Ayuntamiento de Córdoba

DEPARTAMENTO DE SERVICIOS INFORMÁTICOS

Pliego de condiciones técnicas para la adquisición e implantación de un nuevo sistema de seguridad perimetral basado en un Firewall de Nueva Generación NGFW

Diciembre 2014

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	1/22

+E1gpoIWXl33gmqoDXP1XA==

Tabla de contenido

1. Justificación....3
2. Antecedentes....4
3. Objeto....5
4. Características técnicas....5

CARACTERÍSTICAS HARDWARE DE LOS EQUIPOS....6

ESPECIFICACIONES DE RENDIMIENTO Y CAPACIDAD....6

4.1. Cortafuegos o firewall de N7. Funcionalidades y características....9

4.3. Protección frente a intrusos IPS/IDS....13

4.4. Antivirus....14

4.5. Antimalware....15

4.6. Filtrado web de URLs para navegación, para tráfico HTTP y HTTPS....16

4.7. Generación de Informes y monitorización....16

4.8. Gestión y administración centralizada....17

5. Servicios de mantenimiento y garantía....18
6. Alcance del proyecto....20
7. Plazo de ejecución....21

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	2/22

+E1gpoIWXl33gmqoDXP1XA==

1. Justificación

La situación actual de las redes de datos, compuestas por numerosos elementos de red, soportando varios tipos de servicios como voz, datos y video, cada uno con unos requerimientos diferentes, y proporcionando accesos tanto a usuarios dentro de la red como a usuarios externos, e interconectadas con redes de otros organismos y, por otra parte, la evolución de los virus, ataques y amenazas procedentes de Internet o de los propios usuarios de la red, hacen necesario elaborar una estrategia completa de seguridad en varios niveles o capas, aplicando las correspondientes medidas de seguridad en cada nivel, como establece el ENS.

Hay que tener en cuenta que un fallo o un ataque a un componente de la red puede producir una caída en todo el sistema, si no se ponen los medios necesarios para prevenirlos o paliar sus consecuencias. El impacto de un fallo en la red puede implicar diversos niveles de gravedad, desde tiempo de inactividad de la red, los sistemas y aplicaciones que soporta, hasta pérdidas económicas o deterioro del prestigio de la organización.

Uno de los principios básicos del ENS es lo que se denomina **líneas de defensa** o **seguridad en profundidad**, que consiste en que la red ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

1. Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
2. Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
3. Minimizar el impacto final sobre el sistema.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

La norma del ENS [MP.COM.1] de Protección de las Comunicaciones dice:

- Se debe disponer de cortafuegos que separen la red interna del exterior. Todo el tráfico deberá atravesar dichos cortafuegos, que sólo dejarán transitar los flujos previamente autorizados.
- Cuando se requieran niveles de seguridad alta, el sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada, además, cada uno de ellos montados de forma redundante.

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	3/22

+E1gpoIWXl33gmqoDXP1XA==

Por tanto, una de las **medidas principales de seguridad**, de mayor impacto a todos los niveles, consiste en disponer de un **sistema de seguridad perimetral** eficiente, que proteja la red corporativa frente a los virus, ataques y amenazas que actualmente provienen de Internet o de la propia red interna.

El objeto de este pliego de condiciones es la contratación de un sistema adicional de **firewall o cortafuegos de nueva generación** (**NGFW**, *next generation firewall*), que complementará al actual y se convertirá así en el dispositivo de seguridad de mayor importancia estratégica de la red.

El Firewall de nueva generación (NGFW) realizará las funciones de cortafuegos a nivel de aplicación (nivel 7 OSI), sistema de prevención de intrusiones (IPS), filtrado de URLs, antimalware y antivirus perimetral, entre otras, identificando correctamente las aplicaciones que están circulando por la red, los usuarios que las ejecutan, así como las amenazas provenientes de Internet o la propia Intranet, sean del tipo que sean, y filtrando correctamente el acceso a páginas web, seguras (HTTPS) y no seguras (HTTP).

2. Antecedentes

Desde el año 2012, el Ayuntamiento de córdoba viene utilizando como sistema de seguridad perimetral un firewall o cortafuegos de CheckPoint modelo 4600. El sistema de firewall actualmente instalado en el Ayuntamiento de Córdoba es un firewall tradicional de capa de red o de filtrado de paquetes. Éste identifica y controla el tráfico basándose únicamente en las direcciones IP origen, IP destino y puerto.

Con el montaje actual del cortafuegos se controla el tráfico desde los usuarios de Internet a los servidores web del Ayuntamiento, instalados en la DMZ; el tráfico de navegación a Internet de los usuarios internos o de las redes wifi; el tráfico desde los servidores web hacia servidores internos, principalmente servidores de base de datos y el tráfico desde las aplicaciones corporativas o bien de los mismos usuarios a los servicios publicados en la red Eprinet/Sara/Nerea.

Una de las principales deficiencias de este sistema, debida al propio diseño interno del mismo, consiste en que el sistema no distingue y, por tanto, no permite controlar de forma diferenciada los flujos de tráfico. Este sistema no es capaz de aplicar distintas políticas de filtrado a los diferentes flujos de tráfico, esto es, el tráfico desde Internet a los servidores web del Ayuntamiento y el tráfico de navegación de los usuarios, deben compartir las mismas políticas de filtrado, antivirus, IPS, etc. Esta

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	4/22

+E1gpoIWXl33gmqoDXP1XA==

falta de granularidad en la diferenciación de los flujos de tráfico que pasan por el firewall nos impide utilizar las herramientas de filtrado de forma eficiente.

El funcionamiento del sistema actualmente instalado no permite aplicar de forma eficiente y fácil de administrar las políticas de filtrado a nivel de aplicación (nivel 7), filtrado del tráfico cifrado (HTTPs, SSL) y prevención de malware moderno, que consideramos imprescindibles para la protección de la red corporativa frente al estado actual de las amenazas procedentes de Internet y la propia red interna.

3. Objeto

El objeto de este Pliego de Condiciones Técnicas es establecer los requisitos técnicos para la contratación de un **sistema de protección perimetral** para la red corporativa del Ayuntamiento de Córdoba, consistente en el **suministro, instalación, configuración y puesta en marcha de todos los módulos, subsistemas y elementos constituyentes de un Sistema de Seguridad Perimetral de nueva generación (NGFW),** que la proteja frente a las diversas amenazas que provienen de Internet o de la propia red interna. Dicho servicio conlleva la instalación en las oficinas del CPD del Ayuntamiento de Córdoba de al menos dos dispositivos físicos, que no constarían como propiedad del Ayuntamiento, ya que únicamente prestan el servicio de cortafuegos si se contratan las suscripciones o licencias de uso correspondientes a las diferentes funcionalidades que se solicitan en el apartado 4, quedando inutilizables si no se contratan dichos servicios y suscripciones y se renuevan anualmente.

4. Características técnicas

El sistema presentará las siguientes funcionalidades o herramientas:

1. Cortafuegos o firewall de nivel 7
2. Supervisión y control del ancho de banda
3. Protección frente a intrusos IPS/IDS
4. Antivirus
5. Antimalware
6. Filtrado web de URLs para navegación, tanto para tráfico HTTP como HTTPS.
7. Generación de Informes
8. Gestión y administración centralizadas

El sistema estará formado al menos por 2 dispositivos de iguales características, con funcionamiento en alta disponibilidad (activo-pasivo) o en equilibrio de carga (activo-activo) con administración centralizada vía web y deberá incluir una herramienta de

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	5/22

+E1gpoIWXl33gmqoDXP1XA==

monitorización configurable en tiempo real. Las anteriores funcionalidades, cuyos requerimientos se irán detallando en los apartados siguientes, estarán integradas en cada uno de los dispositivos iguales de los que consta el sistema y configuradas de forma exactamente igual.

El diseño del sistema debe proporcionar la seguridad necesaria para realizar las funciones de sistema de seguridad perimetral, filtrado de tráfico, prevención de amenazas y gestión, sobre una plataforma que permita una baja latencia, integrada con un motor de exploración software de única pasada con el fin de maximizar el rendimiento. El plano de gestión y el de datos deben estar separados en el diseño de la arquitectura del sistema, para asegurar que el acceso a la gestión esté siempre disponible, independientemente de la carga de tráfico.

CARACTERÍSTICAS HARDWARE DE LOS EQUIPOS

Las **características técnicas mínimas** del hardware de los equipos serán las siguientes:

- Arquitectura hardware separada para la gestión y el filtrado de tráfico (plano de datos).
- 12 puertos Ethernet 10/100/1000 RJ45.
- 8 puertos Gigabit SFP.
- Disco duro SSD de 120 GB.
- Puerto dedicado para gestión “out-of-band”.
- Puerto de consola RJ45.

ESPECIFICACIONES DE RENDIMIENTO Y CAPACIDAD

Los dispositivos ofertados deberán presentar las siguientes **características mínimas** en cuanto al rendimiento y capacidad:

- *Throughput* (capacidad de procesado de tráfico) del firewall con la identificación de aplicaciones habilitada al 100% (es decir, trabajando a nivel 7 para todo el tráfico): **4 Gbps**
- *Throughput* de la cadena de filtros de prevención de amenazas: IDS/IPS + Antivirus + AntiSpyware + URL filtering + FileBlocking, con el 100% de las firmas disponibles aplicadas sobre cada uno de los filtros: **2 Gbps**
- Rendimiento de VPN basado en IPSEC: 500 Mbps
- Soporte de nuevas sesiones por segundo: 50.000
- Sesiones totales concurrentes: 500.000
- Num. de Túneles Ipsec VPN: 2.000

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	6/22

+E1gpoIWXl33gmqoDXP1XA==

- Núm. usuarios concurrentes SSL VPN: 2.000
- *Virtual Routers* (enrutadores virtuales): 10
- Sistemas virtuales (licencia opcional): 6
- Num. zonas de seguridad: 40
- Num. políticas: 5.000

ESPECIFICACIONES DE NETWORKING

En cuanto al soporte de protocolos de red, deberán ser los siguientes como mínimo:

- Soporte de VLANs con el protocolo IEEE 802.1Q.
- Soporte de protocolos de routing: OSPF, RIPv2, BGP.
- Soporte de NAT y PAT.
- Soporte de *Policy Based Routing*, pudiendo hacerlo basado en:
  - la ip de origen o red
  - la aplicación, categoría o grupo de aplicación
  - el usuario o grupo de usuarios.
- Site to site VPNs (IPSEC).
- SSL VPNs.
- DHCP server/ DHCP relay.
- Alta disponibilidad activo/pasivo y activo/activo.
- *Virtual Routers* (enrutadores virtuales).
- Sistemas virtuales (aunque con licencia opcional). Esta funcionalidad permitiría ejecutar distintas instancias de firewall en un único dispositivo, de forma que cada uno de los sistemas virtuales sea independiente y sea gestionado de forma separada.
- Security Zones. Esto es, arquitectura basada en zonas.

CARACTERÍSTICAS GENERALES DE SEGURIDAD

Como características y funcionalidades generales de seguridad, los equipos deberán presentar al menos las siguientes:

- **Arquitectura de seguridad basada en zonas**, para la aplicación de políticas de seguridad y filtrado independientes.
- Capacidad para definir múltiples reglas de seguridad en las zonas origen/destino, incluyendo “any”. También capacidad para crear reglas con varias zonas origen/destino.
- Soporte de varios modos de funcionamiento y capacidad de activarse simultáneamente en diferentes interfaces:
  - Modo transparente para despliegue *in-line* (*bridging*).
  - Funcionamiento en nivel 2/nivel 3.

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	7/22

+E1gpoIWXl33gmqoDXP1XA==

- Modo TAP o modo IDS, para detectar problemas y permitir la generación de informes sin afectar el funcionamiento de la red.

- Prevención de amenazas en tiempo real, detectando un amplio rango de malware y exploits de vulnerabilidades (virus, spyware, gusanos, etc) sin incurrir en latencia, efectuando la **exploración en una única pasada** para todo tipo de amenazas.
- Uso de la aplicación como criterio principal de selección del perfil de inspección (IPS, AntiVirus, FileBlocking …) con el objetivo de poder implementar políticas, como por ejemplo:
  - Inspeccionar con antivirus las conexiones http excepto cuando la aplicación sea Apple-Store o Google-Play.
  - Impedir el intercambio de ficheros tipo EXE, DLL u otros códigos ejecutables sobre conexiones http excepto cuando la aplicación sea Amazon-Drive o Google-Drive.
  - Permitir el upload de ficheros tipo MS-Office únicamente cuando la aplicación usada sea Sharepoint.
- Tiempo de latencia con reglas integradas: firewall + antivirus + ips/ids + url filtering, no superior a 1 milisegundos.
- Funcionamiento como IPS/IDS.
- Definición de la identificación CVE de las vulnerabilidades detectadas.
- Control de transferencias no autorizadas de ficheros o datos críticos, mediante una arquitectura basada en stream en vez de en tipos de fichero, realizando el análisis en línea tan pronto como el primer paquete llega al motor de escaneo.
- Bloqueo de ficheros por tipo, identificando por el tipo MIME y no basándose en la extensión del fichero.
- DLP: capacidad de búsqueda de patrones como tarjetas de crédito, etc., así como de cadenas concretas.
- Método basado en pesos para evitar falsos positivos.
- Monitorización y control de la navegación web, sin penalizar el tiempo de respuesta ni la satisfacción del usuario.
- Toma de decisiones en tiempo real como permitir / denegar una URL basándose en políticas y en una base de datos de URLs mundiales integrada, que permita establecer controles para un filtrado granular de las URLs.
- Desplegar políticas para monitorizar y controlar las aplicaciones desde un único interfaz de gestión.
- Capacidad para crear informes sin necesidad de equipamiento externo o auxiliar.
- Licenciamiento por equipos, no por usuarios.
- Capacidad para actuar como concentrador de túneles SSL VPN.
- Aplicación de Calidad de Servicio (QoS) por usuario, aplicación, zona, etc.
- Descarga y aplicación automática de actualizaciones de las firmas antivirus, antispyware, base de datos de URLs, firmas IDS/IPS y de las nuevas aplicaciones identificadas.

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	8/22

+E1gpoIWXl33gmqoDXP1XA==

❖ Servicio en la nube para la identificación y análisis de malware moderno desconocido con tecnología de sandboxing en un máximo de 3 horas, dirigido contra objetivos concretos, y que por tanto no tiene gran incidencia en cuanto al número de instancias que se observan. Debe ser posible inspeccionar al menos ficheros APK (Android), EXE, DLL, Office, Java y PDF. Disponer de una consola al servicio para poder obtener información del resultado de las muestras aportadas y opción para poder integrar los veredictos en el log del Firewall.

4.1. Cortafuegos o firewall de N7. Funcionalidades y características.

El Firewall de Nueva Generación NGFW ofertado debe resolver las siguientes necesidades o casuística general:

- Posibilidad de aplicar diferentes perfiles de seguridad (IPS, File Blocking, Spyware, Virus …) al tráfico de diferentes aplicaciones, incluso cuando estas aplicaciones se sirvan desde el mismo servidor web (misma dirección IP, mismo puerto TCP). Esto es, el NGFW debe permitir diferenciar los flujos de tráfico y aplicar diferentes perfiles de seguridad a los mismos.
- En la publicación de aplicaciones WEB (de DMZ a Internet) el Firewall debe ser capaz de clasificar el tráfico en función de la aplicación, para asegurar que cada una de las aplicaciones publicadas tenga un trato diferenciado.
- Posibilidad de desviar el tráfico por rutas alternativas (Policy Based Routing) usando la aplicación como criterio. Conseguir, por ejemplo, que el Firewall desvíe toda la actividad Facebook por una línea ADSL a Internet diferente a la línea principal o ruta por defecto.

Se requiere que el Firewall implemente las siguientes funcionalidades:

- El Firewall debe **clasificar todo el tráfico en función de la aplicación**, de tal manera que se obtenga visibilidad de la actividad en la red en función de la aplicación que se está ejecutando en cada momento y no únicamente en función de la información de origen, destino y puerto. La clasificación del tráfico en función de la aplicación debe estar activa incluso cuando en la programación de las reglas del firewall se ignore el criterio “aplicación”.
- La identificación de las aplicaciones se debe realizar correctamente y con precisión independientemente del puerto utilizado por las mismas, el protocolo, la modificación SSL o la táctica evasiva empleada.
- El reconocimiento de aplicaciones debe ser realizado por un **motor de clasificación del tráfico en una sola pasada** y no un filtro. Es decir, el Firewall debe ser capaz de “clasificar” el tráfico entrante en base a la aplicación en una sola

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	9/22

+E1gpoIWXl33gmqoDXP1XA==

pasada, para después aplicar un “filtro” personalizado al consumo de esa aplicación (IPS, Antivirus, AntiSpyware, FileBlocking, etc.)

- Quedan expresamente excluidos aquellos firewalls que no permitan aplicar un perfil de seguridad diferente (filtro) a aplicaciones que comparten atributos de red. Por ejemplo se excluirá un firewall que no pueda aplicar un perfil de “file blocking” diferente a las sesiones Facebook de las sesiones de Google-Drive.
- Posibilidad de mapear dinámicamente los usuarios con las direcciones IP, usando como fuente de información los eventos de seguridad generados por sistemas de confianza como Domain Controllers.
- Posibilidad de obtener dinámicamente agrupaciones de usuarios usando directorios LDAP.
- Identificación, descifrado, inspección y control del tráfico SSL, para garantizar que las aplicaciones no se enmascaren y las amenazas no se escondan dentro del tráfico SSL.
- Capacidad (aunque fuere con licencia opcional) de mantener dinámicamente un sistema de información con los datos de plataforma de los terminales de los usuarios de la red (sistema operativo, existencia o no de antivirus, cifrado del disco …)
- Control del movimiento de ficheros (upload/download) en aquellas aplicaciones capaces de transferirlos (WebEx, SMB, SharePoint ..) y no sólo sobre las aplicaciones que comúnmente lo han soportado (web-browsing, ftp, smtp, pop3 …)
- El equipo deber incluir funcionalidades en el interfaz gráfico (WebUI) que permitan al administrador modelar aplicaciones propias. Tanto aplicaciones WEB (browser-based) como aplicaciones cliente-servidor.
- API XML abierta y documentada (RESTFul) para la integración del equipo con diferentes aplicaciones de negocio. La API debe permitir operaciones de lectura (recibir datos estadísticos), operaciones de escritura (modificar la configuración), cambios de objetos dinámicos (mapping de direcciones IP de objetos sin cambio de configuración) y la ejecución y obtención de informes (reports).
- Posibilidad (aunque fuere con licencia adicional) de habilitar el uso seguro de dispositivos móviles, con el fin de proteger el dispositivo móvil de virus, contenidos maliciosos, etc., así como determinar los recursos de red a los que puede acceder el dispositivo en un momento dado, bloqueando el acceso a recursos sensibles de la organización por parte de dispositivos y/o usuarios no autorizados, a la vez que manteniendo la privacidad de los datos personales del usuario.

Asociado a las funcionalidades anteriormente descritas, a continuación se muestra un listado detallado de características:

1. <u>Visibilidad de aplicaciones. Características detalladas:</u>

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	10/22

+E1gpoIWXl33gmqoDXP1XA==

- La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con dichas categorías/subcategorías.
- Aplicar técnicas de identificación de aplicaciones en todos los puertos TCP/UDP y no solo en los más comunes.
- Capacidad para identificar un mínimo de 1900 aplicaciones activas actuales (como por ejemplo, Webex, Sharepoint, Dropbox, Facebook, Spotify, Tuenti, Webex, Bit Torrent, SAP, Oracle, GMail, Last.Fm, Skype, Meebo, etc.).
- Posibilidad de identificar no solamente la aplicación, sino las subfunciones dentro de las aplicaciones (como por ejemplo Webex-desktop_sharing, Webex-chat, Webex-file_transfer, Facebook Chat, Facebook Apps, Linkedin-base, Linkedin-mail, …).
- Facilitar la visibilidad de detalles particulares de cada aplicación, como su nivel de riesgo, quién la está usando, cuánto tráfico está generando, cuáles son el origen y el destino, etc.
- Posibilidad de establecer criterios de filtrado sobre características de comportamiento de las aplicaciones: capacidad para transferir archivos, vulnerabilidades conocidas, capacidad para evadir la detección, propensión a consumir ancho de banda y transmisión/propagación de malware, etc.
- Habilitar controles positivos de todas las aplicaciones basándose en un amplio conjunto de criterios desde una tabla de políticas única y centralizada.
- Capacidad para identificar aplicaciones HTTP y TCP propietarias desarrolladas por los clientes.
- Capacidad para identificar las aplicaciones bajo túneles SSL.
- Capacidad para descifrar el tráfico SSH y detectar aplicaciones ilegítimas tunelizadas sobre este protocolo.
- Capacidad de crear reglas de QoS por aplicaciones y/o usuarios.

2. Identificación de Usuarios. Características detalladas:

El sistema debe resolver las siguientes necesidades respecto a la identificación de usuarios y plataformas:

- El sistema de reglas del Firewall debe permitir usar los criterios “usuario”, “grupo” y/o “plataforma” para discriminar las políticas de seguridad y así aplicar diferentes políticas de filtrado a diferentes flujos de tráfico. Permitir, por ejemplo, aplicar protección de Antivirus sólo al tráfico generado por usuarios de un determinado grupo o al generado por un determinado usuario o al generado por un determinado tipo de terminales independientemente del usuario que lo opera.
- El fabricante debe incorporar agentes software que, instalados en los servidores de terminales (Citrix o Microsoft Terminal Services), permita al Firewall

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	11/22

+E1gpoIWXl33gmqoDXP1XA==

discriminar que usuario concreto es el responsable de las conexiones generadas desde esos sistemas.

❑ Realización de análisis y generación de informes sobre la actividad de los usuarios, grupos, etc.

Para cumplir las necesidades anteriores, entre otras, el sistema ofertado debe presentar al menos las siguientes características o funcionalidades:

- Identificar usuarios, integrándose con Microsoft Active Directory, LDAP, open LDAP, etc.
- Soporte de identificación de usuarios en entornos Windows Server 2008.
- Capacidad para leer eventos de syslog recibidos de sistemas de terceros y hacer el parsing del evento para extraer la tupla usuario-IP.
- API XML para poder inyectar usuarios desde sistemas de terceros.
- Control de usuarios Citrix.
- Control de usuarios de Microsoft Terminal Server.
- Autenticación de usuarios vía RADIUS.
- Autenticar usuarios vía Portal Cautivo.
- Autenticar usuarios vía NTLM.
- Autenticar usuarios vía Kerberos.

4.2. Supervisión y control del ancho de banda

El ancho de banda es un recurso costoso y limitado, por lo que controlar su consumo es una parte vital para asegurar el buen funcionamiento de una red. El sistema debe presentar la capacidad de supervisión y control del ancho de banda en tiempo real, cumpliendo las siguientes funcionalidades:

- Catalogación del tráfico para detectar aplicaciones con consumo intensivo de ancho de banda, tales como las aplicaciones multimedia o de almacenamiento de información en la nube, con objeto de mantener el rendimiento de las aplicaciones críticas para la organización.
- Establecimiento de políticas de Calidad de Servicio (QoS) a asignar a cada flujo de tráfico, en función de la aplicación, el usuario, localización, etc.
- Visualización gráfica en tiempo real del consumo de ancho de banda, clasificado por aplicaciones y usuarios.
- Compatibilidad con *diffserv* (definido por IETF como Servicios Diferenciales).

4.3. Protección frente a intrusos IPS/IDS

La protección frente a vulnerabilidades del NGFW debe integrar un conjunto completo de funciones, entre ellas se encuentra el sistema de prevención de intrusiones (*Intrusion Prevention System, IPS*). El IPS deberá bloquear exploits de

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	12/22

+E1gpoIWXl33gmqoDXP1XA==

vulnerabilidades, tanto conocidos como desconocidos en las capas de aplicación y de red, desbordamientos en la memoria intermedia, ataques DoS y exploraciones de puertos, para evitar peligros y daños en los recursos.

Para garantizar un nivel de protección adecuada el sistema IPS/IDS deberá presentar al menos las siguientes funcionalidades:

- **Procesamiento dedicado** para que el funcionamiento del IPS no reste rendimiento a otras funciones de seguridad, lo que sí ocurre con una sola arquitectura de hardware CPU o ASIC/CPU.
- **Formato de firma uniforme,** para eliminar los procesos redundantes comunes a múltiples motores de exploración (reensamblaje de segmentos TCP, búsqueda de políticas, inspección, etc.).
- **Software de única pasada**, independientemente de los elementos de la política que estén activados para un flujo de tráfico determinado.
- Análisis de descifrador de protocolo, descifrando mediante estados el protocolo y aplicando de forma inteligente firmas para detectar exploits de vulnerabilidad.
- Comparación de patrones de estado, que detecta ataques en más de un paquete, teniendo en cuenta elementos como el orden y la secuencia de llegada.
- Detección de anomalías de protocolo.
- Análisis heurístico, que detecta paquetes y patrones de tráfico anómalos como exploraciones de puertos y limpiezas de host.
- Detección de anomalías estadísticas
- Desfragmentación de IP y reensamblaje de TCP
- Bloqueo de paquetes no válidos o malformados
- Firmas de vulnerabilidad personalizadas.
- Protección frente a ataques de denegación de servicio DoS:
  - Protección contra saturaciones (flood) SYN, ICMP, UDP y otros ataques de saturación basados en IP.
  - Detección exploraciones de puertos y limpiezas de direcciones IP, utilizadas por los atacantes para descubrir objetivos de ataques potenciales.
  - Protección contra ataques de paquetes ICM e ICMP de grandes dimensiones.

4.4. Antivirus

El sistema deberá incorporar una protección frente a virus en tiempo real, con la función de detectar y bloquear la mayoría de los tipos de virus y software malicioso a nivel de gateway perimetral, sin que estos lleguen a penetrar en la red corporativa.

El sistema deberá presentar al menos las siguientes funcionalidades:

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	13/22

+E1gpoIWXl33gmqoDXP1XA==

- Formato de firma uniforme para la exploración de virus, que elimina procesos redundantes comunes a muchas soluciones con motor de exploración.
- Actualizaciones de firmas diarias y de emergencia.
- Motor o exploración basada en flujo, para analizar el tráfico en cuanto se empiecen a recibir los primeros paquetes de un archivo, por lo que se eliminan los problemas de ejecución y latencia asociados a una exploración basada en proxy tradicional, o un procedimiento basado en archivos.
- Descompresión de ficheros (.zip, .rar) y análisis de los mismos en línea.
- Decodificación de tráfico SSL para bloquear virus integrados en el tráfico SSL.
- Análisis de botnets basados en DNS para detectar redes de malware y sitios web maliciosos que evolucionan rápidamente.
- Protección contra HTML y Javascript malicioso.
- Protección contra “descargas ocultas”, que provocan que un usuario se descargue malware de forma inadvertida solamente con visitar un página web o haciendo clic en una imagen. Este mecanismo de propagación de malware es cada vez más popular y se conoce como "descargas ocultas".

Consideramos una característica esencial la ***exploración basada en flujo***, con el fin de proteger la red con un bajo nivel de latencia, punto que constituye una debilidad en otras tecnologías de antivirus de red, puesto que dependen de la exploración basada en proxy, que ralentiza mucho más el análisis del tráfico.

4.5. Antimalware

El *malware* actual ha cambiado la forma de ataque a las redes. En la actualidad, los ataques son mucho más sofisticados y permiten a los delincuentes atacar y robar los activos valiosos de una organización con el fin de extorsionar a la misma o bien deteriorar su prestigio. Al evolucionar las nuevas técnicas de ataque para evitar los tradicionales firewall y controles antivirus, este nuevo tipo de software malicioso permite a los atacantes infectar un objetivo interno y, ya desde el interior y con menos controles, atacar el resto de la organización sin ser detectado.

Para detectar o bien paliar los efectos del *malware* moderno, se requiere que el sistema implemente las siguientes funcionalidades:

- Análisis de ficheros para la identificación de virus, con las funcionalidades que se detallan en el apartado 4.3.
- Exploración basada en flujo
- Análisis del malware en comparación con un sistema de firmas uniforme de malware conocido, actualizado diariamente o en caso de emergencia.
- Posibilidad de uso de tecnología Sandbox (aunque con licencia opcional), que permita al sistema Firewall enviar muestras sospechosas a la nube del fabricante para

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	14/22

+E1gpoIWXl33gmqoDXP1XA==

que se ejecuten en un entorno controlado y se puedan observar las acciones maliciosas o no de la actividad que generan. El análisis resultante debe alimentar automáticamente el sistema de firmas de virus, spyware y URL filtering con las nuevas protecciones generadas.

- Análisis de contenidos para identificar comunicaciones con los centros de control de Botnets (spyware, phonehome, adware …)
- Análisis de contenidos para identificación de vulnerabilidades tanto de cliente a servidor como de servidor a cliente.
- Protección frente a amenazas que se propagan a través de “descargas ocultas”.

4.6. Filtrado web de URLs para navegación, para tráfico HTTP y HTTPS.

El sistema deberá incorporar una herramienta de filtrado de URL basada en políticas, personalizable y totalmente integrada con una base de datos de URLs clasificadas en categorías, con el fin de permitir a los administradores aplicar políticas granulares de navegación por Internet, y así proteger al Ayuntamiento frente a un amplio espectro de riesgos legales, reguladores y pérdida de productividad de sus empleados.

El sistema de filtrado web de URLs debe presentar las siguientes funcionalidades:

- Posibilidad de programar un conjunto de reglas que permitan la navegación WEB a todos los “sites” de Internet, pero bloqueando cualquier intercambio de ficheros con aquellos “sites” categorizados como “Malware” o “unknown”.
- Permitir la creación de categorías personalizadas.
- Permitir la creación de políticas de navegación web en función de usuario o grupo de usuarios, en integración con el AD o LDAP, o ubicación.
- Base de datos de URLs local incluida, para permitir un rendimiento óptimo en búsquedas de las URLs de más frecuente acceso.
- Posibilidad de ampliar la base de datos incluida con una base de datos de la memoria caché de URLs dinámicas.
- Posibilidad de habilitar el control de ancho de banda para categorías concretas, creando políticas de QoS.
- Posibilidad de activar el descifrado SSL sólo para determinadas categorías, manteniendo el cifrado para otras categorías sensibles (salud, finanzas, etc).
- Aplicación de políticas de filtrado de URLs introducidas en los sitios de traducción como Google Translate como medios para sortear las políticas.
- Páginas de bloqueo personalizables.
- Permitir a usuarios seleccionados la anulación puntual del filtrado de URL.

4.7. Generación de Informes y monitorización

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	15/22

+E1gpoIWXl33gmqoDXP1XA==

El sistema debe permitir el análisis de incidentes de seguridad, uso de aplicaciones y patrones de tráfico de una forma simple y directa mediante informes o monitorización del tráfico en tiempo real.

El generador de informes de actividad debe ser capaz de plasmar las aplicaciones utilizadas, las categorías de URLs y las páginas de Internet visitadas, así como un listado detallado de todas las URLs visitadas durante un periodo de tiempo determinado y para cada usuario concreto.

En cuanto a la monitorización, el sistema debe mostrar en consola GUI/WEB la actividad de las aplicaciones en tiempo real, las amenazas y los usuarios, por medio de funciones de filtrado dinámicas, activado con sólo hacer clic en el valor de una celda o utilizando un generador de expresiones para definir los criterios de filtrado.

El sistema debe presentar al menos las siguientes características o funcionalidades:

- Generación de informes “out of the box” y personalizados sin necesidad de equipos externos adicionales.
- Posibilidad de utilizar modelos predefinidos de informes o de personalizarlos utilizando un generador de informes.
- Capacidad para obtener informes de actividad por usuario: aplicaciones utilizadas, sitios web visitados.
- Envío automático y programado de los informes por email.
- Capacidad para agrupar informes en un único documento PDF.
- Disponibilidad de mapa geográfico para identificar el origen y destino de los flujos y amenazas que entran y salen de la red.
- Informes sobre el ancho de banda utilizado por cada aplicación.
- Informe basado en el análisis de comportamiento del tráfico observado, para detectar máquinas posiblemente infectadas por botnets desconocidas.
- Informes sobre la actividad de los usuarios.
- Sobre la visibilidad y el reporting de la actividad: Todos los registros de tráfico (LOGs) generados por el sistema deben incorporar el atributo “aplicación”.
- Exportación de informes a formatos CSV, XML o PDF.
- Exportación de logs vía SYSLOG, FTP, SCP y TFTP.
- Capacidad para generar informes sin necesidad de equipamiento externo o auxiliar.

4.8. Gestión y administración centralizada

El sistema debe presentar las siguientes características o funcionalidades respecto a la gestión y administración del mismo:

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	16/22

+E1gpoIWXl33gmqoDXP1XA==

- Soporte de Syslog, SNMPv2 y SNMPv3.
- Administración por GUI (interfaz gráfico vía web) y CLI (línea de comando).
- Creación de diferentes cuentas de administración con diferentes niveles de acceso: administrador, supervisor, operador, etc..
- Auditoría de los cambios realizados en la configuración, que permita comparar entre dos versiones de la configuración, proporcionando información sobre los cambios realizados, quién y cuándo los realizó.
- Bloqueo de cuentas de administrador si se producen intentos fallidos reiterados.
- Desplegar políticas para monitorizar y controlar las aplicaciones desde un único interfaz de gestión.
- El Firewall debe incorporar un interfaz abierto (API) para poder integrar tanto su configuración como su operativa con otros sistemas de negocio.
- Integración con NetFlow, para exportación de la información relativa al flujo de tráfico IP a un dispositivo con Netflow activado.

5. Servicios de mantenimiento y garantía

El adjudicatario deberá garantizar por un periodo mínimo de **un año** los productos derivados de la presente contratación, tanto dispositivos hardware como software, a contar desde la fecha de finalización de los trabajos, entendida como la **fecha de puesta en producción** del sistema completo, obligándose a realizar durante dicho periodo los cambios necesarios para solventar las deficiencias detectadas imputables a la firma adjudicataria.

El contrato incluirá el mantenimiento del equipamiento hardware y software suministrado y de todos los trabajos e instalaciones realizadas durante el período de garantía. El mantenimiento que llevará a cabo la empresa adjudicataria tiene como objeto garantizar el correcto funcionamiento del sistema, de todos los servicios, equipos y subsistemas que lo integran, asegurando la completa disponibilidad y continuidad de servicio.

Este servicio incluirá la subsanación de errores o fallos ocultos que se pongan de manifiesto en la puesta en producción del sistema, la configuración del mismo o que se descubran mediante pruebas o cualesquiera otros medios, la sustitución de materiales defectuosos, así como la conclusión de la documentación incompleta y subsanación de la que contenga deficiencias.

El adjudicatario queda obligado a realizar, como mínimo, las tareas de mantenimiento **preventivo** y **correctivo** (reparación del hardware/software averiado) en remoto o “in-situ” necesarias durante el plazo de duración de la garantía.

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	17/22

+E1gpoIWXl33gmqoDXP1XA==

La garantía y mantenimiento del sistema se ajustarán a las siguientes condiciones:

- Los equipos y el software instalados tendrán un plazo de garantía mínima de 1 año.
- El servicio de mantenimiento tendrá una duración mínima de 1 año.
- La subsanación de los fallos o errores software debe incluirse en el servicio de mantenimiento.
- Los equipos nuevos que, en su caso, sustituyeran a los averiados durante el periodo de cobertura de la garantía tendrán un plazo de garantía de 1 año, contados desde la fecha de puesta en servicio.
- Si la avería detectada en un equipo o material es lo suficientemente grave como para provocar la degradación del servicio, el elemento deberá ser sustituido por otro de la misma marca y modelo igual o superior, completamente nuevo.
- Se considera que un equipo o componente averiado ha sido reparado cuando recupera la funcionalidad y prestaciones que anteriormente tenía. En caso de que no se pueda realizar la total reparación del equipo, se sustituirá por otro de la misma marca y modelo, o si no es posible, de superiores características.
- Dentro del período de garantía podrá ser devuelto el producto si se detecta que no cumple con alguno de los requisitos de este pliego.
- El licitador deberá garantizar la disponibilidad de repuestos para todos los sistemas y equipos ofertados durante un periodo mínimo de cinco años.

Los licitadores deberán especificar en su oferta la garantía del fabricante para los componentes del sistema considerados individualmente, especificando tanto la duración como la cobertura de la misma.

La oferta deberá contener un completo detalle del "Plan de mantenimiento", donde hará constar los niveles de servicio (periodo de atención, tiempos de respuesta, etc.) para cualquier tipo de avería, designando un punto de atención único ante incidencias o fallos del sistema (teléfono, web y/o email), con indicación los medios disponibles (tanto en horario de trabajo como nocturno y festivos), estructuras, material de contingencias, etc.

El mantenimiento se prestará como mínimo en las siguientes condiciones:

	Situaciones críticas	**Situaciones de criticidad media**	**Cambios de configuración**
Horario de atención	24x7	24x7	8x5
Tiempo máx. respuesta	10 minutos	15 minutos	2 horas

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	18/22

+E1gpoIWXl33gmqoDXP1XA==

Tiempo máx. atención in situ/remota	1 hora	8 horas attn remota NBD attn in situ	NBD (*next business day* : siguiente día laborable)
Tiempo máx. Resolución (*)	4 horas	NBD	48 horas (2 NBD)

(*)Tiempo máximo de resolución o establecimiento de medidas provisionales para paliar los efectos de la incidencia.

Se consideran **situaciones críticas** las producidas por fallos mayores del sistema. Este nivel se activará cuando se produzca un interrupción total del servicio, esto es, que los dos dispositivos que componen el sistema fallen simultáneamente por causas internas a los mismos.

Se consideran **situaciones de criticidad media** las producidas por fallos parciales del sistema. Este nivel se activará cuando el sistema presente un funcionamiento degradado, pero que permita seguir prestando el servicio.

El licitador deberá disponer de un Centro de Recepción de Incidencias las 24 horas al día durante los 365 días al año, para la recepción de las posibles incidencias que pudieran surgir y atender las peticiones de cambios de configuración.

6. Alcance del proyecto

El alcance de los trabajos especificados en este pliego comprende el suministro, instalación, configuración y puesta en marcha de todos los módulos, subsistemas y elementos constituyentes del Sistema de Seguridad Perimetral hasta garantizar su plena operatividad. Los suministros y servicios incluidos en el alcance del proyecto deberán ser todos los necesarios para el cumplimiento del objeto del contrato de acuerdo a las funcionalidades solicitadas, a la arquitectura establecida y servicios adicionales requeridos.

La solución propuesta debe cumplir siempre los requisitos y garantías que se especifican en este pliego, y presentar copia de los documentos que se solicitan expresamente en el pliego de cláusulas administrativas: clasificaciones de la empresa, certificados de los instaladores y la empresa, esquemas, planos, hojas técnicas de los elementos, etc.

El alcance global incluye los siguientes aspectos:

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	19/22

+E1gpoIWXl33gmqoDXP1XA==

- Replanteo previo de ingeniería.
- **Formación** en el nuevo sistema de forma presencial. La formación tendrá una duración mínima de 2 días dirigida a 3 personas sobre los aspectos fundamentales de administración del sistema, generación de informes, etc.
- Suministro de equipamiento, licencias, etc.
- Instalación del equipamiento, productos software e integración con el resto de elementos de red: dispositivos, protocolos de red, plan de direccionamiento y medidas de seguridad de la red corporativa.
- Montaje de los dispositivos asociados al sistema en los rack de comunicaciones y suministro de todos los elementos de fijación necesarios.
- Configuración de la totalidad del sistema que compone la solución, de acuerdo a las especificaciones y que como mínimo deberán incluir las funcionalidades descritas en el presente pliego.
- Programación de políticas de filtrado: firewall n7, identificación de usuarios, IPS/IDS, antivirus, antimalware, control QoS, etc.
- Pruebas de funcionamiento.
- Servicios de mantenimiento, garantía y soporte.
- Documentación asociada al sistema.
- Garantía y mantenimiento 24x7 durante 1 año.
- Asistencia técnica presencial, en los casos que fuera necesario, o remota 24x7 durante 1 año.
- Asistencia técnica para cambios de configuración y consultas técnicas Online 8x5 durante 1 año.

7. Plazo de ejecución

El plazo de ejecución del objeto del contrato será de 3 meses a contar desde el día siguiente al de la formalización del mismo, hasta garantizar la completa funcionalidad del sistema.

8. Cualificación técnica

Se requerirá que la empresa instaladora esté certificada por el correspondiente fabricante, para realizar la instalación y prestar el servicio oficial del fabricante.

El técnico o técnicos encargados de la instalación deben estar en posesión de los certificados oficiales de la marca.

9. Presupuesto

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	20/22

+E1gpoIWXl33gmqoDXP1XA==

El presupuesto máximo de licitación del servicio, sin incluir el I.V.A., se establece en la cantidad de 59.000€, que suponen 71.390€ I.V.A. incluido. El presupuesto establecido es adecuado a los precios actuales de mercado.

10. Valoración de las ofertas

De conformidad con lo dispuesto en el Texto Refundido de la Ley de Contratos del Sector Público, cada licitador solo podrá presentar una proposición y no se admitirán variantes sobre la misma. Para la adjudicación del contrato se establecen como criterios de valoración de las ofertas los detallados a continuación:

Propuesta económica: hasta un máximo de 55 puntos.

La puntuación a asignar a cada oferente tendrá un valor máximo de 55 puntos sobre 100 y se calculará mediante la aplicación de la fórmula siguiente:

$$Vi = \frac{Pm}{Pi} \times 55$$

Siendo:
Vi = Valoración de la oferta en cuestión.
Pm = Oferta más baja presentada.
Pi = Oferta presentada por el licitador que se valora.

Solución técnica y prestaciones superiores a las exigidas: hasta un máximo de 45 puntos.

En este apartado se valorará la solución técnica presentada, la adecuación de la misma a los objetivos y fines del contrato, así como la calidad de la solución.

Serán objeto de valoración los siguientes apartados:

	Máxima puntuación
Solución de firewall a nivel de aplicación (NGFW), reconocimiento de aplicaciones e integración con LDAP:	8 puntos
Arquitectura de la solución, capacidad y rendimiento de la máquina que preste el servicio:	8 puntos

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	21/22

+E1gpoIWXl33gmqoDXP1XA==

Solución IDS/IPS	4 puntos
Solución de filtrado http y https	5 puntos
Prevención de amenazas/antimalware	4 puntos
Antivirus perimetral	4 puntos
Herramienta de Gestión, monitorización y generación de informes	5 puntos
Mejoras en los servicios de garantía, mantenimiento, formación, etc	4 puntos
Funcionalidades adicionales a las solicitadas en el PPT	3 puntos

La Analista Jefa de Proyectos,
(Firma electrónica)
Fdo: Carmen Oria Ratia.

Conforme:
EL JEFE DEL DPTO. DE LOS
SERVICIOS INFORMÁTICOS,
(Firma electrónica)
Fdo.: Eduardo Agüera Buendía

Código Seguro de verificación:+E1gpoIWXl33gmqoDXP1XA==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://adela.ayuncordoba.es/verifirmav2/
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	Eduardo Aguera Buendia - Jefe Departamento Servicios Informáticos		FECHA	03/12/2014
	Carmen Oria Ratia			
ID. FIRMA	adela155.ayuncordoba.org	+E1gpoIWXl33gmqoDXP1XA==	PÁGINA	22/22

+E1gpoIWXl33gmqoDXP1XA==