

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO E IMPLANTACIÓN DE EQUIPAMIENTO Y SERVICIOS DE MANTENIMIENTO DE LA INFRAESTRUCTURA DE COMUNICACIONES Y CIBERSEGURIDAD DE TALLER USOA LANTEGIA, S.A.U.M.P.



ÍNDICE

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO E IMPLANTACIÓN DE EQUIPAMIENTO Y SERVICIOS DE MANTENIMIENTO DE LA INFRAESTRUCTURA DE COMUNICACIONES Y CIBERSEGURIDAD DE TALLER USOA LANTEGIA, S.A.U.M.P.	1
Previo.- Del marco regulatorio vigente	3
Cláusula 1.- Introducción	3
Cláusula 2.- Objeto del contrato	3
2.2 Suministro de la infraestructura necesaria	4
2.3 Servicios profesionales	4
2.3.1 Servicios asociados a la implantación de la solución	4
2.3.2 Servicios de fabricante	4
Cláusula 3.- Características técnicas	4
3.1. Consideraciones	4
3.2. Requisitos técnicos de la solución	5
3.2.1 Sistema de cortafuegos	5
3.2.1.1 Características técnicas	6
3.2.1.1.1 Características generales	6
3.2.1.1.2 Características de red	8
3.2.1.1.3 Rendimiento	8
3.2.1.1.4 Factor de forma e interfaces	9
3.2.1.1.5 Punto de acceso inalámbrico adicional	9
3.2.1.1.6 Soporte del fabricante	10
3.2.2 Software de seguridad para puestos de trabajo y servidores	10
3.2.2.1 Activos a proteger	10
3.2.2.2 Ubicación de la plataforma	10
3.2.2.3 Componentes del servicio	10
3.2.2.4 Protección	12
3.2.2.4.1 Endpoint Protection Platform (EPP)	12
3.2.2.4.2 Endpoint Detection and Response (EDR)	12
3.2.2.4.3 Servicio de caza de amenazas (Threat Hunting)	13
3.2.2.4.4 Módulos adicionales requeridos	13
3.2.2.4.5 Agente para plataforma unificada de gestión	13
3.2.2.5 Esquema Nacional de Seguridad	14
3.2.2.6 Información	14
3.2.2.7 Soporte Técnico 24x7x365 por parte del fabricante	14
3.3. Servicios requeridos	15
3.3.1. Servicios de implantación	15

Previo.- Del marco regulatorio vigente

Taller Usoa Lantegia, S.A.U.M.P. (en adelante, USOA) se encuentra dentro del ámbito objetivo de aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en atención a su consideración de entidad perteneciente al Sector Público.

El Esquema Nacional de Seguridad (ENS) persigue los siguientes grandes objetivos:

- Crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Promover la gestión continuada de la seguridad.
- Promover la prevención, detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques.

El mandato principal del ENS es el establecido en el artículo 12 'Política de seguridad y requisitos mínimos de seguridad', según el cual *"cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente"*, la cual *"es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta"* y se establecerá de acuerdo con los principios básicos y se desarrollará aplicando los requisitos mínimos, en proporción a los riesgos identificados en cada sistema.

Cláusula 1.- Introducción

En virtud de la normativa expuesta, USOA requiere evolucionar la infraestructura y servicios de sus comunicaciones y seguridad informática para adaptarla a las nuevas exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La información es un activo estratégico para USOA, y debe ser adecuadamente protegida, sea cual sea la forma en la que esté representada, almacenada o sea procesada.

En este entorno cabe destacar el papel de las Tecnologías de la Información y de las Comunicaciones (TIC) por la creciente importancia en el tratamiento de tal información, de modo que el rápido desarrollo de dichas TIC es uno de los factores principales que está permitiendo que las entidades mejoren su eficiencia, posibilitando a las personas usuarias nuevas capacidades. Pero la información y las tecnologías que la tratan están sometidas a riesgos, internos y externos, que es necesario gestionar adecuadamente para situarlos bajo umbrales aceptables.

En este campo, USOA propone renovar su infraestructura de acceso a redes, así como la ciberseguridad perimetral y del puesto de trabajo.

Cláusula 2.- Objeto del contrato

2.1 El objeto de esta contratación es la provisión de elementos de seguridad perimetral (firewall) y software de seguridad para puestos de trabajo y servidores (antivirus de nueva generación), así como los servicios de puesto en marcha, formación y mantenimiento que se describen en el presente Pliego de Prescripciones Técnicas (en adelante, PPT).

2.2 Suministro de la infraestructura necesaria

El adjudicatario deberá suministrar el nuevo equipamiento tanto hardware como software, incluyendo licencias, que sea necesario para la implantación y el correcto funcionamiento de la infraestructura de ciberseguridad de USOA.

El equipamiento suministrado cumplirá con los requisitos mínimos establecidos en el presente PPT.

2.3 Servicios profesionales

El adjudicatario prestará, al menos, los siguientes servicios, cuyas características técnicas se establecen en la Cláusula 3 del presente PPT.

2.3.1 Servicios asociados a la implantación de la solución

- a) Revisión de la solución final, del plan de trabajo y de la metodología establecida para su validación por parte de USOA.
- b) Instalación, configuración y puesta en marcha del equipamiento, de acuerdo con la arquitectura de la solución propuesta y validada.
- c) Elaboración y ejecución de un plan de pruebas que certifique la adecuada puesta en marcha de la solución.
- d) El mantenimiento durante el primer año desde la puesta en marcha de la infraestructura de comunicaciones y ciberseguridad, que incluya la atención a incidencias en días laborables de 7.30 a 16.00 horas, así como la monitorización durante las 24 horas del día todos los días del año. Este mantenimiento deberá realizarse, en todo caso, en coordinación con el que realice la empresa encargada del mantenimiento de los servidores de USOA (Centro de Proceso de Datos).
- e) Formación continuada a USOA sobre las soluciones y tecnologías desplegadas.
- f) Documentación de la solución desarrollada.

2.3.2 Servicios de fabricante

- a) Garantía y soporte de fabricante, de acuerdo con los requisitos descritos en el presente PPT con una duración de 3 años.
- b) Todo el equipamiento suministrado por el adjudicatario deberá disponer de un contrato de soporte con el correspondiente fabricante. Dicha contratación garantizará, al menos, la modalidad 8x5xNBD. Es decir, soporte técnico 8x5 y tiempo de reemplazo y sustitución hardware NBD (Next Business Day). Además del propio soporte del fabricante, durante la duración del contrato, los licitadores incluirán durante el primer año un servicio de soporte y mantenimiento adicional para la mejora de la cobertura y niveles de servicio del fabricante, en los términos dispuestos en la Cláusula 2.3.1.d) del presente PPT.
- c) La propuesta incluirá todo el software y licencias necesarias para las diferentes funcionalidades y tecnologías propuestas para 3 años en el equipamiento adquirido dentro del alcance de esta licitación.

Cláusula 3.- Características técnicas

3.1. Consideraciones

En este apartado se describen las características técnicas que conforman el objeto del contrato que el adjudicatario deberá prestar. En cualquier caso, el listado que aparece a continuación no representa una relación exhaustiva de las características del servicio a contratar.

Las referidas características técnicas o requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario), de tal modo que los licitadores podrán ampliarlos y mejorarlos en sus ofertas. El licitador puede ofertar prestaciones superiores a las solicitadas para garantizar una óptima respuesta a las necesidades presentes y futuras.

El adjudicatario aportará y describirá los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

3.2. Requisitos técnicos de la solución

La solución propuesta por el licitador incluirá, para el mantenimiento de la infraestructura de seguridad, todos aquellos elementos necesarios, tanto hardware como software, incluyendo licencias y soporte del fabricante.

A continuación, se enumeran aquellas plataformas y equipamiento que se desea evolucionar como parte de esta licitación.

Es importante puntualizar que, por razones de seguridad, las características del equipamiento actual únicamente se describen de forma somera en este PPT. En caso de que alguno de los licitadores necesitara conocer más detalles de las características del equipamiento actual, deberá ponerse en contacto con USOA, quien, en su caso, previo acuerdo de confidencialidad si fuera necesario, dará acceso a dicha información.

La solución propuesta tiene que formar parte de una plataforma de seguridad unificada que disponga de una solución EPDR certificada por el CCN, permitiendo realizar la correlación de eventos con el UTM para ofrecer un sistema unificado de operaciones de seguridad capaz de detectar y responder a incidentes de forma automática.

3.2.1 Sistema de cortafuegos

Actualmente USOA dispone de cortafuegos perimetral de capa 4, con un objetivo de protección perimetral y accesos externos VPN. Esta licitación contempla la evolución del equipamiento y sus capacidades, de forma que sea capaz de asumir crecimientos a medio plazo (en cuanto a capacidad y seguridad) y disponer de redundancia en el equipamiento, por lo que se requieren dos equipos en alta disponibilidad activo-pasivo y de otro dispositivo UTM para una oficina adicional. Además, la plataforma deberá permitir el análisis de contenidos de aplicaciones de capa 7 como la protección avanzada contra amenazas conocidas (IPS, control de aplicaciones, Antivirus, Anti-bot, URL filtering).

Asimismo, debido a la capacitación técnica del personal de USOA, así como para facilitar el manejo de la solución, el control de dichos cortafuegos debe estar ubicado en la nube, para independizarlo del acceso a Internet y de la ubicación de las personas encargadas del mismo.

La gama del fabricante ofertada deberá aparecer como certificada en la Guía de Seguridad de las TIC CCN-STIC-105 del CCN CERT (<https://www.ccn-cert.cni.es/pdf/guias/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/file.html>), conforme a Esquema Nacional de Seguridad. En caso de estar en proceso de certificación, se admitirá igualmente, debiendo aportarse la documentación necesaria para justificación de este punto.

Los equipos a suministrar, incluidos sus componentes, deberán ser nuevos. No se admitirá el suministro de equipos o componentes reparados.

El suministro, configuración e instalación del equipamiento se realizará según un plan de instalación que, previa presentación por parte del adjudicatario dentro de la siguiente semana a la firma del contrato deberá ser aprobado por el responsable del contrato designado por USOA.

El suministro, configuración e instalación de los equipos incluye:

- Transporte y emplazamiento en el lugar que se indique
- Cableado e instalación física de los equipos en el CPD según la solución propuesta
- Actualización de firmware
- Configuración de la conectividad
- Realización de las pruebas que garanticen el perfecto funcionamiento de los equipos
- Realización de las tareas de configuración y optimización que se requieran para conseguir un funcionamiento óptimo en el entorno informático existente.

El adjudicatario deberá realizar la migración de toda la configuración existente hasta la fecha de los cortafuegos actuales a la nueva plataforma, así como añadir las políticas y configuraciones necesarias para la activación y puesta en marcha de las nuevas funcionalidades no existentes con anterioridad.

Se considerará instalado y configurado el equipamiento una vez sea revisado por USOA, quedando documentado en un acta de recepción cumplimentado por las partes. Este acto servirá para acreditar la fecha de comienzo de la garantía de los equipos instalados.

Esta recepción deberá incluir copia del albarán de entrega, en el que constará el número de serie de los equipos.

La implantación se considera a todos los efectos “llave en mano”, de forma que debe quedar instalado, configurado y operativo todo el equipamiento, incluyendo los servicios asociados y el material que se necesite (transceptores, cableados, etc.).

Los servicios de instalación, configuración y puesta en marcha de los equipos deberán realizarse por un técnico certificado por el fabricante, haciendo uso de buenas prácticas, de manera que los usuarios se vean mínimamente afectados, siendo necesario presentar un Plan de Implantación que garantice este aspecto. Todos estos trabajos se realizarán en colaboración con los técnicos de USOA.

Atendiendo a la naturaleza del suministro y el servicio de soporte y mantenimiento que deben ser incluidos, para la correcta prestación se establecen 3 años como el plazo de duración del servicio de soporte por parte del fabricante.

Igualmente, la empresa adjudicataria deberá impartir la transferencia tecnológica precisa para garantizar el correcto uso del equipamiento configurado, siendo a cargo de ésta todos los gastos inherentes a dicha formación.

Estará orientada al personal técnico USOA y tendrá como objetivo que este personal adquiera las competencias necesarias para poder mantener, administrar y configurar la infraestructura propuesta. El licitador incluirá en su propuesta una descripción del plan de formación ofertado, detallando los puntos a exponer y horas formativas propuestas.

3.2.1.1 Características técnicas

Todos los sistemas UTM contarán con las siguientes características generales:

3.2.1.1.1 Características generales

- Firewall capa 7
- Inspección de paquetes stateful
- Inspección profunda de paquetes
- Firewall Proxy transparente
- Sistema de prevención de intrusiones (IPS)
- Antivirus perimetral basado firmas

- AntiSPAM
- Protección APT basada en Sandboxing en cloud
- Control de aplicaciones
- Filtrado de Web basado en categorías
- Servicios de reputación web basado en filtro de reputación IP
- Anti-phishing basado en filtro de reputación DNS
- Geolocalización que permita bloquear el tráfico E/S hacia cualquier país definido mediante lista negra.
- Integración con Directorio Activo en modo clientless
- Portal de Autenticación, para validar los accesos basado en usuarios local o integrados con servidores de autenticación externos (LDAP, AD, RADIUS, MFA).
- Aquellos servicios requieran el uso de la nube, deben estar alojados dentro de Europa cumpliendo la GDPR
- Los dispositivos deben estar incluidos en el catálogo del CCN con calificación nivel ALTO
- Varias plataformas de gestión:
 - Consola local basada en software cliente que permite generar configuraciones offline.
 - Consola local basada en WEBUI
 - CLI
 - Consola cloud de gestión centralizada y Unificada sin coste adicional
 - Herramienta monitorización dual On-premises y Cloud
 - Permite visibilidad del estado de la red mediante la interpretación de los logs generados por el sistema que permita detectar tendencias, problemas y amenazas de seguridad.
 - Branding de los informes
 - Debe incluir la posibilidad de generar informes automatizados que sean distribuidos mediante correo electrónico.
 - Ambas herramientas deben incluir sin coste adicional dentro del licenciamiento del producto.
- Herramienta que mantenga un diagrama actualizado de nuestra red de forma automática.
- La solución debe ofrecer SD-WAN con monitorización de enlaces, QoS y selección dinámica de caminos. Estas características deben tener en cuenta tanto la caída de enlaces como la calidad de la línea de forma dinámica en función del número de paquetes perdidos, la latencia y el jitter.
- Se debe incluir un segundo motor de antivirus perimetral basado en una tecnología de inteligencia artificial que detecte amenazas conocidas y desconocidas en pre-ejecución.
- El motor de análisis https debe permitir la inspección de tráfico TLS 1.3.
- El almacenamiento de los report y de los logs de monitorización de la solución debe poder realizarse on-premises y en nube de forma simultánea. En ningún caso dentro del mismo equipo, para garantizar independencia en el acceso a la información en caso de fallo físico o vulneración de los accesos administrativos.

- Posibilidad de despliegue sin necesidad de intervención previa (ZeroTouch)
- Debe disponer de una funcionalidad de verificación “Enforce Endpoint Installation” que agregue una verificación de integridad que limitan las conexiones VPN móviles a dispositivos que siguen la política corporativa.
- Se debe incluir Herramienta de detección y respuesta en puesto de trabajo para bloquear malware avanzado. Debe enviar ficheros sospechosos a sandboxing y aislar automáticamente equipos en caso de infección. La solución debe ser del mismo fabricante del UTM
- Solución avanzada contra ransomware en puesto de trabajo basada en comportamiento. No ha de requerir conexión a Internet para funcionar.
- Integración con servicios XDR. Se requiere que la solución del endpoint sea del mismo fabricante que la solución UTM. Esta integración debe ser gratuita no conllevar ningún coste adicional.

3.2.1.1.2 Características de red

- NAT estático, dinámico, 1-to-1
- Soporte de VLAN 802.1Q
- Soporte de VPN Site-to-site
- Soporte de hasta cuatro protocolos VPN Móviles (IKEv2, SSL, L2TP, Ipsec).
- Enrutamiento dinámico (BGP4, OSPF, RIP v1/v2)
- Balanceo de carga multiWAN (Failover, RoundRobin, Overlap).
- Balanceo de carga entre servidores
- QoS (802.1P sobre PPPoE)
- Soporte de VoIP (SIP y H.323)
- Soporte de enlaces agregados (802.x, static,..)
- Soporte de Syslog y SNMP v2/v3
- SD-WAN:
 - Monitorización de enlaces: jitter, latencia y pérdida de paquetes
 - Distribución dinámica del tráfico
 - Equilibrio de cargas
 - SD-WAN directamente desde el dispositivo para obtener un mejor desempeño y mejor resiliencia de red.
 - Capacidades para balanceo de túneles IPSec (BOVPN)
 - Soporte para marcación PPPoE
- Soporte para funciones de hotspot

3.2.1.1.3 Rendimiento

Para el equipo en clúster activo/pasivo de las oficinas centrales:

- Capacidad de filtrado firewall: 5.8 Gbps
- Capacidad de filtrado VPN: 800 Mbps
- Capacidad de filtrado antivirus: 1.4 Gbps

- Capacidad de filtrado IPS: 1.3 Gbps
- Capacidad de filtrado HTTPS (con IPS habilitado): 650 Mbps
- Capacidad de filtrado con todos los servicios de seguridad activados: 1,1 Gbps
- Número máximo de conexiones concurrentes TCP/IP: 3.500.000
- Número máximo de nuevas conexiones TCP/IP por segundo: 34.000

Para el equipo en delegación:

- Capacidad de filtrado firewall: 3,14 Gbps
- Capacidad de filtrado VPN: 300 Mbps
- Capacidad de filtrado antivirus: 470 Mbps
- Capacidad de filtrado IPS: 520 Mbps
- Capacidad de filtrado HTTPS (con IPS habilitado): 200 Mbps
- Capacidad de filtrado con todos los servicios de seguridad activados: 400 Mbps
- Número máximo de conexiones concurrentes TCP/IP: 1.300.000
- Número máximo de nuevas conexiones TCP/IP por segundo: 16.000

3.2.1.1.4 Factor de forma e interfaces

Para el equipo en clúster activo/pasivo de las oficinas centrales:

- Factor de forma: 1 unidad de rack (1U) por cada nodo del clúster
- Número de interfaces: 8 1000BASET por cada nodo del clúster

Para el equipo en delegación:

- Factor de forma: Sobremesa o enrackable (max. 1U)
- Número de interfaces: 5 1000BASET

3.2.1.1.5 Punto de acceso inalámbrico adicional

Para la delegación de Usoa, se deberá aprovisionar de un punto de acceso inalámbrico adicional, con las siguientes características:

- Mismo fabricante que el UTM, de cara a homogeneizar el soporte, la formación necesaria, garantías, etc.
- Tecnología 2,5 y 5Ghz
- Tecnología MIMO 2x2.
- Alimentación POE (se proveerá el alimentador POE)
- Soporte para VLANs, portal cautivo, portal de invitados, etc.
- Logs de acceso (para lo que se puede apoyar en la tecnología del UTM asociado).

NOTA: Este punto de acceso inalámbrico no requiere estar presente en el “Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación” (CPSTIC) Publicado por el CCN (Centro

Criptográfico Nacional). Sin embargo, se requiere todo lo anterior para mantener una cohesión con dicho catálogo de seguridad.

3.2.1.1.6 Soporte del fabricante

- 24x7 con reemplazo NBD
- En caso de RMA el fabricante asumirá los costes del transporte, del nuevo equipo y de la devolución del equipo dañado. (Solo UE)
- Soporte basado en web, email y teléfono en castellano
- Posibilidad para habilitar/deshabilitar asistencia remota del fabricante directamente al dispositivo.

3.2.2 Software de seguridad para puestos de trabajo y servidores

Actualmente USOA dispone de un despliegue de software de seguridad (antivirus) para puestos de trabajo y servidores basado en firmas.

Con esta licitación se requiere un software más avanzado, que tenga en cuenta las nuevas amenazas en ciberseguridad y los ataques Zero-Day. Además, debido a la especial naturaleza de los datos manejados en USOA, se deberá cumplir con una serie de requerimientos en relación con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3.2.2.1 Activos a proteger

La solución deberá ser capaz de proteger al menos 100 equipos (CPU)

3.2.2.2 Ubicación de la plataforma

Con el fin de reducir los costes de mantenimiento y explotación de la solución, no deberá ser necesario el uso de una plataforma interna, se precisa una solución basada en cloud. Es requisito mínimo que la plataforma donde se aloje la infraestructura se encuentre fuera de las instalaciones de USOA y operada por el fabricante de la solución en un modelo cloud, en el que no haya un inconveniente en el crecimiento y escalabilidad de la plataforma. Asegurando que independientemente del número de nodos de la instalación la plataforma funcione en el mismo nivel de eficiencia.

La ubicación de la plataforma debe estar alojada en la Unión Europea.

Existen nodos que están distribuidos por diferentes sedes e incluso en movilidad por lo cual estos aprovecharán la disponibilidad de la infraestructura cloud para que estén integrados de forma completa en la configuración y actualización de la solución.

La plataforma de gestión debe cubrir los principales niveles de certificación como, por ejemplo, la ISO 27001 para el diseño y la implantación de un Sistema de Gestión de la Seguridad de la Información.

3.2.2.3 Componentes del servicio

Infraestructura Cloud

El adjudicatario proveerá, desde la nube, el conjunto de servidores, bases de datos y procesos de tratamiento de la información relacionada con el servicio. Los procesos

capturados de los clientes serán tratados en la nube de tal forma que el impacto sobre los sistemas corporativos sea mínimo. La gestión de los equipos se realizará desde la nube permitiendo que puedan ser gestionados equipos en diferentes ubicaciones e incluso en movilidad

Agente, a desplegar en los equipos.

El agente desplegado permitirá la comunicación y gestión de tanto la protección de antivirus tradicional, así como de la protección de procesos desconocidos y la gestión y conexión remota a los equipos.

Recogerá la información correspondiente a los eventos y los componentes que los producen, sin recopilar información, ni documentos de usuario. El impacto sobre los dispositivos del parque deberá ser menor al 5 % de rendimiento de la CPU, memoria y disco

El agente debe ser capaz de proteger equipos de sobremesa y portátiles con los siguientes sistemas operativos:

Sistemas operativos soportados

Estaciones de trabajo

- Windows XP SP3 (32 bits)
- Windows Vista (32 y 64 bits)
- Windows 7 (32 y 64 bits)
- Windows 8 (32 y 64 bits)
- Windows 8.1 (32 y 64 bits)
- Windows 10 (32 y 64 bits)
- Windows 11 (64 bits)

Servidores

- Windows 2003 (32, 64-bit y R2) SP2 y superiores
- Windows 2008 (32 y 64-bit) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012, 2012 R2
- Windows Server 2016 y 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 y 2019
- Windows Server 2022 (64-bit)

La desinstalación de la protección deberá protegerse mediante contraseña.

La solución debe poder desplegarse de manera silenciosa mediante los siguientes mecanismos: por dirección IP, rango de direcciones IP, nombre de máquina y grupos de Directorio Activo de Microsoft basado en políticas de dominio.

Consola Web

El adjudicatario proporcionará un interfaz en el que se puedan consultar datos en tiempo real, descargar informes/alertas, acceder a la configuración y políticas y disponer de las actualizaciones de los agentes.

Los administradores del servicio podrán gestionar desde una única consola y de manera centralizada, mediante cualquier navegador web la seguridad y productividad de todas las estaciones de trabajo y servidores Windows incluso ordenadores portátiles y oficinas remotas.

3.2.2.4 Protección

La protección solicitada se dividirá en dos partes:

- Endpoint Protection Platform (EPP)
- Endpoint detection and response (EDR)

Las dos primeras partes deben estarán combinadas y fusionadas a nivel de configuración, tan solo estarán divididas a nivel de funcionalidades. Y estar compuesto por un solo agente y solución. No se permitirá el uso de diferentes componentes. Con el fin de conseguir una protección contra amenazas desconocidas en la que colabore el antivirus tradicional con la protección avanzada.

3.2.2.4.1 Endpoint Protection Platform (EPP)

Se requiere una solución de EPP (Endpoint Protection Platform) con las siguientes funcionalidades:

- Antivirus para archivos, correo y web. Permitiendo la detección y desinfección de cualquier tipo de amenaza. Detectando malware por comportamiento. El correo detectara en POP3. En cuanto a la protección web se detectarán los intentos de acceso a páginas web que contengan elementos maliciosos, bloqueándolos.
- Firewall personal gestionado en local o de forma centralizada desde la consola web. Debe permitir:
 - Bloquear las conexiones entrantes y/o salientes de las aplicaciones que desee
 - Prevención de intrusiones
 - Crear reglas de firewall para permitir/denegar el tráfico en sentido entrante/saliente de las máquinas que quiera para los protocolos/puertos que desee.
- Bloqueo de todos los dispositivos o dispositivos específicos (unidades de almacenamiento extraíbles, dispositivos de captura de imágenes, unidades de CD/DVD, módems USB, Bluetooth, etc.), impidiendo la entrada de malware y fugas de información. Permitiendo la definición de diferentes acciones para cada tipo de dispositivo (bloqueo, acceso, lectura/escritura).
- Bloqueo de acceso a páginas web no deseadas. Deberá ser posible configurar esta protección basada en categorías, aunque se podrán también añadir listas blancas y negras de sitios y dominios permitidos.

3.2.2.4.2 Endpoint Detection and Response (EDR)

Se requiere una solución de tipo EDR (endpoint detection and response) para proteger de las siguientes amenazas:

- Malware avanzado
- PUP (potential unwanted programs)
- Amenazas zeroday tipo ransomware
- Decoy files
- Shadow Copies
- Troyanos de nueva generación indetectables por los antivirus.

Esta solución tendrá que evitar al máximo las infecciones de forma proactiva, nunca reactiva. La solución debe aportar contramedidas diferentes a las siguientes:

- Firmas locales, que requieren de constantes actualizaciones
- Motores heurísticos, que necesitan de un uso de CPU y pueden producir falsos positivos.
- Sistemas de listas blancas, ya que no disponemos de personal suficiente para la administración de este tipo de sistemas.
- Sistemas de sandboxing que consume recursos y el malware puede eludirlos.

El sistema de protección tiene que ser capaz de clasificar el 100% de los procesos ejecutados en las máquinas, generando una clasificación de malware o goodware.

Es un requisito que se produzca el bloqueo de los procesos desconocidos que se intente ejecutar para evitar la posibilidad de dañar los datos accesibles por la máquina (como puede ser el cifrado no deseado) o el robo o acceso de datos.

Debe incluir un sistema Anti-Exploit que permite la detección y bloqueo del uso de exploits conocidos o desconocidos.

Se debe poder establecer diferentes niveles de bloqueo (más o menos restrictivos) así como diferentes niveles en la capacidad de los usuarios de poder desbloquear individualmente los procesos bloqueados por el sistema.

La solución debe incluir la posibilidad de bloquear aplicaciones por nombre y por hash que el administrador desee.

3.2.2.4.3 Servicio de caza de amenazas (Threat Hunting)

Se requiere un servicio que alerte y tome las medidas correctivas adecuadas cuando sea detectado una actividad anómala en los equipos basada en el comportamiento normal auditado anteriormente en el parque de equipos.

Este servicio deberá estar ofrecido por el fabricante de la solución EDR por técnicos especializados usando los datos que haya recogido en la auditoría forense.

Deben poder realizar la alerta y la inclusión en la inteligencia del sistema EDR de las medidas correctivas

3.2.2.4.4 Módulos adicionales requeridos

Se requiere que la solución escogida disponga de módulos adicionales para ampliar las funcionalidades en ciberseguridad:

- Gestión de parches de sistema operativo y terceros
- Gestión de control de datos.

3.2.2.4.5 Agente para plataforma unificada de gestión

Se requiere que la solución escogida disponga de un agente específico adicional, centrado en la gestión del parque de servidores y endpoints, con las siguientes características:

- Inventariado tanto de hardware como de software.
- Automatización y distribución de parches de seguridad, políticas, scripts, etc.
- Control remoto.
- Alertas de estado, monitorización.
- Herramientas de ticketing

3.2.2.5 Esquema Nacional de Seguridad

La solución obligatoriamente tiene que estar incluida en el “Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación.” (CPSTIC) Publicado por el CCN (Centro Criptográfico Nacional), dentro de la familia de protección del Puesto de Trabajo como CUALIFICADO.

Tecnología Cloud Pública, es obligatoria que tenga la certificación de conformidad frente al ENS, de categoría alta.

3.2.2.6 Información

El sistema debe generar información forense relacionada con cada equipo de tal forma que pueda ser explotada posteriormente. El sistema deberá incluir informe por amenaza detectada en la que se correlacione las acciones que ha hecho el proceso o en el contexto que ha estado envuelto, por ejemplo, si ha sido descargado de Internet o ha sido extraído de un fichero comprimido. Se valorará mucho un entorno amigable y fácil de seguir, sin exigir grandes conocimientos de amenazas avanzadas. Además, debe incluir informes de estado de las protecciones, de las detecciones de malware y algún informe ejecutivo con el resumen de la información global.

Los informes se deben de poder obtener de forma inmediata con los datos en tiempo real y también de forma periódica por correo electrónico y en diferentes formatos para su posterior tratamiento.

3.2.2.7 Soporte Técnico 24x7x365 por parte del fabricante

Se establecerá el mantenimiento y asistencia técnica que permita asegurar el correcto funcionamiento en todos los puestos y servidores de la organización. Mediante:

- Servicio de soporte ofrecido por el fabricante por teléfono en castellano.
- Service Packs y hotfixes: Acceso a las mejoras técnicas del producto durante el tiempo de activación del servicio
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, enciclopedia de virus...
- Soporte técnico vía email 24x7x365, por técnicos certificados en la solución implementada
- Acceso a análisis online de virus ocultos
- Acceso ilimitado al Helpdesk: sin límite de incidencias.

3.3. Servicios requeridos

3.3.1. Servicios de implantación

De forma complementaria al suministro del equipamiento cuyos requisitos se han descrito en apartados anteriores, el licitador deberá proporcionar y describir los servicios de implantación asociados a cada una de las plataformas descritas anteriormente, considerando los siguientes puntos dentro del alcance de cada uno de los proyectos de implantación asociados.

- a) Fase de diseño que abordará la viabilidad, así como la definición del procedimiento de migración minimizando el impacto en el servicio.
- b) Implantación de la solución y migración de los servicios actuales a las nuevas plataformas.
 - i. Suministro de equipamiento hardware y software, así como licencias.
 - ii. Despliegue de la nueva infraestructura.
 - iii. Definición de la configuración y/o migración de la configuración actual al nuevo equipamiento en los casos de evolución, siguiendo las mejores prácticas de diseño siempre que sea posible. En la solución de seguridad perimetral para aumentar el nivel de seguridad, se requiere una política de Nivel 7.
- c) Plan de pruebas y puesta en producción. Deberá considerarse en la propuesta que, en caso de necesidad, y dependiendo del impacto de la puesta en producción, ciertas acciones podrán llevarse a cabo fuera del horario habitual del servicio, que será el siguiente: 07:30 a 16:00 horas durante los meses de enero, febrero, marzo, abril, mayo, octubre, noviembre y diciembre, y de 07:30 a 14.30 horas durante los meses de junio, julio, agosto y septiembre.
- d) Formación continuada de la solución instalada al personal de USOA.
- e) Documentación de la solución desplegada.
- f) El licitador definirá claramente el plazo de implantación de la solución, de la forma más detallada posible.