TABAKALERA

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DEL SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DEL EQUIPAMIENTO INFORMÁTICO DE SEGURIDAD PARA LA RED DE COMUNICACIONES PERIMETRAL, ASÍ COMO DE LA FORMACIÓN EN EL MANEJO DEL MISMO PARA EL CENTRO INTERNACIONAL DE CULTURA CONTEMPORÁNEA, S.A.

1. ANTECEDENTES, JUSTIFICACIÓN DE LA CONTRATACIÓN Y ESTADO ACTUAL 2
2. OBJETO DEL CONTRATO 3
3. ALCANCE 4
4. CARACTERÍSTICAS TÉCNICAS MÍNIMAS 5
   4.1. ARQUITECTURA Y RENDIMIENTO 5
   4.2. INTERFAZ FÍSICA 5
   4.3. FUNCIONALIDADES DE SEGURIDAD 6
   4.4. VPN Y ACCESO REMOTO 6
   4.5. ALTA DISPONIBILIDAD 6
   4.6. INTEGRACIÓN CON RED Y CONTROLADORA WIFI 6
   4.7. ADMINISTRACIÓN Y MONITORIZACIÓN 7
   4.8. FUNCIONALIDADES ADICIONALES REQUERIDAS 7
5. REQUISITOS MÍNIMOS EXIGIDOS RESPECTO AL EQUIPAMIENTO A SUMINISTRAR 7
6. ENTREGA, INSTALACIÓN, PUESTA EN MARCHA Y FORMACIÓN DEL EQUIPAMIENTO 9
   6.1. ENTREGA DEL EQUIPAMIENTO 9
   6.2. INSTALACIÓN 10
   6.3. PUESTA EN MARCHA 10
7. SERVICIOS POSTVENTA A PRESTAR DURANTE EL PLAZO DE GARANTÍA 11

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DEL SUMINISTRO, DE LA INSTALACIÓN, DE LA CONFIGURACIÓN Y DE LA PUESTA EN MARCHA DEL EQUIPAMIENTO INFORMÁTICO DE SEGURIDAD PARA LA RED DE COMUNICACIONES PERIMETRAL, ASÍ COMO DE LA FORMACIÓN EN EL MANEJO DEL MISMO PARA EL CENTRO INTERNACIONAL DE CULTURA CONTEMPORÁNEA, S.A.

1. ANTECEDENTES, JUSTIFICACIÓN DE LA CONTRATACIÓN Y ESTADO ACTUAL

La renovación del sistema de cortafuegos actualmente operativo en el Centro Internacional de Cultura Contemporánea, S.A. (en adelante, CICC) se enmarca dentro del proceso de evolución de su infraestructura de red perimetral y está directamente relacionada con la reciente modernización de la red WiFi del centro.

En el año 2021, CICC adquirió e instaló dos cortafuegos modelo **FortiGate 301E**, que han venido prestando servicio desde entonces. Inicialmente se contrató un soporte de tres años mediante licitación pública, prorrogado posteriormente por dos años más, alcanzando una cobertura de soporte actual hasta el **15 de abril de 2026**. Con el fin de garantizar la continuidad operativa, evitar la obsolescencia tecnológica y asegurar la compatibilidad con la nueva red WiFi, se impulsa esta nueva licitación de suministro, instalación, configuración y puesta en marcha, que también incluirá una sesión formativa presencial de conformidad con lo establecido en la Cláusula 6 del presente Pliego de Prescripciones Técnicas.

En 2025, CICC abordó una **renovación integral de la red WiFi del centro**, motivada por la necesidad de:

- Redimensionar la infraestructura de acuerdo al uso real localizado.
- Sustituir equipos al final de su vida útil.
- Adaptar los costes de mantenimiento a las nuevas necesidades.

El resultado ha sido una nueva red con **86 puntos de acceso Fortinet,** gestionados de forma centralizada mediante controladora. En este contexto**, los nuevos cortafuegos deberán asumir también la función de controladora de estos APs**, por lo que se requiere una solución plenamente integrada y compatible con el ecosistema Fortinet, con capacidades avanzadas de gestión, visibilidad y seguridad.

El uso de la red WiFi en CICC es intensivo y diverso. A las **WLAN privadas** para personal e infraestructura, se suman las **redes públicas**, esenciales para el funcionamiento del centro como espacio cultural abierto: usuarios de la mediateca, artistas, eventos, talleres y público general.

Adicionalmente, se ha identificado que, si bien los cortafuegos actuales no presentan fallos técnicos, su capacidad podría quedar limitada para afrontar la carga combinada de tráfico generado por **hasta 300 usuarios simultáneos**, la gestión de **86 APs activos**, y los nuevos requisitos de protección, control y administración centralizada. Por tanto, se considera imprescindible una actualización que garantice el rendimiento, la seguridad y la escalabilidad necesarias para el entorno actual y futuro de CICC.

2. OBJETO DEL CONTRATO

El objeto del contrato es el suministro, instalación, configuración y puesta en marcha de una solución de seguridad perimetral compuesta por dos equipos cortafuegos en alta disponibilidad para el CICC, en sustitución de los equipos actualmente en operación.

Asimismo, el objeto del contrato incluirá la impartición de una sesión de formación presencial en las instalaciones de CICC sobre: (i) Administración y uso básico del sistema; (ii) monitorización de tráfico y eventos; (iii) gestión de configuraciones, copias de seguridad y restauración; (iv) procedimientos ante incidencias.

Igualmente, formarán parte del objeto del contrato los servicios postventa a prestar durante el plazo de garantía establecido en el punto 25 de la Carátula, de conformidad con lo establecido en la Cláusula 7 del presente Pliego de Prescripciones Técnicas.

El contrato se ejecutará de conformidad con lo establecido en el Pliego de Cláusulas Administrativas Particulares y en su Carátula y en el presente Pliego de Prescripciones Técnicas.

La solución deberá ser compatible con el ecosistema desplegado en CICC y habilitar la funcionalidad de controladora de los puntos de acceso WiFi del centro.

El Código CPV del contrato es el siguiente: **32424000-1 - Infraestructura de red (Principal).**

3. ALCANCE

El contrato abarca el suministro, instalación, configuración y puesta en marcha de una solución de seguridad perimetral compuesta por **dos cortafuegos físicos en alta disponibilidad**, destinada a sustituir el sistema actualmente operativo en el CICC.

Dicha solución deberá garantizar la **continuidad del servicio**, la **protección integral del tráfico de red** y la integración completa con la infraestructura de comunicaciones ya desplegada en el centro. De forma específica, se requiere que el sistema ofertado y suministrado sea **plenamente compatible con la red WiFi Fortinet existente**, permitiendo afrontar la carga combinada de tráfico generado por hasta 300 usuarios simultáneos y la gestión centralizada de **los 86 puntos de acceso inalámbrico instalados en 2025**, así como su control desde una única plataforma de administración.

El contrato incluye también los siguientes servicios complementarios, con carácter no limitativo:

- **Migración de la configuración actual** y puesta en marcha de la nueva solución garantizando la continuidad del servicio en condiciones normales de operación y minimizando el impacto en la actividad del CICC. En su caso, las actuaciones que puedan implicar interrupciones deberán planificarse y coordinarse previamente con el CICC, ejecutándose en ventanas de mantenimiento acordadas, con procedimientos de contingencia y reversión.

- **Licencias activas y soporte técnico completo durante un periodo de cinco años,** de conformidad con lo establecido en la **Cláusula 7** del presente Pliego (cobertura completa de garantía y soporte del fabricante, **incluyendo hardware, licencias/suscripciones y servicios de soporte** durante dicho periodo), así como soporte técnico básico postventa asociado a la instalación y configuración realizadas, durante un plazo de tres (3) meses desde la puesta en marcha, para la resolución de incidencias y ajustes menores.

- **Formación técnica básica** al personal de CICC, de conformidad con lo establecido en la Cláusula 6.3 del presente Pliego de Prescripciones Técnicas.

- **Entrega de la documentación técnica detallada,** incluyendo esquemas, configuración y manuales de operación.

El contratista deberá asumir todas las tareas necesarias para la correcta ejecución del

contrato que incluirá el suministro, la instalación física, la configuración, las pruebas de funcionamiento, , la impartición de la formación y los servicios postventa a prestar durante el plazo de garantía.

4. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

La solución ofertada deberá consistir en **dos equipos físicos de seguridad perimetral en alta disponibilidad (HA)**, con las características técnicas mínimas que se describen a continuación. A efectos orientativos, se considera como referencia válida el modelo **FortiGate 400F o equivalente**, siempre que la solución ofertada **cumpla íntegramente todos los requisitos funcionales, de rendimiento, compatibilidad e integración** definidos en el presente Pliego de Prescripciones Técnicas, y sea plenamente **compatible con la infraestructura de red ya implantada en CICC**.

4.1. ARQUITECTURA Y RENDIMIENTO

- Dos dispositivos de seguridad de red independientes, en configuración activa-activa o activa-pasiva, con soporte de failover automático.
- Capacidad mínima de **rendimiento de cortafuegos de 40 Gbps** (para tráfico con paquetes grandes).
- **Rendimiento de protección ante amenazas** no inferior a **5 Gbps**, incluyendo inspección profunda de paquetes, filtrado web, antivirus y control de aplicaciones.
- Latencia máxima: 3 microsegundos (µs) para paquetes de 64 bytes (UDP).
- Capacidad mínima de **4 millones de sesiones concurrentes.**
- Capacidad para procesar **300.000 sesiones nuevas por segundo.**
- Rendimiento VPN IPsec de al menos **20 Gbps** y rendimiento SSL VPN de al menos **2,5 Gbps**.

4.2. INTERFAZ FÍSICA

Al menos:

- 16 puertos RJ45 Gigabit Ethernet.
- 16 ranuras SFP Gigabit.
- 2 puertos dedicados para gestión (MGMT).
- 1 puerto de consola.
- 1 puerto USB.

Montaje en rack en **formato 1U** máximo.

4.3. FUNCIONALIDADES DE SEGURIDAD

- Sistema de prevención de intrusiones (IPS) con posibilidad de creación de firmas personalizadas.
- Capacidad para control granular de aplicaciones con una base mínima de 4.000 aplicaciones identificables, incluyendo aplicaciones cifradas (HTTPS).
- Protección frente a botnets mediante reputación IP en tiempo real.
- Inspección de tráfico cifrado (SSL/TLS).
- Sistema de protección frente a pérdida de datos (DLP), con soporte para detección de patrones (DNI, tarjetas de crédito, palabras clave, expresiones regulares, etc.).
- Capacidad de detección y bloqueo de amenazas en documentos ofimáticos mediante análisis dinámico.

4.4. VPN Y ACCESO REMOTO

Soporte nativo para los siguientes protocolos:

- VPN SSL en tres modos: web, túnel y port forwarding.
- IPsec (IPv4/IPv6), GRE sobre IPsec, L2TP, PPTP, ADVPN.

Incluido en la solución ofertada, sin costes/licencias **adicionales más allá de las incluidas** en el suministro, el soporte de al menos **300 usuarios simultáneos en VPN SSL.**

4.5. ALTA DISPONIBILIDAD

- Sincronización de configuración y sesiones.
- Soporte de clustering y redundancia sin licencias adicionales.
- Interfaces dedicadas para Heartbeat y gestión.
- Soporte para reenvío de tráfico sin interrupciones ante fallo de nodo.

4.6. INTEGRACIÓN CON RED Y CONTROLADORA WIFI

- Compatibilidad plena con sistema de control y gestión centralizada de puntos de acceso WiFi.

- Capacidad para actuar como controladora inalámbrica, permitiendo la administración y monitorización de al menos 86 puntos de acceso simultáneos.
- Soporte para segmentación VLAN, gestión de SSID, políticas de acceso por usuario y dispositivo, portal cautivo personalizado y autenticación 802.1X.
- Gestión basada en identidad de usuario, integración con Active Directory, LDAP, Radius y TACACS+.
- Control de acceso basado en tipo de dispositivo sin necesidad de agente local (identificación de sistema operativo cliente, tipo de terminal, etc.).

4.7. ADMINISTRACIÓN Y MONITORIZACIÓN

- Administración por interfaz gráfica web (GUI) y línea de comandos (CLI).
- Exportación de registros por SYSLOG, FTP, SCP y TFTP.
- Soporte para SNMP v2/v3 y sFlow.
- Soporte de cuentas de administración múltiples con diferentes perfiles de permisos.
- Aplicación de cambios sin reinicio ni interrupción del servicio.

4.8. FUNCIONALIDADES ADICIONALES REQUERIDAS

- Balanceo dinámico de enlaces WAN según latencia, carga o rutas.
- Capacidad SD-WAN sin licenciamiento adicional.
- Soporte de protocolos de routing dinámico: RIP, OSPF, BGP, Multicast IPv4/IPv6.
- Virtualización interna de seguridad con mínimo 10 dominios virtuales (VDOM) configurables sin coste adicional.
- Soporte para balanceo de servidores y offloading de tráfico SSL entrante.
- Licencia activa durante 5 años para:
    - Protección de amenazas (Threat Protection).
    - Antivirus.
    - Control de aplicaciones.
    - Reputación de IP y antispam.
    - Filtrado de contenidos.
    - Sandbox y análisis de tráfico ofimático.

5. REQUISITOS MÍNIMOS EXIGIDOS RESPECTO AL EQUIPAMIENTO A SUMINISTRAR

- **Estado del equipamiento**: Todos los equipos deberán ser nuevos de fábrica, sin uso previo, sin haber sido reacondicionados, reparados, remanufacturados ni utilizados como producto de exposición o demostración.

- **Certificaciones y normativa**: Todos los equipos deberán contar con marcado CE, en cumplimiento con las directivas europeas aplicables, especialmente en materia de seguridad eléctrica (Low Voltage Directive) y compatibilidad electromagnética (EMC Directive).

  Asimismo, deberán cumplir con las directivas RoHS (limitación de sustancias peligrosas) y REACH (registro, evaluación y autorización de sustancias químicas).

  Adicionalmente, el equipamiento de seguridad perimetral (cortafuegos) ofertado y suministrado deberá estar certificado conforme al Esquema Nacional de Seguridad (ENS) en categoría MEDIA o superior. A estos efectos, el/los modelos propuestos y suministrados deberán figurar como producto certificado o cualificado en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del Centro Criptológico Nacional, o bien disponer de un certificado de conformidad ENS en vigor que acredite el cumplimiento del ENS en dicha categoría o superior.

- **Compatibilidad eléctrica y de red:** Los equipos deberán ser compatibles con la red eléctrica europea (230V/50Hz) y con los estándares internacionales de comunicación de red, incluyendo TCP/IP, IPv4, IPv6, SNMP, HTTP/HTTPS, SSH, SYSLOG, entre otros.

- **Homogeneidad e interoperabilidad:** Los dos equipos suministrados deberán ser idénticos en modelo, características y versión de firmware, garantizando el correcto funcionamiento en configuración de alta disponibilidad (HA).

  Todos los componentes de la solución (hardware, licencias, software de gestión y módulos de seguridad) deberán ser plenamente compatibles entre sí y con la infraestructura de red existente en CICC.

- **Estado de soporte:** Los equipos propuestos y suministrados deberán estar dentro del ciclo de vida activo del fabricante, sin fecha de fin de venta (End of Sale) ni de fin de soporte (End of Support) prevista dentro de los cinco años siguientes a la entrega.

No se admitirán productos que estén en fase de obsolescencia o con disponibilidad limitada.

- **Documentación técnica:** El contratista deberá entregar manuales de usuario, guías de instalación y fichas técnicas oficiales de los equipos suministrados, en formato digital o papel, en castellano o inglés.

- **Ciberseguridad:** La solución deberá incorporar mecanismos de cifrado y autenticación adecuados para garantizar que las comunicaciones y la administración del sistema se realizan de forma autenticada y segura (gestión por HTTPS/SSH, control de acceso por roles, registro/auditoría y envío de logs a SYSLOG, y posibilidad de aplicar actualizaciones de seguridad durante el periodo de soporte).

6. ENTREGA, INSTALACIÓN, CONFIGURACIÓN, PUESTA EN MARCHA Y FORMACIÓN DEL EQUIPAMIENTO

El contratista será responsable de realizar la **entrega, la instalación, la configuración y la puesta en marcha** del sistema de seguridad perimetral suministrado, en coordinación con el equipo técnico de CICC, según se detalla a continuación.

Asimismo, el contratista deberá impartir la sesión de **formación** presencial, de conformidad con lo establecido en la Cláusula 6.3 del presente Pliego de Prescripciones Técnicas.

6.1. ENTREGA DEL EQUIPAMIENTO

- El equipamiento deberá ser entregado en las instalaciones de CICC, ubicadas en Andre Zigarrogileak Plaza, 1 – 20012 Donostia / San Sebastián (Gipuzkoa), conforme a lo indicado en el punto 5 de la Carátula.

- Todo el material deberá estar en su embalaje original de fábrica, incluyendo manuales, licencias, accesorios, cables, soportes de montaje y demás elementos necesarios para su correcto funcionamiento.

- La entrega deberá garantizar la integridad del equipamiento, acompañada del albarán detallado.

6.2. INSTALACIÓN Y CONFIGURACIÓN INICIAL

El contratista deberá llevar a cabo la instalación completa del sistema, incluyendo:

- Montaje físico de los dispositivos en el rack designado por CICC.
- Conexionado eléctrico y de red de los puertos necesarios.
- Configuración inicial de red y de la alta disponibilidad (HA) entre ambos dispositivos.
- Integración con la red interna del centro (VLANs, enlaces troncales, sistemas de gestión).
- Preparación del sistema para actuar como controladora de los 86 puntos de acceso inalámbricos.
- Parametrización inicial segura del sistema, incluyendo la configuración de accesos de administración (HTTPS/SSH) y perfiles/roles de usuario, de acuerdo con las políticas de CICC.
- Configuración de servicios base necesarios para la operación (direccionamiento, rutas, DNS/NTP) y centralización de registros mediante SYSLOG, cuando aplique conforme a la infraestructura de CICC.
- Realización de una copia de seguridad inicial ("baseline") de la configuración y entrega al CICC del fichero de backup y del procedimiento de restauración.
- Etiquetado y ordenación profesional del cableado.

6.3. PUESTA EN MARCHA

El contratista deberá ejecutar la puesta en marcha del sistema y proporcionar formación básica al personal técnico designado por CICC. Como mínimo, esta fase incluirá:

- Migración de la configuración existente desde los cortafuegos actuales, **minimizando el impacto en el servicio**; en su caso, las posibles interrupciones se realizarán en **ventanas de mantenimiento acordadas** con el CICC.

- **Verificación funcional** del sistema: firewall, políticas de seguridad, NAT, VPN, filtrado, control de aplicaciones y demás servicios habilitados.

- Prueba del sistema en **modo de alta disponibilidad (HA),** incluyendo conmutación automática ante fallo.

- **Integración completa con los puntos de acceso inalámbricos,** asegurando su gestión desde la nueva solución.

- **Sesión formativa presencial en las instalaciones de CICC** (mínimo 2 horas) sobre:

    - Administración y uso básico del sistema.
    - Monitorización de tráfico y eventos.
    - Gestión de configuraciones, copias de seguridad y restauración.
    - Procedimientos ante incidencias.

- Entrega de documentación técnica y material didáctico, en castellano o inglés, en formato digital o físico.

La aceptación y recepción final del sistema quedará condicionada a la superación satisfactoria del protocolo de pruebas y la validación del equipo técnico de CICC.

7. SERVICIOS POSTVENTA A PRESTAR DURANTE EL PLAZO DE GARANTÍA

Durante el periodo de garantía del equipamiento, y sin coste adicional para CICC, el contratista deberá prestar los servicios mínimos siguientes:

- **Gestión y tramitación de incidencias** cubiertas por la garantía del fabricante, actuando como interlocutor único entre CICC y el fabricante cuando sea necesario.

- **Asistencia para la sustitución del hardware defectuoso** en caso de fallo cubierto por la garantía o el servicio de soporte del fabricante (RMA).

- **Soporte técnico básico postventa** para cuestiones relacionadas con la instalación realizada, durante un plazo de **3 meses** desde la recepción, para resolver dudas o realizar pequeños ajustes en la configuración.

- **Acceso a las actualizaciones y parches** de seguridad y firmware del fabricante, incluidos en el servicio contratado (FortiCare/FortiGuard o equivalente).

- **Cobertura completa de garantía del fabricante,** incluyendo hardware, licencias y servicios de soporte durante el periodo de cinco años.

7.1. PLAZOS DE RESPUESTA

Durante el periodo de garantía establecido en el punto 25 de la Carátula, el contratista deberá cumplir los siguientes plazos de respuesta ante incidencias:

- **Incidencias críticas** (aquellas que comprometan la seguridad de la red, la disponibilidad del servicio o el funcionamiento general del sistema):
    - Tiempo máximo de **respuesta**: **2 horas laborables** desde la notificación por parte de CICC.
    - Tiempo máximo de **resolución** (o propuesta de solución temporal): **3 días laborables** a contar desde la notificación por parte de CICC.

- **Incidencias no críticas** (fallos menores, ajustes o dudas sin impacto inmediato en la seguridad o funcionamiento):
    - Tiempo máximo de **respuesta: 24 horas** laborables desde la notificación por parte de CICC.
    - Tiempo máximo de **resolución: 5 días** laborables desde la notificación por parte de CICC.

Los plazos y servicios de soporte indicados en este apartado se entenderán incluidos en el precio del contrato, sin coste adicional para CICC, sin perjuicio de ampliaciones o servicios adicionales que, en su caso, CICC pudiera solicitar expresamente y que no estén previstos en el presente Pliego.

Se entenderán por Horas Laborables aquellas que transcurran de Lunes a Viernes, de 8:00 a 18:00 horas, excluyendo las horas que transcurran los días festivos nacionales, autonómicos y locales de Donostia / San Sebastián. Asimismo, se entenderán por días laborales, aquellos que transcurran de lunes a viernes, excluyendo los días festivos nacionales, autonómicos y locales de Donostia / San Sebastián.