Cortex XSIAM almacenará los eventos recibidos de las fuentes de información que la DSI considere oportunas, hasta un máximo de 100 Gigabytes de ingesta diaria (código PAN-XSIAM-BASE-GB), y buscará patrones de posibles ciberataques. Al inicio del servicio, las fuentes de información que enviarán eventos al almacén del Cortex XSIAM serán las siguientes:

- 1.250 agentes de Cortex XSIAM, instalados en los escritorios virtuales y servidores.
- Cortafuegos interno (FWORGT), detallado en el apartado 6.
- Cortafuegos externo (FWVDF).
- Cortafuegos de aplicaciones web (WAF) del apartado 7.
- Dos balanceadores de carga Citrix Netscaler.

- Tres controladores de dominio (DC, por sus siglas en inglés *Domain Controller*) Microsoft Windows del ORGT.
- Dos servidores de DNS (por sus siglas en inglés *Domain Name System*).
- Ocho servidores de la DMZ (por sus siglas en inglés *Demilitarized Zone*).
- Dos sondas de red.

El contratista aportará servicio de soporte del fabricante de la solución de gestión, monitorización y automatización de procesos de ciberseguridad (código PAN-XSIAM-PREM-SUCCESS).

Los licitadores propondrán el precio de ampliación para proteger 1 agente adicional de CORTEX XSIAM.

### 4.3. SERVICIO REGULAR.

#### 4.3.1. MONITORIZACIÓN DE LA CIBERSEGURIDAD, DETECCIÓN Y ANÁLISIS DE INCIDENTES Y AMENAZAS.

El servicio de monitorización de seguridad se llevará a cabo en modalidad 24x7 y tiene como objetivo la detección de cualquier amenaza potencial o efectiva en la ciberseguridad del ORGT que pueda ser detectada en base al análisis continuo de los eventos o alertas de seguridad reportados por los sistemas del ORGT. Este servicio se fundamenta en el uso de la solución de gestión, monitorización y automatización de procesos de ciberseguridad que ha sido detallada en el apartado 4.2.

Este servicio debe realizar:

- Monitorización continua de los eventos y alertas en tiempo real generados por las fuentes de información que envían sus eventos de seguridad a la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Detección, identificación y clasificación de los posibles incidentes de seguridad y recopilación de evidencias necesarias para el análisis posterior.
- Priorización de la resolución de los incidentes en función de su peligrosidad real y su impacto.
- Notificación al SOC y al Referente Técnico (5.6), con descripción del incidente detectado y su categorización.
- Análisis completo de los incidentes teniendo en cuenta todas las posibles fuentes de información (evidencias, análisis de vulnerabilidades, otros incidentes, indicadores de compromiso, etc.), para obtener el impacto del incidente, activos afectados, nivel de compromiso del servicio y cualquier

información que permita optimizar la contención, mitigación y erradicación del incidente.

- Proponer un plan de contención, mitigación y recuperación del incidente detectado en base a procedimientos establecidos y con el objetivo de resolver el incidente lo antes posible y con total garantía.
- Elaborar análisis preliminar de los incidentes.
- Gestión del escalado de los incidentes de nivel de peligrosidad muy alto (L4) (5.7) o los que la DSI considere oportuno, al equipo especializado de respuesta a incidentes (CSIRT) con todos los recursos necesarios.
- Coordinar la ejecución de los planes de contención, mitigación y recuperación hasta que se dé por cerrado el incidente, con todo el equipo involucrado en el mismo, bajo la supervisión de la DSI.

### 4.3.2. DETECCIÓN, ANÁLISIS Y GESTIÓN DE VULNERABILIDADES.

El objetivo del servicio es disponer de un mecanismo para detectar y contrarrestar las vulnerabilidades que puedan existir en los sistemas del ORGT, así como poder realizar un seguimiento del ciclo de vida de las vulnerabilidades detectadas (detección, corrección y verificación).

Este servicio llevará a cabo:

- La supervisión de las nuevas vulnerabilidades descubiertas a nivel mundial y comprobación de si afectan a los activos del ORGT.
- La detección e identificación de vulnerabilidades mediante herramientas especializadas.
- La notificación a la DSI de las vulnerabilidades detectadas.
- La propuesta de corrección o mitigación de las vulnerabilidades.
- El seguimiento de la corrección de las vulnerabilidades con un proceso de gestión del ciclo de vida de la vulnerabilidad en el que se verificará si se han realizado las correcciones adecuadas y si estas han solucionado las vulnerabilidades detectadas.

Las vulnerabilidades detectadas deberán ser clasificadas y documentadas de acuerdo con los organismos especializados y bases de datos de conocimiento como son CVE (*Common Vulnerabilities and Exposures*) y CWE (*Common Weakness Enumeration*), utilizando el método de cálculo CVSS (*Common Vulnerability Scoring System*) para clasificar su criticidad. Se deberá facilitar la lectura y comprensión de las debilidades encontradas mediante este servicio.

Como consideraciones generales de los análisis de vulnerabilidades se deberá tener en cuenta que:

- No se realizarán ataques o pruebas de denegación de servicio.
- Se deberán prever posibles impactos en el servicio debidos a las acciones llevadas a cabo durante los análisis. Se deberán notificar a la DSI antes de realizarlas, para programarlas y acordar las condiciones de las ejecuciones, con el fin de no afectar a los servicios.
- Se hará énfasis en las recomendaciones de las vulnerabilidades y errores de seguridad detectados previamente pero que aún no han sido corregidos.
- En toda intervención será requerido que haya un responsable de la DSI al corriente de las actividades realizadas, durante todo el tiempo de vida del análisis.
- Las pruebas realizadas, la descripción de vulnerabilidades encontradas con las evidencias y el estudio del impacto en términos de confidencialidad, integridad y disponibilidad, así como las recomendaciones de seguridad para resolver o evitar las vulnerabilidades, se incluirán en el informe de Gestión de las Vulnerabilidades (5.13).

#### 4.3.2.1. Gestión de vulnerabilidades de los sistemas base de los servidors.

El contratista realizará un análisis de vulnerabilidades semanal de los servidores del ORGT, inicialmente serán 250 servidores, mediante herramientas especializadas de gestión integral, detección y respuesta a vulnerabilidades que permitan realizar tanto análisis de los activos directamente desde la red como análisis exhaustivos mediante un agente y un usuario autenticado. El resultado de estos análisis se incluirá en el informe de gestión de las vulnerabilidades (5.13).

Los servidores a analizar disponen de uno de los siguientes sistemas operativos: Windows Server 2012R2 o superior, VmWare Vsphere ESXi 8.0 U3, Oracle Linux 5.15 y otras variantes de Linux.

Si se detectan vulnerabilidades críticas, el contratista lo comunicará antes de 24 horas a la DSI, proponiendo medidas correctoras.

La DSI puede solicitar el análisis de vulnerabilidades de un servidor bajo demanda; el contratista deberá llevarlo a cabo antes de una semana y el correspondiente informe se entregará antes de dos semanas.

#### 4.3.2.2. Gestión de vulnerabilidades de la red LAN.

El contratista instalará dos escáneres de red (NIPS, por sus siglas en inglés *Network Intrusion Prevention System*) que realizarán una prevención en tiempo real de ataques de ciberseguridad gracias al análisis del tráfico de red. Uno de los escáneres se instalará en la red de servidores públicos, en la que se encuentra la sede electrónica, el portal Citrix y otros servidores (10 servidores), y el otro se instalará en la red de servidores internos en la que están los controladores de dominio, los servidores DHCP y otros servidores (20 servidores).

El resultado de estos análisis del tráfico de red se incluirá en el informe de gestión de las vulnerabilidades (5.13).

Si se detectan vulnerabilidades muy críticas, el contratista lo comunicará antes de 24 horas a la DSI, proponiendo medidas correctoras.

#### 4.3.2.3. Gestión de vulnerabilidades de los sitios web.

El contratista realizará pruebas de intrusión (*Pentesting*, por sus siglas en inglés *Penetration Testing*) en sitios web del ORGT publicados en internet, en las que simulará de manera controlada un ciberataque. El objetivo de estas pruebas de intrusión es la detección de vulnerabilidades reales, comprender su impacto potencial y proponer medidas de corrección antes de que el ORGT sea víctima de un ataque real.

Las metodologías a seguir para realizar las pruebas de intrusión estarán alineadas con PTES (*Penetration Testing Execution Standard*) y OSSTMM (*Open Source Security Testing Methodology Manual*).

Las pruebas de intrusión se realizarán anualmente en dos sitios web que decidirá la DSI durante el primer trimestre del año, siguiendo el escenario de caja gris, en el que se simula un atacante con algunos conocimientos de la organización, y permite hacer un análisis de la seguridad de los servicios web más profundo que en el caso del escenario de caja negra, en el que se simula un atacante sin ningún conocimiento de la organización.

Las actividades a realizar en las pruebas de intrusión serán:

- Definición del alcance y objetivos.
- Recopilación de información.
- Enumeración y análisis de vulnerabilidades.

- Explotación de las vulnerabilidades encontradas.
- Actividades de post-explotación.

El contratista incluirá el resultado de las pruebas de intrusión en el informe de gestión de las vulnerabilidades (5.13). El informe deberá contener los siguientes apartados:

- Descripción detallada de las vulnerabilidades encontradas.
- Pruebas de concepto realizadas.
- Valoración del impacto y riesgo.
- Recomendaciones técnicas de corrección de las vulnerabilidades.
- Conclusiones ejecutivas para el equipo directivo.

#### 4.3.2.4. Simulacro de ciberataque a la organización.

El contratista realizará simulacros de ciberataque diseñados para poner a prueba la seguridad de la organización, imitando las tácticas, técnicas y procedimientos de un adversario real. El objetivo principal no es solo identificar vulnerabilidades técnicas en un servidor específico, como en el caso de una prueba de intrusión, sino también evaluar la capacidad de detección, respuesta y resiliencia de la organización frente a amenazas persistentes avanzadas (APT, por sus siglas en inglés *Advanced Persistent Threat*).

Se realizarán dos simulacros de ciberataque: uno en el transcurso del segundo trimestre del segundo año de contrato y el otro durante el segundo trimestre del cuarto año de contrato.

En estos ejercicios de seguridad ofensiva, también llamados ejercicios de Red Team, intervienen los siguientes actores:

- Red Team: Actúa como un atacante, está formado por especialistas en seguridad ofensiva, que intentan comprometer sistemas, robar datos o acceder a información crítica sin ser detectados.
- Blue Team: Es el equipo defensivo que protege, detecta y responde a los incidentes de seguridad de la organización.
- White Team: Supervisa el ejercicio, gestiona la coordinación y controla el impacto para evitar consecuencias negativas reales durante la realización del ejercicio.

Los objetivos de la realización de un ejercicio de Red Team son:

- Comprobar si un atacante podría obtener acceso a información sensible.

- Evaluar el tiempo de detección y respuesta del Blue Team.
- Detectar carencias en procesos, herramientas de seguridad y entrenamiento del personal.
- Mejorar la postura general de ciberseguridad.

El contratista incluirá el resultado del ejercicio de Red Team en el informe de gestión de las vulnerabilidades (5.13). El informe deberá contener los siguientes apartados:

- Resumen Ejecutivo.
- Alcance y objetivos.
- Metodología utilizada.
- Cronología del ejercicio.
- Vectores de entrada y acceso inicial.
- Movimiento lateral y escalada de privilegios.
- Impacto conseguido.
- Detección y respuesta: Evaluación del Blue Team.
- Recomendaciones y mejoras.

### 4.3.3. ADMINISTRACIÓN, GESTIÓN, MANTENIMIENTO Y MONITORITZACIÓN DE LA INFRAESTRUCTURA DE CIBERSEGURIDAD.

El contratista deberá prestar servicios de administración, gestión, mantenimiento y monitorización de toda la infraestructura de ciberseguridad interna adquirida en el presente contrato. El contratista será responsable de su correcto funcionamiento, siempre bajo la supervisión y aprobación de la DSI.

Este servicio, de manera general, deberá cubrir, para la infraestructura de ciberseguridad interna:

- Mantenimiento de los equipos: gestionar el contrato de mantenimiento y garantías con los fabricantes del equipamiento. Gestionar casos con el fabricante, como por ejemplo la sustitución de piezas o del equipamiento completo. Acceso a la base de datos de conocimiento del fabricante.
- Supervisión del estado de los equipos: monitorizar de forma permanente (24x7) el estado de las variables de funcionamiento idóneas para cada dispositivo administrado. Estas variables deberán ser las necesarias para garantizar el correcto funcionamiento de los equipos (uso de CPU, uso de RAM, espacio en disco, espacio en los sistemas de archivos, tabla de conexiones, número de sesiones, etc.) y notificar si existe algún problema.
- Resolución de consultas: resolver cualquier duda que los técnicos de la DSI puedan plantear referente a ciberseguridad, tanto de sistemas administrados

en el presente contrato como de otros sistemas relacionados con la ciberseguridad.

- Resolución de peticiones de servicio: realizar las peticiones de servicio sobre los equipos administrados, así como la ejecución de tareas de operación solicitadas por la DSI.
- Realización de copias de seguridad: efectuar copias de seguridad de la configuración del equipamiento gestionado por la empresa contratista. Verificar la validez de las copias de seguridad.
- Actualizaciones del software de los dispositivos: realizar las actualizaciones de los equipos administrados recomendadas por el fabricante. Se hará un seguimiento de las versiones de los equipos y se alertará sobre nuevas recomendaciones de actualización.
- Registro y control de actuaciones: inventariar y registrar todas las actuaciones realizadas en los equipos administrados y las motivaciones que las han provocado.
- Revisión mensual de la infraestructura de ciberseguridad y elaboración de informe que permita conocer el estado actual de seguridad de los equipamientos administrados, así como el número, el detalle y el estado de las peticiones e incidentes, y la disponibilidad de los equipos.

En cuanto a la infraestructura de ciberseguridad en la nube (firewalls FWVDF y equipamiento anti-DDoS), el SOC del contratista realizará las siguientes tareas:

- Interlocución con el SOC del operador de comunicaciones para llevar a cabo nuevas peticiones.
- Seguimiento de los incidentes.
- Seguimiento del servicio ofrecido por el SOC del operador de comunicaciones.

### 4.3.4. GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD.

El ORGT toma todas las medidas preventivas que están a su alcance, tanto a nivel técnico, procedimental y personal, para alcanzar un alto nivel de ciberseguridad, pero aun así es susceptible de sufrir incidentes de seguridad.

El ORGT requiere, en caso de sufrir un incidente de ciberseguridad de nivel de peligrosidad muy alto (L4) y aquellos de nivel inferior que la DSI considere oportuno, que este sea atendido por un equipo de respuesta a incidentes (CSIRT, por sus siglas en inglés Computer Security Incident Response Team). (Nota: Los niveles de peligrosidad de los incidentes se encuentran documentados en el apartado 5.7).

El CSIRT deberá proporcionar el soporte y la experiencia necesarios para llevar a cabo las tareas de análisis, contención, erradicación y recuperación del incidente para minimizar su impacto.

La empresa contratista deberá ser miembro del foro FIRST (por sus siglas en inglés Forum of Incident Response and Security Teams) y de la Red Nacional de SOCS en nivel plata. Ambas entidades garantizan que sus miembros disponen de las herramientas y conocimientos necesarios para mejorar sus capacidades de prevención, protección, detección y respuesta a incidentes.

Todas las tareas que el contratista deba realizar para analizar, contener, erradicar y recuperar de un ciberincidente de nivel de peligrosidad muy alto (L4) y aquellos de nivel inferior que la DSI considere oportuno, se considerarán servicios de respuesta a incidentes de muy alta peligrosidad (apartado 4.5).

#### 4.3.5. CUSTODIA DE EVIDENCIAS DIGITALES.

El contratista custodiará durante 2 años y utilizando sus sistemas de información, todas las alertas e incidencias de la solución de gestión, monitorización y automatización de procesos de ciberseguridad. Estas alertas e incidencias se almacenarán siguiendo las recomendaciones del CCN-CERT, para que sean válidas como evidencias digitales en posibles investigaciones judiciales. En el Protocolo de Actuación (cláusula 5.2) se detallará el procedimiento a seguir para que el contratista entregue las evidencias digitales de un día concreto al ORGT con un tiempo de respuesta de dos días.

### 4.4. SERVICIOS ADICIONALES.

La ciberseguridad es un entorno en constante cambio y por ello es difícil prever todas las necesidades que tendremos en los próximos años. Para dar respuesta a posibles imprevistos, la DSI considera necesario contratar una bolsa de horas de técnico para ejecutar tareas relacionadas con la ciberseguridad que no estén previstas en el servicio regular (4.3). A estas tareas las denominamos servicios adicionales.

Los servicios adicionales se llevarán a cabo bajo demanda y siguiendo las directrices del apartado 5.9.

### 4.5. SERVICIOS DE RESPUESTA A INCIDENTES DE MUY ALTA PELIGROSIDAD.

Para dar respuesta a los posibles incidentes de nivel de peligrosidad muy alto (L4) y aquellos de nivel inferior que la DSI considere oportuno, el ORGT considera necesario contratar una bolsa de horas de equipo de respuesta a incidentes (CSIRT) para ejecutar tareas relacionadas con el análisis, contención, erradicación y recuperación de incidentes.

El siguiente es un listado orientativo de posibles servicios de respuesta a incidentes de muy alta peligrosidad que puede ser necesario llevar a cabo, en respuesta a un incidente, durante la vigencia del contrato:

- Tareas de contención para minimizar el impacto del incidente.
- Tareas de mitigación y erradicación del incidente.
- Tareas de recuperación de los servicios afectados por el incidente.
- Soporte a las tareas que realizará la DSI como respuesta al incidente.
- Coordinación durante el incidente con la DSI y todas las partes que puedan estar involucradas, como por ejemplo: Diputación de Barcelona, operador de telecomunicaciones y organismos oficiales a los que sea necesario reportar.
- Análisis de código malicioso para identificar sus capacidades (vectores de entrada, técnicas de ofuscación, métodos de propagación, técnicas de exfiltración, etc.), obtener los indicadores de compromiso (IOC, por sus siglas en inglés Indicator of Compromise).
- Asistencia técnico-jurídica en la comunicación del incidente a los organismos oficiales que corresponda (CCN-CERT, AEPD, etc.) y a los afectados por un incidente.

Cuando se produzca un incidente de nivel de peligrosidad muy alto (L4) y aquellos de nivel inferior que la DSI considere oportuno, el contratista deberá realizar un análisis del incidente y elaborará un Plan Preliminar de Respuesta al Incidente que contendrá las medidas para contener, mitigar y erradicar el incidente, y para recuperar los sistemas afectados por el mismo. También incluirá la dedicación necesaria del contratista para llevar a cabo estas tareas.

El Plan Preliminar de Respuesta al Incidente se presentará a la DSI en los plazos establecidos en el apartado 5.7.

Los servicios de respuesta a incidentes de muy alta peligrosidad detallados en el Plan Preliminar de Respuesta al Incidente se considerarán finalizados cuando hayan sido

validados por la DSI. El contratista los facturará trimestralmente en función de su realización efectiva.

## 5. PRESTACIÓN DEL SERVICIO.

### 5.1. IMPLANTACIÓN DEL SERVICIO

La implantación de los servicios de ciberseguridad del presente contrato se llevará a cabo siguiendo las siguientes fases:

- **Fase 1.** A partir de la firma del contrato y hasta el inicio efectivo del mismo previsto para el 1 de agosto de 2026, se deberán realizar las siguientes tareas:
  - Asignar responsable del servicio y referente técnico del servicio desde el primer día de contrato.
  - Configurar la infraestructura de comunicación entre ORGT y el contratista (apartado 5.3).
  - Informar a la DSI de los canales de comunicación (apartado 5.4) que deberán utilizarse en el servicio.
  - Elaborar el Plan de Implantación, validado y aceptado por la DSI, que incluirá los mecanismos necesarios para ejecutar la implantación del servicio:
    - Reuniones de coordinación e información,
    - conectividad al entorno,
    - planificación de la renovación del nuevo firewall,
    - planificación de la implantación del gestor de vulnerabilidades,
    - planificación de la implantación de las sondas de red,
    - planificación de la implantación del servicio WAF,
    - planificación de la implantación de la solución de gestión de accesos privilegiados,
    - planificación de la implantación del servicio de concienciación.
  - Implantar la solución de gestión, monitorización y automatización de procesos de ciberseguridad (apartado 4.2).
  - Elaborar el protocolo de actuación (apartado 5.2).
  - Renovar las suscripciones de licencias actuales del firewall FWORGT, detalladas en el apartado 2.
  - Instalar herramienta que permita consolidar los logs de los dos nodos del firewall.

- **Fase 2.** Doce meses de duración desde el inicio del contrato. En esta fase el contratista llevará a cabo:
  - Renovación tecnológica del firewall (apartado 6).
  - Implantación del gestor de vulnerabilidades (apartado 4.3.2.1).
  - Implantación de las sondas de red (apartado 4.3.2.2).
  - Implantación del Servicio de WAF (apartado 7).

- Implantación de la solución de gestión de accesos privilegiados (apartado 8.1).
- Implantación del servicio de concienciación en ciberseguridad para los empleados del ORGT (apartado 9.1).

### 5.2. PROTOCOLO DE ACTUACIÓN.

El contratista elaborará, de manera consensuada con la DSI, el Protocolo de Actuación. Este documento es un compendio de los procedimientos a seguir entre ORGT y el contratista para llevar a buen término el servicio de SOC.

El Protocolo de Actuación, como mínimo, deberá detallar los siguientes aspectos:

- Descripción del servicio y recursos humanos dedicados al mismo.
- Contacto del Responsable del servicio y del Referente Técnico.
- Relación de técnicos de la DSI autorizados para comunicar peticiones e incidentes.
- Clasificación del nivel de peligrosidad de los incidentes de seguridad.
- Procedimiento de comunicación, tratamiento y notificación de los incidentes.
- Procedimiento de escalado de los incidentes.
- Procedimiento de comunicación de peticiones y consultas.
- Procedimiento de solicitud de servicios adicionales.
- Procedimiento de solicitud de servicios de respuesta a incidentes de muy alta peligrosidad.
- Tareas que realizará el SOC.
- Tareas a realizar en el análisis de vulnerabilidades trimestral.
- Tareas que se realizarán en las revisiones periódicas mensuales.
- Contenido del informe de seguimiento del servicio.
- Contenido del informe de gestión de vulnerabilidades.
- Acuerdos de servicio a alcanzar.

### 5.3. INFRAESTRUCTURA DE COMUNICACIÓN ENTRE CONTRATISTA Y ORGT.

El acceso remoto al equipamiento objeto de este contrato no puede depender de la infraestructura de comunicaciones del ORGT. Por lo tanto, el contratista establecerá una conexión remota entre su centro de gestión y cada uno de los dos CPDs del ORGT. Esta conexión incluye la provisión de línea, router y el establecimiento de un túnel cifrado extremo a extremo. Este router se conectará directamente a la consola del firewall.

El coste de las líneas de comunicación y licencias necesarias para llevar a cabo la conexión remota correrá a cargo del contratista.
Es responsabilidad del contratista configurar adecuadamente los puestos de trabajo de sus técnicos y su infraestructura de red, para poder conectarse de manera segura a la infraestructura del ORGT.

### 5.4. CANALES DE COMUNICACIÓN.

El contratista dispondrá de una aplicación web en la que se puedan dar de alta las peticiones e incidencias, consultar su evolución y acceder a los informes del servicio. El ORGT también podrá comunicar las peticiones e incidencias mediante correo electrónico o teléfono.

El técnico referente dispondrá de acceso a la aplicación interna de gestión de incidencias del ORGT, denominada U33.

### 5.5. RESPONSABLE DEL SERVICIO.

La empresa contratista nombrará un Responsable del servicio que responderá ante el ORGT de la calidad del servicio, velará por el cumplimiento de los compromisos adquiridos y promoverá el servicio para mejorar la ciberseguridad del ORGT.

El Responsable del servicio realizará, como mínimo, las siguientes tareas:

- Convocar las reuniones de seguimiento del servicio (5.12).
- Redactar el acta de las reuniones de seguimiento del servicio (5.12).
- Velar por el cumplimiento de los acuerdos de servicio.

### 5.6. REFERENTE TÉCNICO DEL SERVICIO.

La empresa contratista designará un Referente Técnico del servicio, asignado en dedicación exclusiva al ORGT durante toda la duración del contrato.
El Referente Técnico llevará a cabo su actividad de manera presencial desde las dependencias del ORGT, un mínimo de dos días semanales, consensuados con la DSI.

De manera no limitativa, las tareas que deberá realizar el Referente Técnico son las siguientes:

- Ser interlocutor principal ante el ORGT para la gestión, el escalado y la coordinación de las necesidades o incidentes que puedan surgir.

- Realizar el primer nivel de atención de las incidencias, peticiones y consultas relacionadas con la ciberseguridad.
- Añadir fuentes de información a la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Configurar casos de uso en la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Trasladar las incidencias, peticiones y consultas que no esté capacitado para resolver o cuando esté demasiado ocupado, al resto de integrantes del SOC.
- Realizar cualquier tarea del servicio regular (apartado 4.3).
- Gestionar las tareas del servicio regular (apartado 4.3), los servicios adicionales (apartado 4.4) y los servicios de respuesta a incidentes de muy alta peligrosidad (apartado 4.5) solicitados al SOC, controlando los escalados y optimizando las gestiones internas del contratista para agilizar su resolución.
- Supervisar todas las tareas que realice el contratista, incluso las que se lleven a cabo en horario nocturno o días festivos.
- Coordinar a los técnicos de la empresa contratista que intervengan en cualquier actividad del servicio.
- Interlocución con el operador de comunicaciones para realizar cambios en la política de seguridad de la infraestructura de seguridad del ORGT en la nube.
- Interlocución con la Dirección de Servicios de Tecnologías y Sistemas Corporativos de la Diputación de Barcelona para realizar cambios necesarios para el ORGT en la política de seguridad de DiBa.
- Interlocución con cualquier proveedor del ORGT en temas relacionados con la ciberseguridad.
- Llevar a cabo actividades mitigadoras y correctivas de vulnerabilidades detectadas en los análisis de vulnerabilidades.
- Proponer, gestionar y llevar a cabo mejoras del servicio.
- Elaborar protocolos técnicos y operativos de respuesta a incidentes.
- Elaborar los informes de seguimiento del servicio.

El Referente Técnico deberá disponer de teléfono móvil y estar disponible para atender llamadas de 8:00 a 18:00, los días laborables en la ciudad de Barcelona. También recibirá, a cualquier hora, las notificaciones de aviso de incidente de muy alta peligrosidad (L4).

Esporádicamente se llevarán a cabo actividades que deberán realizarse en horario de mínima afectación a los servicios que ofrece el ORGT, en horario nocturno o festivo. El Referente Técnico deberá realizar o supervisar estas tareas.

La empresa contratista no tendrá que sustituir al Referente Técnico cuando esté de vacaciones o afectado por una incapacidad temporal inferior a dos semanas. Sus funciones las asumirá el SOC durante su ausencia.

### 5.7. GESTIÓN DE INCIDENTES.

El contratista seguirá la metodología del CCN-CERT en lo relativo a la gestión y respuesta a incidentes de ciberseguridad, detallada en las guías CCN-STIC-403 “Gestión Incidentes de Seguridad Informáticos” y CCN-STIC-817 “Esquema Nacional de Seguridad. Gestión de Ciberincidentes”.

Teniendo en cuenta el documento CCN-STIC-817, los posibles incidentes sufridos por el ORGT se clasifican con los siguientes niveles de peligrosidad real:

- Nivel bajo (L1).
- Nivel medio (L2).
- Nivel alto (L3).
- Nivel muy alto (L4).

Los únicos incidentes considerados de muy alta peligrosidad (L4) que puede sufrir el ORGT son las amenazas persistentes avanzadas (APT, por sus siglas en inglés Advanced Persistent Threat). Para estos incidentes y aquellos que la DSI considere oportuno, el SOC activará el equipo de respuesta a incidentes de ciberseguridad (CSIRT) y se aplicarán los acuerdos de servicio para incidentes de muy alta peligrosidad (L4).

La DSI comunicará al SOC los incidentes que detecte clasificados en uno de los 4 niveles de peligrosidad. Los incidentes detectados por el servicio regular del SOC (4.3.1) serán categorizados de la misma manera por la empresa contratista.

Para medir los acuerdos de nivel de servicio, se tendrán en cuenta las siguientes definiciones:

- Tiempo de notificación del incidente: Es el tiempo transcurrido entre la detección del incidente por el sistema de monitorización hasta que el contratista lo notifica a la DSI.
- Tiempo de análisis preliminar: Es el tiempo transcurrido entre la detección del incidente por el sistema de monitorización o la comunicación del incidente al contratista hasta que la empresa contratista entrega el informe con el análisis preliminar del incidente y presenta el plan preliminar de respuesta al incidente.

- Horario de servicio: Es el intervalo horario en el que se contabilizarán los acuerdos de niveles de servicio.

Los acuerdos de nivel de servicio establecidos en la gestión de los incidentes, dependiendo de su peligrosidad, son:

- Incidentes de peligrosidad baja (L1) e incidentes de peligrosidad media (L2). El tiempo de notificación del incidente es de un día y el tiempo del análisis preliminar es de 2 días, teniendo en cuenta que el horario de servicio es de 8:00 a 18:00 los días laborables en la ciudad de Barcelona.
- Incidentes de peligrosidad alta (L3). El tiempo de notificación del incidente es de cuatro horas y el tiempo del análisis preliminar es de ocho horas, teniendo en cuenta que el horario de servicio es de 8:00 a 18:00 los días laborables en la ciudad de Barcelona.
- Incidentes de peligrosidad muy alta (L4). El tiempo de notificación del incidente es de una hora y el tiempo del análisis preliminar es de cuatro horas, teniendo en cuenta que el horario de servicio es 24x7.

Una incidencia se considerará resuelta si está plenamente documentada y cuenta con el visto bueno funcional y técnico de la DSI.

Para los incidentes de peligrosidad muy alta (L4) y aquellos que la DSI considere oportuno, se elaborará un informe de análisis del incidente, que como mínimo contendrá:

- Fecha y hora de detección.
- Fecha y hora de notificación.
- Fecha y hora de resolución y cierre.
- Nivel de peligrosidad del incidente.
- Causa del incidente.
- Resumen de las acciones recomendadas para mitigar, contener y erradicar el incidente, y para recuperar los sistemas de información.
- Impacto del incidente: Equipos afectados, valoración en la imagen, afectación en la confidencialidad e integridad de la información y afectación en la disponibilidad de los servicios.

### 5.8. GESTIÓN DE PETICIONES.

Los técnicos de la DSI autorizados darán de alta peticiones de cambio en la política de seguridad mediante los canales de comunicación establecidos (5.4), y el SOC será

responsable de proponer e implementar la solución más adecuada y segura, bajo la supervisión de la DSI.

Aunque se prevé un volumen inferior a 400 peticiones anuales, el contratista deberá atender todas las peticiones solicitadas por la DSI.

Una relación no exhaustiva de posibles peticiones es la siguiente:

- Cambio de contraseña de acceso a los equipos.
- Añadir o modificar una política del firewall.
- Añadir o modificar una política de traducción de direcciones (NAT, por sus siglas en inglés Network Address Translation) en el firewall.
- Crear un túnel IPSEC con una empresa colaboradora.
- Crear un túnel SSL-VPN con una empresa colaboradora.
- Añadir o modificar un caso de uso en la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Configurar respuestas automáticas a eventos en la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Forzar la actualización de las firmas de malware en el firewall.
- Modificar el alcance del análisis de vulnerabilidades.
- Modificar la configuración del firewall de aplicación web (WAF, por sus siglas en inglés Web Application Firewall).
- Modificar la configuración del gestor de accesos privilegiados (PAM, por sus siglas en inglés Privileged Access Management).
- Modificar la configuración del servicio de concienciación en ciberseguridad.

A criterio de los técnicos del ORGT, las peticiones se clasificarán en dos niveles de prioridad: normal y urgente.

Una petición se considerará cerrada si está plenamente documentada y cuenta con el visto bueno funcional y técnico de la DSI.

Los acuerdos de nivel de servicio establecidos en la gestión de las peticiones, dependiendo de su prioridad, serán:

- Peticiones ordinarias: El tiempo de resolución de estas peticiones es de 8 horas, teniendo en cuenta que el horario de servicio es de 8:00 a 18:00 los días laborables en la ciudad de Barcelona.
- Peticiones urgentes: El tiempo de resolución de estas peticiones es de 4 horas, teniendo en cuenta que el horario de servicio es 24x7.

## 5.9. GESTIÓN DE SERVICIOS ADICIONALES.

Cuando el ORGT necesite llevar a cabo alguna de las intervenciones enumeradas en el apartado Servicios Adicionales 4.4, o cualquier otra tarea relacionada con la ciberseguridad que no esté incluida en el servicio regular (4.3), se solicitará al Referente Técnico, quien elaborará una propuesta de valoración que contendrá como mínimo:

- Descripción de la tarea a realizar.
- Documentación a entregar al finalizar la tarea.
- Perfil y dedicación del técnico para llevar a cabo la tarea.
- Planificación de fechas en que se realizará la tarea.

El contratista entregará la propuesta de valoración a la DSI en el plazo de dos semanas desde la fecha de la petición. Una vez recibida la propuesta de valoración, la DSI decidirá la aprobación del servicio adicional. Si se aprueba, se llevará a cabo de acuerdo con el calendario presentado. Si no se aprueba, se desestimará su implementación, se cerrará la petición y no supondrá ningún coste para el ORGT.

Se considera que el horario ordinario para la realización de los servicios adicionales es de 8:00 a 18:00 (de lunes a viernes, no festivos), si bien esporádicamente se llevarán a cabo actividades que deberán realizarse en horario de mínima afectación a los servicios que ofrece el ORGT, en horario nocturno o festivo.

La estimación de servicios adicionales a realizar en horario de mínima afectación es de 4 tareas anuales con una dedicación aproximada de 40 horas. Este número es puramente orientativo y deberán llevarse a cabo todas las tareas adicionales en horario de mínima afectación que se soliciten.

Los servicios adicionales se considerarán finalizados cuando estén en producción, documentados y hayan sido validados por la DSI. El contratista los facturará trimestralmente en función de su realización efectiva.

## 5.10. REVISIONES PERIÓDICAS.

Mensualmente se realizarán las siguientes comprobaciones en el equipamiento de Ciberseguridad:

- Análisis de las nuevas versiones de software del equipamiento y de la necesidad de aplicarlas.

- Análisis de actualizaciones de seguridad del equipamiento y de la necesidad de aplicarlas.
- Análisis del rendimiento de los dispositivos con el fin de detectar necesidades de escalado del equipamiento.
- Análisis de la política de seguridad de los firewalls.
- Análisis de la configuración del WAF.
- Análisis de la configuración de la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Análisis de las amenazas e incidentes de seguridad publicados por los CERT (Equipos de Respuesta a Incidentes) como, por ejemplo, INTECO-CERT, CCN-CERT o CESICAT-CERT. Comprobar si el ORGT está afectado por estas amenazas y, si es necesario, proponer las medidas preventivas adecuadas.

El resultado de estas tareas se incluirá en el informe mensual de seguimiento del servicio.

### 5.11. INFORME DE SEGUIMIENTO DEL SERVICIO.

El referente técnico del servicio elaborará un informe mensual donde figurará la evolución de todos los servicios prestados en el presente contrato y lo presentará a la DSI antes del día 20 del mes siguiente. En el informe, como mínimo, deberá constar:

- Detalle de todas las peticiones abiertas durante el mes, en el que se informará:
  - Descripción.
  - Prioridad (urgente u ordinaria).
  - Estado de la petición.
  - Fecha/hora en que se ha comunicado la petición.
  - Fecha/hora en que un técnico asume la resolución.
  - Fecha/hora en que ha quedado resuelta.
  - Indicador (Sí/No) de cumplimiento del ANS (Acuerdo de Nivel de Servicio).
  - Número de horas de desviación del ANS (solo se informará en las peticiones que no cumplen el ANS).
- Detalle de todas las incidencias abiertas durante el mes, en el que se informará:
  - Descripción.
  - Grado de peligrosidad de la incidencia (L1, L2, L3 o L4).
  - Estado de la incidencia.
  - Tareas realizadas para resolverla.
  - Fecha/hora en que se ha comunicado la incidencia.

  - Fecha/hora en que un técnico inicia el análisis preliminar.
  - Fecha/hora en que se finaliza el análisis preliminar.
  - Indicador (Sí/No) de cumplimiento del ANS.
  - Número de horas de desviación del ANS (solo se informará en las incidencias que no cumplen el ANS).
- Detalle de los servicios adicionales solicitados durante el mes y los pendientes de finalización, en el que se informará:
  - Descripción del servicio adicional.
  - Fecha de solicitud del servicio.
  - Fecha de entrega de la propuesta de valoración.
  - Estado de realización del servicio adicional.
  - Planificación: fecha en que estará en producción el servicio.
- Enumeración de días en que no ha habido referente técnico asignado al servicio.

El informe de seguimiento del servicio también contendrá los resultados de la revisión periódica (5.10) y de la revisión de la infraestructura (4.3.3).

El contenido de este informe se consensuará con la DSI y se detallará en el Protocolo de Actuación.

### 5.12. REUNIONES DE SEGUIMIENTO.

El Responsable del servicio convocará mensualmente una reunión de seguimiento del servicio en la que se tratarán, como mínimo, los siguientes temas:

- Incidencias más habituales.
- Revisión de los servicios adicionales y de los servicios de respuesta a incidentes de muy alta peligrosidad llevados a cabo.
- Seguimiento de la calidad del servicio.
- Posibles mejoras en el servicio.
- Posibles mejoras en la infraestructura de ciberseguridad del ORGT.

El Referente Técnico del servicio asistirá a la reunión de seguimiento y el Responsable del servicio elaborará un acta.

### 5.13. INFORME DE GESTIÓN DE LAS VULNERABILIDADES.

El referente técnico elaborará trimestralmente un informe de gestión de las vulnerabilidades para poder evaluar el estado de seguridad de la infraestructura del ORGT y lo presentará a la DSI durante el primer mes del siguiente trimestre.
Este informe contendrá:

- Detalle del análisis de vulnerabilidades de los sistemas base de los servidores (4.3.2.1).
- Detalle del análisis del tráfico de red (4.3.2.2).
- Detalle de las pruebas de intrusión de los sitios web (4.3.2.3).
- Detalle del simulacro de ciberataque (4.3.2.4).

El contenido de este informe se consensuará con la DSI y se detallará en el Protocolo de Actuación.

### 5.14. DEVOLUCIÓN DEL SERVICIO.

El penúltimo trimestre de vigencia del contrato, la empresa contratista elaborará el Plan de Devolución del Servicio que incluya los mecanismos necesarios para transferir competencias, conocimiento, documentación y las evidencias digitales custodiadas (4.3.5) al ORGT, al finalizar el contrato. Este plan deberá ser aprobado por la DSI y contendrá como mínimo la siguiente información:

- Configuración del firewall perimetral.
- Configuración y casos de uso de la solución de gestión, monitorización y automatización de procesos de ciberseguridad.
- Configuración del servicio de WAF.
- Configuración de la solución de gestión de accesos privilegiados.
- Configuración del servicio de concienciación en ciberseguridad.
- Evidencias digitales de los últimos 2 años.

El coste de elaboración del Plan de Devolución del Servicio y todos los recursos necesarios para llevarlo a cabo está incluido dentro del precio del servicio.

## 6. RENOVACIÓN DEL FIREWALL.

El contratista se encargará del mantenimiento, la gestión y la suscripción de las licencias enumeradas en el apartado 2, del firewall perimetral actual, desde el inicio del contrato. A continuación, se describen las características del nuevo firewall.

### 6.1. ESPECIFICACIONES DE HARDWARE

El ORGT necesita renovar el firewall interno FWORGT, que consiste en un clúster de dos nodos del modelo PA3220 del fabricante Palo Alto Networks por el modelo actualizado PA3410 del mismo fabricante, incluido en el Catálogo de Productos y

Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSSTIC) elaborado por el Centro Criptológico Nacional (CCN).

El nuevo firewall dispone de 10 interfaces ópticas SFP+ de 10 Gbps, 4 interfaces ópticas SFP28 de 25G y un rendimiento en modo prevención de amenazas superior a 10 Gbps.

El contratista suministrará los 2 nodos PA3410 (código PAN-PA-3410), 4 transceptores SFP+ tipo 10GBase-SR (código PAN-SFP-PLUS-SR) del fabricante Palo Alto Networks y 4 transceptores SFP+ tipo 10GBase-SR (código RTXM228-551-C98) del fabricante Cisco Systems, compatibles con los conmutadores del CPD que son del modelo Cisco Nexus 9360, así como las 4 fibras ópticas necesarias para interconectar el nuevo firewall a la infraestructura de red del ORGT.

### 6.2. SUSCRIPCIÓN DE LICENCIAS.

El nuevo firewall PA3410 requiere las mismas suscripciones que dispone el firewall actual, y estas son:

- Advanced URL Filtering (código PAN-PA-3410-BND-CORESEC-5YR),
- Advanced DNS Security (código PAN-PA-3410-BND-CORESEC-5YR),
- GlobalProtect (código PAN-PA-3410-GP-5YR-HA2),
- Advanced Threat Prevention (código PAN-PA-3410-BND-CORESEC-5YR), y
- Advanced Wildfire (código PAN-PA-3410-BND-CORESEC-5YR).

También se requiere licencia del producto Panorama (código PAN-PRA-25) para conseguir que los logs de los dos nodos se consoliden en un único entorno, facilitando así el análisis forense de los incidentes y la elaboración de informes.

### 6.3. IMPLANTACIÓN.

La renovación del nuevo firewall implicará que el contratista deberá llevar a cabo las siguientes tareas:

- Suministro del hardware.
- Suministro de todo el cableado necesario para realizar la instalación (red eléctrica y red de datos).
- Contratación de las suscripciones de licencias necesarias.
- Instalación de cada nodo del firewall en el correspondiente CPD.
- Conexión de los nodos del firewall a la red eléctrica y a la red de datos.

- Migración de la configuración actual al nuevo firewall.
- Puesta en producción del nuevo firewall durante un fin de semana, con una interrupción del servicio inferior a dos horas.
- Documentación de las tareas realizadas.
- Formación de los técnicos de la DSI.
- Borrado de datos de los nodos del firewall FWORGT.
- Traslado de los nodos del firewall FWORGT a las dependencias del ORGT.

### 6.4. SERVICIO DE GARANTÍA

El contratista contratará el servicio de garantía del fabricante para todo el hardware adquirido (código PAN-SVC-BKLN-3410-5yr), a partir de la fecha de entrega de los equipos (6.3) y hasta la finalización del contrato.

La garantía del fabricante permitirá:

- Acceder a las actualizaciones y parches de seguridad del software de los equipos.
- Acceder a la base de datos de conocimiento.
- Proporcionar piezas de repuesto nuevas para sustituir las piezas averiadas.
- Proporcionar transceptores nuevos para sustituir los transceptores averiados.
- Disfrutar de un servicio de atención y resolución de casos.

### 6.5. SERVICIO DE MANTENIMIENTO

El servicio de mantenimiento tiene por objetivo corregir y reparar las incidencias o averías que surjan en los equipos físicos y en la corrección de problemas derivados del funcionamiento incorrecto de los programas asociados al equipamiento. El contratista llevará a cabo el servicio de mantenimiento del cortafuegos y, por tanto, realizará las siguientes acciones:

- Registrar las incidencias,
- Seguimiento de las incidencias,
- Gestionar la garantía con el fabricante,
- Diagnosticar e intentar una primera resolución de la incidencia,
- Configurar el nuevo hardware,
- En caso de averías de hardware, se enviará un técnico de campo para sustituir las piezas averiadas por las aportadas por el fabricante,
- Aportar fibras de conexión entre el equipamiento y la infraestructura de red de datos,
- Aportar cables de conexión entre el equipamiento y la red eléctrica,

• Sustitución de los transceptores y de las fibras que unen el equipamiento a la infraestructura de red.

El servicio de mantenimiento tendrá las siguientes características:

• La comunicación de los incidentes se realizará usando los canales de comunicación previstos en el apartado 5.4,
• Servicio de asistencia en modalidad 24 x 7,
• La mano de obra, los desplazamientos, los repuestos, los costes derivados del diagnóstico, el desmontaje del equipo averiado, la configuración y la puesta en marcha están incluidos en el servicio,
• Los repuestos utilizados serán los originales del fabricante,
• Número ilimitado de incidentes.

En cuanto al nivel de servicio que deberá cumplir el servicio de mantenimiento del cortafuegos, se considera que deberá atender dos tipos de averías:

• Normales. Averías que afectan a un elemento de hardware redundante del cortafuegos activo, o bien el cortafuegos pasivo puede asumir el servicio del cortafuegos activo,
• Críticas. Averías que provocan la interrupción del servicio, como por ejemplo que el cortafuegos activo sufra un problema y el pasivo no entre en funcionamiento.

Para las averías normales se deberá cumplir:

• Tiempo de notificación del incidente de 4 horas,
• Tiempo de sustitución de un nodo averiado de 8 horas.

Para las averías críticas se deberá cumplir:

• Tiempo de notificación del incidente de una hora,
• Tiempo de respuesta presencial, si se requiere, de 2 horas.

## 7. SERVICIO DE CORTAFUEGOS DE APLICACIÓN WEB (WAF).

El ORGT necesita proteger su sede electrónica y otros servicios web de posibles ataques maliciosos llevados a cabo mediante tráfico HTTP y HTTPS. Para conseguirlo, es necesario implantar un cortafuegos de aplicaciones web (WAF, por sus siglas en inglés Web Application Firewall) que funciona como una capa intermedia entre los usuarios y los servicios web, y protege frente a los siguientes ciberataques:

• SQL Injection. Intentos de inyectar código SQL malicioso para leer, modificar o eliminar datos de la base de datos.

• Cross-Site Scripting (XSS). Inserción de scripts maliciosos dentro de páginas web para robar cookies, tokens de sesión.
• Cross-Site Request Forgery (CSRF). Hace que un usuario autenticado realice acciones no deseadas en una aplicación donde está autenticado.
• Command Injection. Inserción de comandos del sistema operativo a través de campos de entrada vulnerables.
• Path Traversal. Permite acceder a archivos o directorios fuera de la raíz de la aplicación.
• Session Hijacking. Captura y uso de tokens de sesión para suplantar usuarios legítimos.
• HTTP Request Smuggling / Splitting. Manipulación de la forma en que los servidores interpretan las cabeceras HTTP para evadir controles de seguridad.
• Bots maliciosos. Redes de ordenadores que recopilan información excesiva y extraen datos.
• Brute-force y credential stuffing. Ataque que realiza intentos masivos de inicio de sesión. Intenta provocar una denegación de servicio.
• Otros ataques a servicios web que surjan durante la vigencia del contrato.

Las características del servicio de cortafuegos de aplicación web a implantar son las siguientes:

• Servicio ofrecido en modo SaaS (del inglés *Software as a Service*).
• Proteger 10 sitios web.
• Ancho de banda a proteger de 100 Mbps.
• Bloquear futuras técnicas de ataque a sitios web.
• Integración con la solución de gestión, monitorización y automatización de procesos de ciberseguridad, detallada en el apartado 4.2.

### 7.1. IMPLANTACIÓN.

La implantación del servicio de cortafuegos de aplicación web implicará que el contratista deberá llevar a cabo las siguientes tareas:

• Configurar en el WAF las aplicaciones protegidas.
• Redirección del tráfico destinado a los sitios web del ORGT hacia el WAF.
• Aplicar políticas de seguridad en el WAF.
• Poner en producción el WAF con una interrupción del servicio inferior a dos horas.
• Documentar las tareas realizadas.
• Formación de los técnicos de la DSI.

La administración, soporte y monitorización del servicio se llevarán a cabo como tareas incluidas en el servicio regular (4.3.3).

## 8. GESTOR DE ACCESOS PRIVILEGIADOS (PAM).

El ORGT necesita proteger a los usuarios con roles críticos (administradores de sistemas, administradores de bases de datos, ingenieros de red, etc.) y por ello quiere implantar una solución de gestión de accesos privilegiados (PAM, por sus siglas en inglés *Privileged Access Management*).

El PAM debe aportar las siguientes funcionalidades:

- Control de acceso privilegiado. Limita quién puede acceder a qué máquinas, aplicaciones y bajo qué condiciones.
- Gestión de credenciales. Almacena y gestiona contraseñas privilegiadas en una caja fuerte virtual, con rotación automática de contraseñas.
- Sesión auditada y monitorización en tiempo real. Registra las sesiones de acceso privilegiado para detectar y responder a acciones sospechosas o no autorizadas.
- Elevación y delegación de privilegios. Permite conceder acceso temporal o limitado según la necesidad, sin compartir contraseñas.
- Grabación de las sesiones. Permite registrar las sesiones.
- Descubrimiento de cuentas de usuario privilegiadas.
- Importación de secretos almacenados en un Keepass.
- Medidas de seguridad disponibles:
    - o Autenticación mediante multifactor.
    - o Copia de seguridad cifrada y periódica de los secretos.
    - o Generación de un archivo de recuperación para la restauración del entorno.
    - o Posibilidad de disponer de una instancia secundaria preconfigurada en el CPD pasivo.
    - o Modo emergencia para acceder a las credenciales en caso de desastre.

Las características de la solución PAM a implantar en el ORGT son las siguientes:

- Solución instalada en alta disponibilidad en los hipervisores VmWare Vsphere ESXi 8.0 U3 de los dos CPD del ORGT.
- Protegerá a 75 usuarios privilegiados: 40 internos y 35 externos.
- Protegerá el acceso a 200 servidores con sistemas operativos Windows Server 2012R2 o superior, Oracle Linux 5.15 y VmWare Vsphere ESXi 8.0 U3.
- Protegerá el acceso a servidores de la DMZ.

• Integración con el Directorio Activo.
• Integración con la solución de gestión, monitorización y automatización de procesos de ciberseguridad detallada en el apartado 4.2.

### 8.1. IMPLANTACIÓN.

La implantación del gestor de accesos privilegiados implicará que el contratista deberá llevar a cabo las siguientes tareas:

- Contratación de las suscripciones de licencias necesarias.
- Instalar el gestor de accesos privilegiados en servidores virtuales del ORGT.
- Configurar el gestor de accesos privilegiados
    - Proteger el acceso de los administradores de sistemas y los técnicos de las empresas externas colaboradoras a los servidores del ORGT.
    - Activar la rotación automática de contraseñas.
    - Activar el acceso temporal con aprobación.
    - Configurar todas las medidas de seguridad disponibles.
- Crear instancia secundaria preconfigurada en el CPD pasivo.
- Documentar las tareas realizadas.
- Formación de los técnicos de la DSI.

La administración, soporte y monitorización del PAM se llevarán a cabo como tareas incluidas en el servicio regular (4.3.3).

## 9. CONCIENCIACIÓN EN CIBERSEGURIDAD.

El contratista llevará a cabo un servicio de concienciación en ciberseguridad para los empleados del ORGT que disponga de las siguientes funcionalidades:

- Formación estructurada por niveles: Habilidades prácticas agrupadas en módulos temáticos como contraseñas, navegación web, correo electrónico, redes sociales, dispositivos móviles, datos confidenciales, GDPR, entre otros. Cada tema debe presentarse en varios niveles de dificultad adaptándose al perfil de riesgo de cada empleado.
- Cursos principales y exprés: El curso principal proporciona una formación exhaustiva con lecciones interactivas, refuerzos, tests y simulaciones de phishing. El curso exprés, en cambio, es una formación breve en formato audiovisual, ideal para refrescar conocimientos o para sesiones rápidas.
- Aprendizaje progresivo y adaptado a los conocimientos adquiridos por el empleado.
- Recordatorios periódicos para consolidar los conocimientos.

• Simulaciones de phishing: Se llevarán a cabo campañas de phishing simuladas con plantillas personalizables, permitiendo evaluar y mejorar la capacidad de los empleados para detectar correos electrónicos maliciosos.
• Tipologías de phishing: Las campañas de phishing simularán ataques de las siguientes tipologías:
    o Phishing de clic en un enlace.
    o Phishing de descarga de un documento malicioso.
    o Phishing de captura de credenciales.
    o Phishing de escaneo de QR.
• Automatización completa: El servicio de concienciación estará completamente automatizado, desde la programación de cursos hasta el envío de recordatorios e informes, reduciendo la carga administrativa.
• Visibilidad de la evolución de la concienciación en ciberseguridad:
    o Disponibilidad de cuadros de mando para disponer de una visión en tiempo real.
    o Informes de evolución de las campañas de phishing.
    o Informes sobre la madurez en ciberseguridad de los empleados, nivel de riesgo del empleado.
• La interfaz de usuario final y los contenidos de los cursos deben estar disponibles en catalán.

Las características del servicio de concienciación en ciberseguridad a implantar en el ORGT son las siguientes:

• Dimensionar para 1100 empleados.
• Soporte al idioma catalán. Todas las comunicaciones con los alumnos deben poder realizarse en catalán.
• Integrable con el Directorio Activo.
• Integrable con la solución de gestión, monitorización y automatización de procesos de ciberseguridad detallada en el apartado 4.2.
• El servicio de concienciación en ciberseguridad puede apoyarse en una solución en las instalaciones propias o en la nube, pero en ambos casos debe adoptar las medidas de seguridad oportunas.
• El contratista aportará todas las licencias necesarias.

### 9.1. IMPLANTACIÓN

La implantación del servicio de concienciación en ciberseguridad implicará que el contratista deberá llevar a cabo las siguientes tareas:

- Instalación en los servidores virtuales del ORGT.
- Integrar con el Directorio Activo.
- Segmentar a los empleados según su rol (administrativos, técnicos y directivos) y definir su ruta de formación.
- Configurar el servicio de concienciación en ciberseguridad.
- Programar campañas de phishing.
- Configurar informes de seguimiento.
- Documentar las tareas realizadas.
- Formación de los técnicos de la DSI.

La administración, soporte y monitorización de la solución de concienciación en ciberseguridad se llevarán a cabo como tareas incluidas en el servicio regular (4.3.3).

**DILIGENCIA** para hacer constar que el texto que antecede es traducción al castellano del Pliego de Prescripciones Tècnicas Particulares, aprobado por acuerdo de la Junta de Gobierno de la Diputació de Barcelona, número 764, de fecha 18 de diciembre de 2025.

En caso de discrepancia entre dicho Pliego de Prescripciones Tècnicas Particulares, en catalán, y esta traducción al castellano, prevalecerá el primero.

## Metadades del document

| | |
|---|---|
| **Núm. expedient** | ORGT/2025/0035517 |
| **Tipus documental** | Plec de clàusules o condicions |
| **Títol** | Pliego de Prescripciones Técnicas - Traducción |

## Signatures

| Signatari | | Acte | Data acte |
|---|---|---|---|
| Jordi Valls Moya (SIG) | Cap Servei d'Explotació i Sistemes | Signa | 18/12/2025 16:19 |

## Validació Electrònica del document

| Codi (CSV) | Adreça de validació | QR |
|---|---|---|
| 6432fb0a8af2d2945a87 | https://seuelectronica.diba.cat | |