Suministro para el equipamiento destinado a la seguridad perimetral y el acceso a internet seguro en varios segmentos de red

Memoria Técnica

Ariadnex Tecnología Flexible. S.L.

Revisión 23/08/21

Versión 1.0

DIPUTACIÓN DE CÁCERES

Proyecto: *SUMINISTRO PARA EL EQUIPAMIENTO DESTINADO A LA SEGURIDAD PERIMETRAL, EL ACCESO A INTERNET SEGURO EN VARIOS SEGMENTOS DE RED A UN CONJUNTO DE ENTIDADES LOCALES DE LA PROVINCIA DE CÁCERES Y LA PRESTACIÓN DEL SERVICIO DE ATENCIÓN A LAS ENTIDADES RECEPTORAS DE LOS SUMINISTROS, ASÍ COMO EL SERVICIO DE MANTENIMIENTO DE LAS LICENCIAS NECESARIAS PARA SU CORRECTO FUNCIONAMIENTO* ***Documento***: *Memoria técnica* ***Cliente:*** Diputación de Cáceres

ARIADNEX TECNOLOGÍA FLEXIBLE

Empresa Certificada IEC/ISO 20000 e ISO 27001
www. ariadnex .com

00817884G JUAN MIGUEL TREJO (R: B06383814)

Firmado digitalmente por 00817884G JUAN MIGUEL TREJO (R: B06383814)
Fecha: 2021.08.23 08:56:42 +02'00'

Hoja de Control

Título:	*SUMINISTRO PARA EL EQUIPAMIENTO DESTINADO A LA SEGURIDAD PERIMETRAL Y EL ACCESO A INTERNET SEGURO EN VARIOS SEGMENTOS DE RED*		
Documento:	Propuesta técnica		
Nombre del Fichero:	MemoriaTecnica_F.odt		
Autor:	David Romero		
Versión:	1.0	Fecha:	23/08/21

Registro de cambios

Versión	Fecha	Autor	Modificación
0.1	23/08/21	David Romero	Creación del documento
0.2	23/08/21	Jose Ángel Pastor	Soporte técnico
1.0	23/08/21	Juan Miguel Trejo	Propuesta, Revisión y entrega

Índice

1 Descripción General Ejecutiva

Ariadnex Tecnología Flexible S.L., empresa con 20 años de experiencia en el sector y altamente especializada en seguridad de la información desde sus orígenes, se presenta a este proyecto de "**Suministro de equipamiento de seguridad y acceso a Internet de Diputación de Cáceres"** asumiendo la oportunidad que se le presenta en caso de resultar adjudicatarios de desplegar todas sus capacidades en su estadio natural, un entorno altamente exigente en cuanto a seguridad se refiere y un cliente como **Diputación de Cáceres** que representa una referencia muy importante para nosotros, como empresa extremeña formada por extremeños.

La propuesta se compone de un suministro de los equipos de referencia en el pliego de prescripciones técnicas, de la implantación y configuración del hardware propuesto y de unos servicios de muy alto valor añadido para la gestión y el control de la seguridad de la información del cliente y de la infraestructura de comunicaciones, que solo se pueden ofrecer desde el convencimiento de que representamos un *proveedor equilibrado, cercano y comprometido*, que estará permanentemente a disposición de los técnicos y responsables de seguridad de la información y las comunicaciones de **Diputación de Cáceres** de una forma ágil y cercana, lejos de la compleja estructura y formalismos de las grandes corporaciones que detraen agilidad y eficiencia en entornos especialmente críticos como lo es el compromiso con la seguridad de la información de Diputación de Cáceres.

Para ello, **Ariadnex S.L**. cuenta con certificaciones dentro del ámbito de su competencia, así como un equipo de profesionales altamente cualificados, formados y certificados en los sistemas que provee, certificaciones éstas que solo reflejan la excelencia de nuestro trabajo, avalado cada día por nuestros clientes que se relacionan con los equipos de personas que efectivamente tienen asignados de una forma directa, lo que implica que directamente la atención sobre los servicios posteriores se realiza por los ingenieros involucrados directamente en la integración de la plataforma.

En definitiva, en los años de evolución de nuestra trayectoria profesional hemos podido conseguir un grado de especialización y motivación en nuestros trabajos que nada tienen que desmerecer de otras organizaciones mucho más voluminosas pero que acarrean una carga administrativa y de gestión que desvirtúan en muchos casos la calidad de servicio, la orientación al cliente y la agilidad y eficiencia de la entrega de servicios y productos.
La presente propuesta tiene como base fundamental el fabricante Fortinet para la implementación de toda la plataforma de seguridad, control y gestión de la seguridad y los accesos, junto con el fabricante Alienvault (ATT) sobre el que basamos nuestra herramienta *Ariolo SIEM Premium* ® que permite la monitorización y correlación de eventos de toda la plataforma.
Todo ello complementado con nuestros servicios continuados a la seguridad SOC, en nuestro centro de control de Mérida, junto a la centralización de la gestión de dispositivos y sistemas de alerta permanente en nuestro Centro De Datos propio en Extremadura.
Con un firme compromiso con el éxito del proyecto y una dedicación y esfuerzo porque Cáceres sea un referente en implementación y gestión de la conectividad de las zonas que lo necesitan tanto o más que el resto de nuestro país. Ademá reafirmando la posibilidad de desplegar ubicaciones de trabajo remoto en cualquier Entidad del proyecto siempre con el punto de vista de la seguridad como objetivo.

2 Descripción General Técnica

Nuestra propuesta para el proyecto se basa en un modelo estratificado de seguridad por capas siguiendo los mayores estándares internacionales del sector.
En el siguiente esquema planteamos nuestra propuesta:

Ariadnex S.L. propone una solución de infraestructura y servicio con tres niveles de seguridad que se describen a continuación:

- El primer nivel (etiquetas 1 y 2 dibujo) ofrecerá seguridad a nivel físico, donde se establecerán criterios que permitirán controlar y aportarán visibilidad sobre los equipos conectados en las sedes de las entidades locales, así mismo, gracias a la tecnología NAC incluida en los dispositivos de red se podrá ubicar de manera automática cada dispositivo en su segmento de red correspondiente.

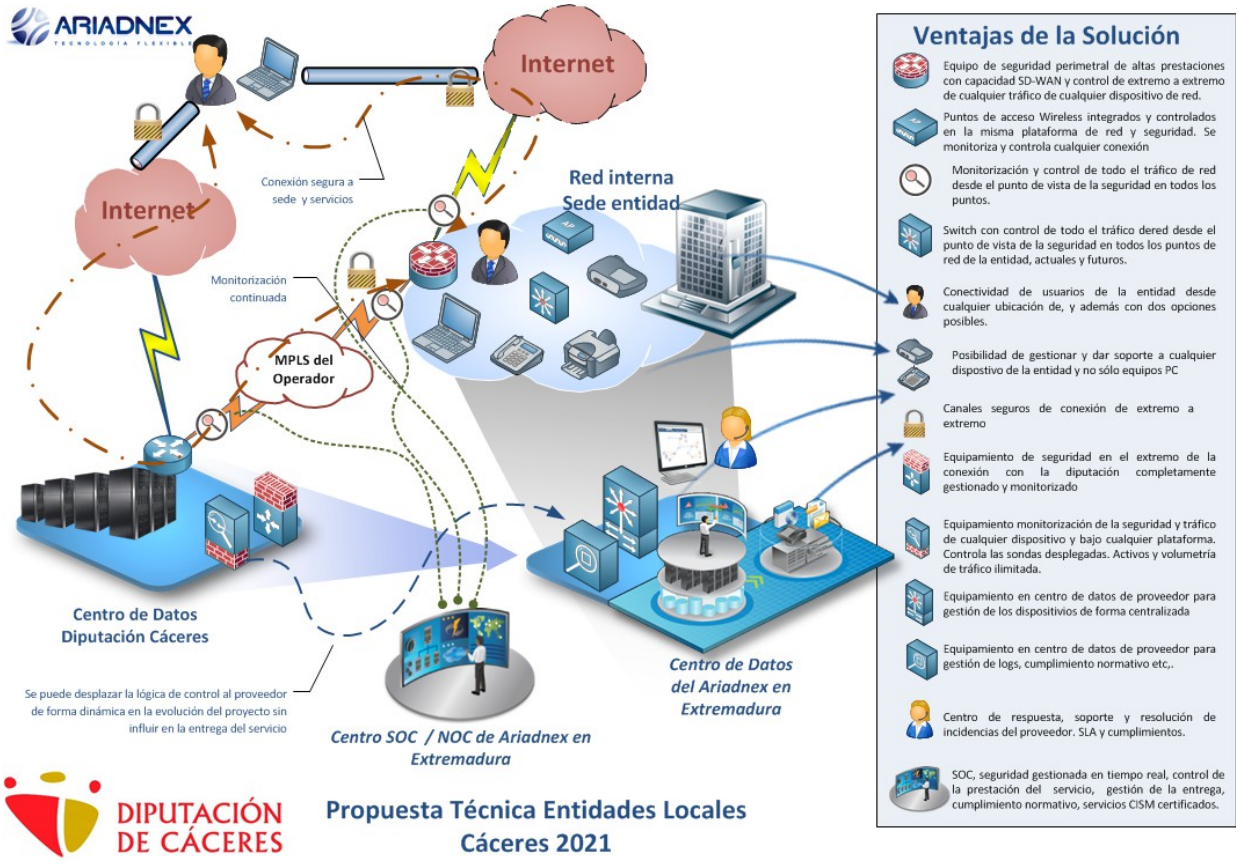
- El segundo (etiqueta 3 dibujo) nivel ofrecerá seguridad perimetral a las conexiones de las entidades locales, permitiendo gestionar el tráfico de forma granular. Incluyendo la posibilidad de crear perfiles de seguridad en base a las necesidades de cada departamento, además ofrece la posibilidad de realizar SD-WAN para añadir accesos a internet independientes a la red segura de Diputación de Cáceres.

- El tercer nivel (etiqueta 4 dibujo) ofrecerá seguridad centralizada de las conexiones de las entidades locales permitiendo tanto gestionar los dispositivos ubicados en los

ayuntamientos y entidades así como establecer unas políticas de acceso a internet genéricas.

De forma transversal a estos tres niveles se proveerá una herramienta de monitorización y gestión de eventos de seguridad que aportará visibilidad sobre las conexiones que supongan un riesgo potencial, o no, de todos los dispositivos pertenecientes a Diputación Provincial de Cáceres. Además se proveerá una herramienta de gestión y almacenamiento de logs.

El anterior esquema estratégico y metodológico se traslada al detalle técnico y de infraestructura mediante el siguiente diagrama técnico:

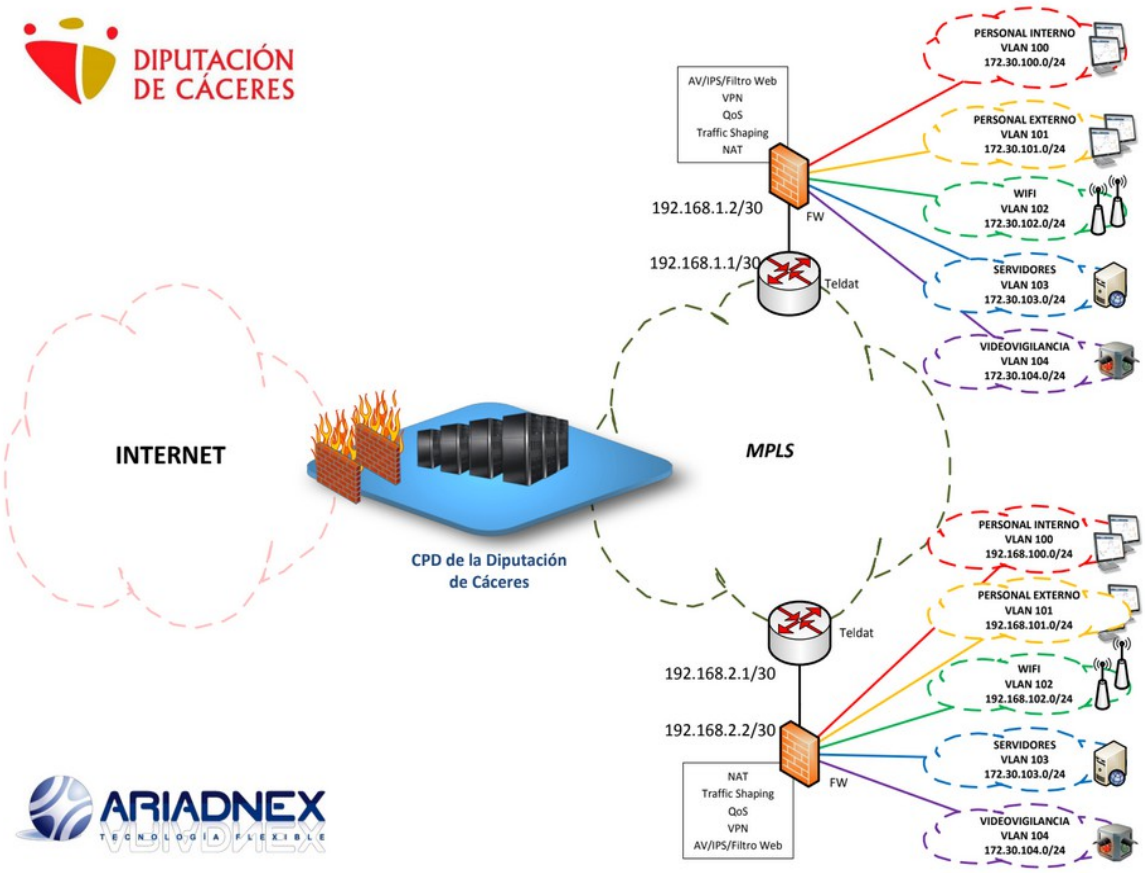


En cada una de las sedes de las entidades locales pertenecientes a Diputación Provincial de Cáceres se instalarán puntos de acceso y switches cuyo objetivo principal será proveer de acceso a la redes de servicio actuales. Estos dispositivos irán conectados a su vez, a un equipo de seguridad perimetral que será el encargado de gestionar el tráfico tanto de entrada como de salida de forma completamente transparente al usuario y que será el elemento encargado de controlar, gestionar, encapsular, cifrar, monitorizar, y en definitiva dotar de seguridad todas las comunicaciones de la entidad, tanto los que se realicen a través de la red segura de Diputación como a internet de forma directa.

Cada una de las sedes de las entidades locales estará conectada con el centro de datos de Diputación Provincial de Cáceres mediante la red corporativa, ésta es una conexión encapsulada bajo parámetros de la tecnología de capa 2 de operador MPLS que además permite la conexión con otras sedes.. Adicionalmente a ésta conexión, se establecerá un túnel IPSec extremo a extremo con el CPD de Diputación de Cáceres y el CPD de Ariadnex / Ariolo.

Una de las principales ventajas que ofrece la solución propuesta es, además de la securización de la conexión hacia internet, hacerlo también con la conexión MPLS intersede y hacia y desde Diputación de Cáceres. Otra ventaja de la implementación de productos de Fortinet es **Security Fabric** que aporta una solución que permite la integración de los productos de Fortinet ofertados y servicios inteligentes que conforman un tejido de seguridad contra intrusos, virus y ataques, aportando mayor visibilidad para cada segmento de red y dispositivo así como una detección de amenazas ágil y eficiente.

Para dar más detalle de cómo nos parece que podríamos llevar a cabo la implantación, justo al día siguiente de la propuesta de comienzo, una planificación de direccionamiento y uso "lógico" de una sede tipo sería la siguiente:



Este modelo de ejemplo que se deberá consensuar con los servicios de comunicaciones de Diputación de Cáceres, como se puede observar tiene en cuenta, desde una perspectiva de

la conectividad, la funcionalidad, la gestión y la seguridad, los potenciales y posibles usuarios de la plataforma así cómo su direccionamiento propio.
Esto supone disponer en todo momento, y desde el punto de vista de la trazabilidad, de una visión exacta de "Quién, Como, y Donde", es decir Quién está usando la red, Cómo lo está haciendo y Desde Donde la está utilizando para poder tener un control exhaustivo de la misma.

3 Dotación de los Ayuntamientos y Entidades Locales

Para satisfacer las necesidades de seguridad de la información de las entidades locales, se propone, como se ha comentado, a nivel de entidad, de una infraestructura de seguridad completa y escalable estructurada en dos niveles.

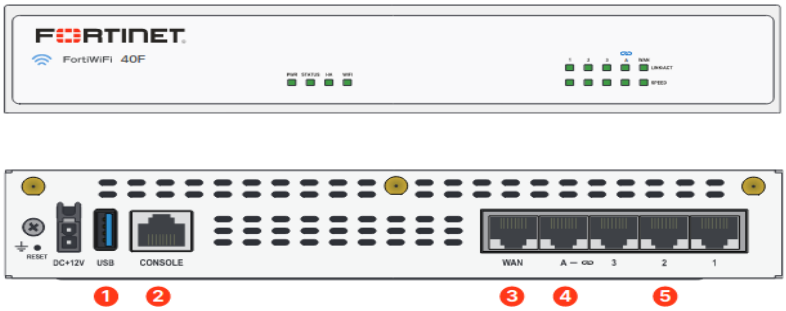
El primer nivel ofrecerá un control de acceso a la red, aportando una mayor visibilidad de dispositivos conectados tanto por red inalámbrica como red cableada.

El segundo nivel ofrecerá las capacidades de firewalling, entre las que destacan, el control de acceso lógico de los dispositivos, el filtrado de las conexiones, estableciendo perfiles de seguridad en base a las necesidades específicas de cada entidad local.

La principal ventaja de desplegar una infraestructura basada en dispositivos Fortinet recae en la impecable integrabilidad de los diferentes dispositivos así como la sencillez a la hora de afrontar necesidades de escalado, tanto horizontal para aumentar de forma sencilla el número de dispositivos ya existentes en la plataforma, como vertical para añadir nuevos productos.

3.1 Cortafuegos de nueva generación

La plataforma NGFW de las entidades locales estará formada por equipos de seguridad perimetral Fortinet FortiGate 40F:



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 1x GE RJ45 WAN Port
4. 1x GE RJ45 FortiLink Port
5. 3x GE RJ45 Ethernet Ports

Hardware Features

FortiGate, líder del mercado, proporciona una solución integrada de seguridad compuesta por las funcionalidades más eficaces que proporcionan una protección completa de las comunicaciones, como son: Firewall, VPN (IPSEC y SSL), Antimalware, Anti-Botnet, Anti-DoS, Sistemas de Detección/Prevención de Intrusiones, Filtrado Web, Antispam, Control de Aplicaciones, Inspección de Contenido en SSL, firewall de aplicaciones WEB e inspección del acceso a aplicaciones cloud (CASI). Además, todas las funcionalidades de seguridad se integran de forma conjunta con funcionalidades añadidas como Traffic Shaping, Alta Disponibilidad, balanceo de carga, aceleración y balanceo WAN, Soporte a VoIP, Controlador Wireless, Enrutamiento dinámico RIP, OSPF y BGP, etc.

La tecnología Fortinet es una poderosa combinación de software y hardware basada en el uso de “Circuitos Integrados de Aplicación Específica”, conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones.

La tecnología incluye los Procesadores FortiASIC™ y el Sistema Operativo FortiOS™ los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos.

Los procesadores FortiASIC™, diseñados por Fortinet, poseen un motor propietario de análisis de contenido que acelera los intensivos procesos de análisis requeridos por la seguridad a nivel de aplicación (Antimalware, filtrado de contenidos y procesos relacionados), estos procesos tendrían un rendimiento mucho más bajo y una mayor latencia si fueran llevados a cabo por procesadores de propósito general.

La familia de equipos físicos **FortiGate 40F**, incluye la cuarta generación del Sistema en un chip de Fortinet, SoC4 que soporta la transformación del borde de la WAN del cliente con las clasificaciones de cómputo de seguridad más altas de la industria. El SoC4 consolida las funciones de procesamiento tanto de redes como de contenido en un solo chip, lo cual proporciona una identificación rápida de las aplicaciones, dirección y rendimiento de superposición.

El SoC4 es un conjunto de funciones de seguridad completamente integrado, incluido un firewall de Capa 7, en un chip rápido y rentable. Cumple con los requisitos de alto rendimiento para una experiencia óptima del usuario final y protege las sucursales implementadas en entornos SD-WAN.

3.1.1 Firewall

Los equipos FortiGate poseen la funcionalidad de firewall basada en tecnología Stateful Inspection Packet. Esto le permite hacer un análisis exhaustivo de la cabecera de cada paquete, identificando la sesión a la que pertenece, chequeando el correcto orden de los paquetes y realizando control sobre el tráfico de la red.

3.1.2 Inspección en modo Proxy o Flow

El modo de inspección controla la forma que tiene FortiGate de aplicar y controlar los perfiles de seguridad. Una vez configurado el modo de inspección, aplica de forma global a todos los perfiles de seguridad, por lo que no es posible configurar una política con un perfil de seguridad en modo proxy y otra regla con otro perfil en modo flow.

3.1.3 Routing

Los equipos FortiGate pueden trabajar con enrutamiento dinámico, soportando RIP (v1 y v2), OSPF (IPv4 ó IPv6) y BGP v4 (mediante BGP4+ soportado IPv6), así como con enrutamiento multicast (PIM sparse/dense mode), además de trabajar con enrutamiento estático (IPv4 ó IPv6) y ofrecer la posibilidad de realizar *policy routing* y balanceo de líneas WAN, permitiendo incluso la utilización de distinta línea en función del tráfico de las distintas aplicaciones.

3.1.4 Detección y Prevención de Intrusos

El Sistema de Detección y Protección de Intrusión de FortiGate constituye un sensor de red en tiempo real que utiliza definiciones de firmas de ataques y detección de comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red.

El motor IDS provee seguridad hasta la capa de aplicación, sin mermar por ello el rendimiento de la red. La capacidad de IDS de los equipos FortiGate se basa en el módulo de routing, el módulo de firewall y la capa de aplicación. De esta forma el sistema de detección de intrusiones no se limita únicamente a la detección de ataques de nivel de red ni tampoco al análisis individual de cada paquete. FortiGate reensambla el contenido de los paquetes en línea y los procesa para identificar ataques hasta el nivel de aplicación.

3.1.5 Inspección de tráfico cifrado SSL

Mediante la aplicación de perfiles de inspección SSL/SSH, FortiGate será capaz de llevar a cabo acciones (escaneos, filtros, etc) sobre el tráfico cifrado.

3.1.6 Control de aplicaciones

Con la función de control de aplicaciones, FortiGate permite detectar y tomar medidas contra el tráfico de red en función de la aplicación.

El control de aplicaciones utiliza los decodificadores IPS que pueden analizar el tráfico de red para detectar el tráfico de aplicaciones, incluso si el tráfico utiliza los puertos o protocolos no estándar.

FortiGate puede reconocer el tráfico de red generado por un gran número de aplicaciones.

3.1.7 Filtrado Web

La distribución y visualización de contenido no autorizado supone un riesgo importante para cualquier organización. Para las empresas, la monitorización del uso que sus empleados hacen de los accesos a Internet y la prevención de visualización de contenidos web inapropiados, o no autorizados, se ha convertido en algo necesario, justificado por los costes financieros y las implicaciones legales que conlleva la pasividad en este aspecto.

El servicio FortiGate web filtering puede ser configurado para escanear toda la cadena del contenido del protocolo http permitiéndonos filtrar direcciones URL potencialmente no

asociadas al desarrollo de la normal actividad laboral, contenidos embebidos en las propias páginas web o scripts basados en java, activeX o cookies, contenidos potencialmente peligrosos.

La funcionalidad de filtrado web puede definirse mediante listas creadas por el propio usuario, o bien mediante la utilización del servicio FortiGuard Web Filtering.

3.1.8 Filtro de antivirus y antispam

FortiGate incorpora un sistema antimalware de alto rendimiento gracias a su optimizada arquitectura y configuración. Los componentes principales del sistema antimalware de FortiGate son:

- La arquitectura hardware basada en FortiASIC.
- Su optimizado sistema operativo FortiOS.
- La infraestructura, los laboratorios y centros de desarrollo distribuidos a lo largo de todo el mundo mediante la red FortiGuard.

La funcionalidad AntiSpam de los equipos FortiGate permite gestionar los correos no solicitados detectando los mensajes de spam e identificando esas transmisiones. Los filtros antispam se configuran de un modo global, si bien son aplicados en base a perfiles de protección, al igual que el resto de funcionalidades del equipo.

3.1.9 Integración con Active Directory y LDAP

La plataforma de FortiGate soporta la autenticación de usuarios empleando diferentes mecanismos, como son, usuarios locales mediante la creación de una base de datos local, o contra servidores externos, que pueden RADIUS, TACACS +, LDAP o Active Directory.

3.1.10 Controlador Wifi

Todos los dispositivos FortiGate, son capaces de actuar como controladores Wireless para los puntos de acceso fabricados por Fortinet (FortiAPs). Esto supone un ahorro de costes considerable para los clientes al no tener que adquirir un controlador Wireless.

La solución de Fortinet se integra de forma directa con el Firewall, siendo cada SSID wifi una nueva interfaz del Firewall. Esto permite aplicar las mismas políticas de seguridad en la red Wifi que en la red cableada, pudiendo configurar en la wifi reglas de Firewall, Traffic-Shapping, Control de Aplicaciones, filtrado web, etc. de forma sencilla y transparente.

Dispone además de opciones de portal cautivo para invitados, pudiendo delegar la gestión de dichos invitados. Para ello dispone de un portal de administración restringido que permite dar acreditaciones a la red wifi de manera sencilla, pudiendo suministrar la información de usuario y contraseña de varios métodos, incluyendo SMS, email o impreso.

Con Fortinet es además posible reconocer el tipo de dispositivo que conecta a la red wifi, pudiendo crear reglas de seguridad basadas en tipo de dispositivo.

A nivel de conectividad, la solución de Fortinet cuenta con las funcionalidades de conectividad más requeridas para los entornos Enterprise, funcionalidades tales como

meshing, local bridging, asignación dinámica de canales, asignación dinámica de potencia, balanceo de clientes entre puntos de acceso, fast roaming, etc.

3.1.11 Soporte de Fabric Connectors

La nueva plataforma FortiOS 6.2 de Fortinet soporta nuevos conectores que permiten la integración con entornos Cloud y de Threat Intelligence así como también se integra con conectores externos para bloquear tráfico malicioso. Los nuevos conectores permiten:

- Soporte de múltiples conexiones al mismo tipo de Cloud (por ejemplo conexión a dos entornos distintos en Azure o AWS).
- Soporte de conectores Cloud: Alibaba AliCloud, VMware ESXi y VCENTER, Azure Stack, Openstack y Kubernetes sobre entornos cloud de AWS, Azure, Oracle, Google GPC o Cloud Privado.
- Conectores de Threat Intelligence para alimentar a FortiGate con feeds de HASHES maliciosos y soporte de autenticación en las conexiones a feeds externos.
- Capacidad de bloquear tráfico a nivel IP, DNS (DNS Filter) o URL (Web Filter) mediante categorías dinámicas generadas a partir de feeds externos.

3.1.12 WAN Definida por Software (SD-WAN)

La red WAN definida por software (SD-WAN) es un enfoque ágil basado en software para redes de área extensa (WAN). Sustituye al hardware de red WAN tradicional por software SDN para ofrecer de manera más eficaz aplicaciones a usuarios en largas distancias. El objetivo de la red SD-WAN es reducir los costos de los enlaces WAN privados, aumentar el rendimiento y hacer que la red sea más ágil.

Algunas de las funcionalidades diferenciadoras de Fortinet son las siguientes:

- Agregación de túneles IPSec y Per Packet Load Balancing.
- Funcionalidad FEC (Forwared Error Correction).
- Monitorización de SLAs y Dashboards históricos.
- Funcionalidad Overlay Controller.

A continuación se puede ver la agregación de túneles VPN IPsec que se representa en los cortafuegos FortiGate como una sola interfaz.

3.1.13 VPN

Los equipos FortiGate soportan el establecimiento de Redes Privadas Virtuales basadas en protocolos IPSec y SSL. La funcionalidad VPN está integrada en la propia plataforma Forti-Gate sin necesidad de licencia, así como también se puede utilizar mediante la instalación de la suite de aplicaciones Forticlient Endpoint Security, que permite el establecimiento de VPNs desde un equipo cliente.

3.1.14 Características Técnicas Fortigate 40F

Las características técnicas de Fortinet FortiGate 40F están en el **Anexo I.**

3.2 Infraestructura inalámbrica. FortiAP

3.2.1 Descripción de la solución

La solución diseñada para la red inalámbrica de la entidades locales consiste en la instalación y configuración de nuevos puntos de acceso para proveer de cobertura inalámbrica a los Ayuntamientos.

La solución inalámbrica de Fortinet se integra de forma directa con el cortafuegos, siendo cada red WiFi una nueva interfaz del cortafuegos. Esto permite aplicar las mismas políticas de seguridad en la red Wifi que en la red cableada, pudiendo configurar en la WiFi reglas de Firewall, Traffic-Shaping, Control de Aplicaciones, filtro web, etc de forma sencilla y transparente.

Dispone además de opciones de portal cautivo para invitados, pudiendo delegar la gestión de dichos invitados. Para ello dispone de un portal de administración restringido que permite dar acreditaciones a la red wifi de manera sencilla, pudiendo suministrar la información de usuario y contraseña de varios métodos, incluyendo SMS, email o impreso.

Con Fortinet además es posible reconocer el tipo de dispositivo que se conecta a la red inalámbrica, pudiendo crear reglas de seguridad basadas en el tipo de dispositivo.

A nivel de conectividad, la solución de Fortinet cuenta con las funcionalidades de conectividad más requeridas para los entornos empresariales, funcionalidades tales como meshing, local bridging, asignación dinámica de canales, asignación dinámica de potencia, balanceo de clientes entre puntos de acceso, fast roaming, etc.

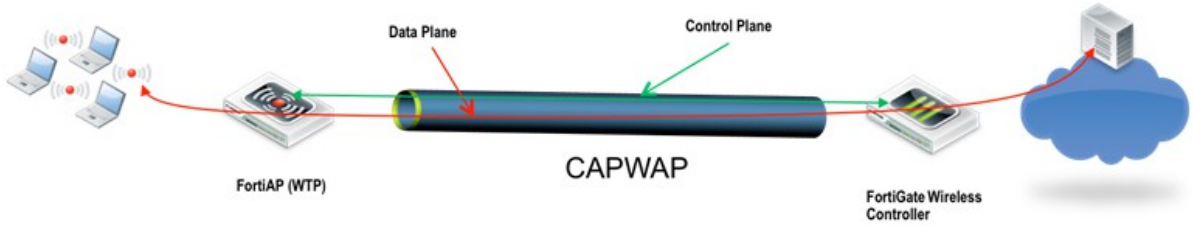
3.2.2 Arquitectura de red

Los equipos FortiGate incorporan un controlador wireless capaz de controlar puntos de acceso de Fortinet. El punto de acceso, FortiAP, puede ser emplazado en cualquier lugar de la red siempre y cuando haya comunicación en capa 3 con el Firewall.

Los puntos de acceso de Fortinet se pueden configurar según las siguientes dos arquitecturas:

- Con APs ligeros, de gestión centralizada, tunelizando el tráfico hasta el controlador.
- Con APs ligeros, de gestión centralizada, conmutando el tráfico directamente a la red cableada (Local Bridging).

En este proyecto se considera el primer caso, es decir, tunelizar el tráfico hasta el controlador, con lo que nos aseguramos que cualquier paquete de la red WiFi pase a través del cortafuegos, pudiendo así aplicar sobre dicho tráfico todas las funcionalidades de FortiGate: Control de Aplicaciones, IPS, filtro web, Antivirus, Firewalling, etc. El diagrama inferior muestra la arquitectura basada thin APs con tráfico tunelizado.



CAPWAP es el protocolo empleado para establecer el túnel entre el AP y el Controlador. En caso de requerirlo por motivos de seguridad y privacidad, este tráfico puede ir cifrado. La aplicación de CAPWAP en las redes WiFi de Fortinet cumple con el estándar RFC-5415.

3.2.3 Seguridad

La solución se enfoca desde el punto de vista de la seguridad.

La WiFi de Fortinet permite dotar a la red inalámbrica de las mismas medidas de seguridad que aplicamos al tráfico cableado. Cada SSID que creamos en modo túnel es una nueva interfaz del cortafuegos a todos los niveles, como una interfaz cableada. Es decir, podemos definir routing, políticas de filtrado, control de aplicaciones, filtro web, IPS, antivirus, DLP, etc. de igual forma que haríamos con una interfaz cableada. Fortinet aplica estas reglas y perfiles de capa 7 mediante políticas, las cuales pueden estar basadas en identidad, es decir, en base al usuario.

3.2.4 Gestión centralizada de la red Wi-Fi

Para la gestión centralizada de la nueva infraestructura inalámbrica compuesta por puntos de accesos FortiAP de Fortinet se propone utilizar la controladora inalámbrica FortiGate 40F que tiene cada entidad local e integrar en esta los nuevos puntos de accesos para poder gestionar, mantener y monitorizar toda la red Wifi desde una misma y única gestión web.

3.2.5 Equipamiento y características técnicas

En este apartado se presentan y describen las características técnicas de los puntos de accesos ofertados en la presente propuesta.

3.2.5.1 Punto de acceso FortiAP

Los puntos de acceso a instalar serán productos del fabricante Fortinet denominados FortiAP.

El FortiAP es un punto de acceso inalámbrico que trabaja en los estándares 802.11a/b/g/n/ac wave 2 que ofrece alto rendimiento inalámbrico seguro en combinación con el FortiGate® embedded wireless controller. El FortiAP tiene a su vez comportamiento dual para trabajar en dos radios concurrentes, ideal para los despliegues en el interior.

Con respecto a las posibilidades de configuración, un radio puede configurarse automáticamente en la frecuencia de 2,4 GHz mientras que el segundo radio puede ofrece un acceso ininterrumpido en la frecuencia de 5 GHz para clientes WiFi con alto rendimiento.

El equipo FortiAP tiene capacidad de soportar hasta 16 SSIDs por radio (14 para acceso de clientes y dos para monitorización). Al ser un dispositivo de la familia Fortinet, se integra con el equipo FortiGate donde quedarán registradas las características del tráfico.

Además, su diseño al estilo detector de humo es ideal para instalar en pasillos donde la discreción es deseable para evitar robos.

Entre las característica principales del producto, encontramos:

- La existencia de dos radios proporcionando conexiones 802.11a/b/g/n/ac simultáneas con elevado throughput.
- La existencia de un tercer radio para monitorización de seguridad de la red inalámbrica.
- Las cuatro antenas internas no impactan sobre la decoración del edificio.
- Secuencia espacial dual 2x2 MU-MIMO
- Dos puertos Ethernet con soporte para 802.3af/802.3at PoE.
- 802.11 avanzado para mejorar la velocidad por encima del estándar.
- Detección de puntos de acceso aledaños, monitorización y control al mismo tiempo que el acceso de los clientes.
- WPA, WPA2 y WPA3 con 802.1X o PSK, WEP, portal cautivo, listas blancas y negras de direcciones MAC.
- Cifrado: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
- SSID privado para Hotspot.
- Priorización de tráfico de capa 7 para proporcionar características de rendimiento de nivel empresarial.
- Roaming rápido que evita pérdida de conectividad Wifi y VoIP sobre VLAN.
- Gestión centralizada y posibilidad de generación de informes mediante la integración con la controladora FortiGate.
- Gestión de perfiles globales.
- Aprovisionamiento de recursos por radio distribuidos automáticamente (DARRP).
- Soporte de Kensington lock para evitar robos de los puntos de accesos.

3.2.5.2 Gestión de la Autenticación

La gestión de la autenticación de los clientes/dispositivos se puede realizar desde la base de datos interna de la controladora inalámbrica FortiGate o desde un sistema externo de gestión de identidades como Active Directory de Microsoft. Además, la gestión de la autenticación se puede integrar con el servicio Radius de AAA (Authentication, Authorization, y Accounting) soportando el estándar 802.1X para controlar el acceso a la red por puerto.

Las solución Wifi de Fortinet permite emplear mecanismos de autenticación seguros. Así pues, por cada SSID configurado podemos definir qué tipo de autenticación se quiere emplear:

Para la autenticación de los usuarios se puede utilizar los protocolos RADIUS, LDAP y TACACS+ contra cualquier servidor que soporte estos estándares, como por ejemplo Microsoft IAS RADIUS Server, Cisco ACS Server, FreeRADIUS, Interlink RADIUS Server, Steel Belted Radius, así como también Microsoft Active Directory. Además, es de destacar que los usuarios también pueden ser almacenados y autenticados en una base de datos interna de la propia controladora inalámbrica.

Portal Cautivo

Es también posible crear un SSID con autenticación basada en Portal Cautivo, de forma que el usuario se autentique a través de un portal web en la red Wireless. El portal cautivo puede ser modificado para adaptarse a los requisitos del cliente. La captura inferior muestra la personalización de uno de los portales cautivos.

Los usuarios se autenticarán en el portal cautivo bien con sus contraseñas de dominio o bien con contraseñas de uso temporal creadas para la ocasión (por ejemplo usuarios invitados). Para facilitar la creación de usuarios temporales la solución de FortiGate incorpora una herramienta de Gestión de Invitados.

Independientemente del mecanismo de autenticación empleado, la controladora presenta varias vistas que permiten monitorizar y controlar los usuarios autenticados en la red Wifi.

La solución inalámbrica de Fortinet dispone de mecanismos para que cada punto de acceso monitorice el espectro y radie en el canal que menos interferencias presenta. La funcionalidad de Automatic Radio Resource Provision (ARRP) permite seleccionar los canales sobre los que queremos trabajar y dejar al equipo elegir el canal óptimo. Otra funcionalidad interesante es el ajuste de potencia automático. En despliegues con mucha densidad de puntos de accesos es importante que estos ajusten la potencia de forma automática para evitar solapes cuando todos los puntos de accesos están presentes y para cubrir zonas que pudieran quedar sin cobertura en el caso de fallo de un punto de acceso.

3.2.6 Especificaciones Técnicas

Las especificaciones técnicas están en el **Anexo I.**

3.3 Infraestructura de equipos de switch FortiSwitch

3.3.1 Descripción de la solución

La solución diseñada para la red de la entidades locales consiste en la instalación y configuración de nuevos switches para ofrecer conectividad a los equipos de los ayuntamientos.

Fortinet ofrece un enfoque centrado en la seguridad, rendimiento y capacidad de gestión para las redes Ethernet mediante su dispositivo FortiSwitch. Estrechamente integrado en Fortinet Security Fabric a través de FortiLink, FortiSwitch se puede administrar directamente desde la interfaz de los diferentes FortiGate instalados en las diversas entidades locales, lo que permite configurar y proteger los puertos Ethernet con solo un par de clics. Este único panel de gestión proporciona una visibilidad y un control completos de los usuarios y dispositivos en la red independientemente de cómo se conecten. Esto hace que FortiSwitch sea ideal para implementaciones de SD-Branch, lo que permite a las empresas converger su seguridad y acceso a la red.

FortiLink es una tecnología clave de apoyo de FortiSwitch, que permite que sus puertos se conviertan en extensiones del appliances de seguridad de FortiGate. Cuando se conecta a través de FortiLink, las políticas de seguridad de FortiSwitch pueden reflejar que FortiGate hace que las interfaces del Firewall y los puertos del Switch sean igualmente seguros. Con una capa de acceso integrada, FortiGate proporciona visibilidad consolidada e informes que facilitan la administración y la resolución de problemas.

Por último, destacar la posibilidad de configurar una política de control de acceso a la red (NAC) que haga coincidir los dispositivos con unos criterios especificos, con un grupo de usuarios concretos o con una etiqueta FortiClient EMS. Los dispositivos que coincidan con algunos de los criterios establecidos previamente, se podrán asignar a una VLAN específica o se les aplicará una configuración concreta en el puerto conectado.

3.3.2 Equipamiento y características técnicas

En este apartado se presentan y describen las características técnicas de los switches ofertados en la presente propuesta.

3.3.2.1 FortiSwitches

Los switches a instalar serán productos del fabricante Fortinet denominados FortiSwitch. Se suministrarán dos modelos: 108F (8 puertos) y 124F (24 puertos).

El FortiSwitch es un switch que ofrece seguridad, rendimiento y capacidad de gestión excepcionales. Seguro, simple y escalable, FortiSwitch es la elección correcta para empresas de todos los tamaños que tengan conciencia de amenazas

A continuación podemos ventajas y características de los FortiSwitch:

- Ideal para implementaciones SD-Branch

- Gestión centralizada de seguridad y acceso desde las interfaces de FortiGate mediante FortiLink.
- Óptimo para entornos de redes convergentes; permitiendo que el tráfico de voz, datos e inalámbrico se entregue a través de una sola red.
- Admite implementaciones que no son de FortiLink a través de una interfaz gráfica de usuario integrada, una API o mediante consola.
- Apilable hasta 300 switches por FortiGate, según el modelo.
- Admite cambio de velocidad y modo de reenvío y almacenamiento.

3.3.2.2 Especificaciones Técnicas

Las características técnicas de los FortiSwitch están en el **Anexo I.**

3.4 Armarios racks de comunicaciones

Se proveerán los siguientes armarios de rack:

- Armario de rack de 19” estándar de al menos 16 u’s 1 cuerpo 600x600 con puerta de cristal con llave.

- Armario de rack de 19” de mural de al menos 12 u’s 1 cuerpo 600x450 con puerta de cristal con llave.

4 Dotación de los centros de datos centralizados

Como plataforma de seguridad de la información para la Diputación Provincial de Cáceres se ofrece una solución global de seguridad que garantice la calidad, rendimiento y escalabilidad de la infraestructura subyacente. Dicha solución está conformada por elementos de firewalling, un sistema de administración centralizada de los diferentes dispositivos de seguridad perimetral establecidos en las sedes de las entidades locales, un sistemas de gestión y almacenamiento de logs y una plataforma de monitorización y gestión de eventos de seguridad en la red.

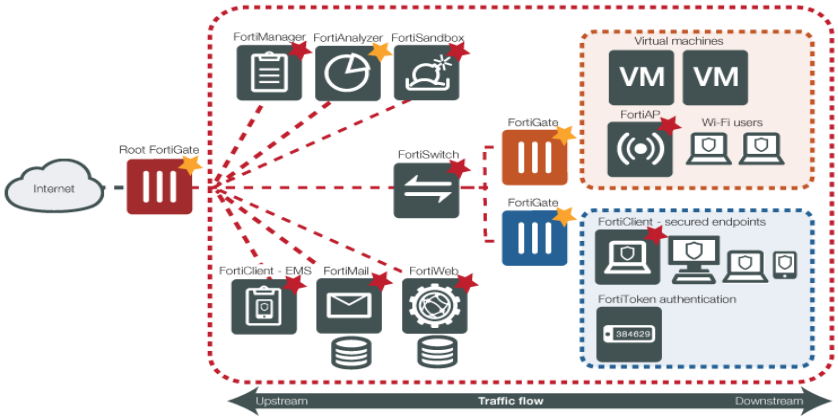
4.1 Cortafuegos de nueva generación Fortigate 201 F

La transformación digital desbloquea el potencial masivo, pero también introduce amenazas de ciberseguridad avanzada. Las arquitecturas de seguridad tradicionales están demostrando ser inútiles. Por este motivo, Fortinet ha desarrollado el concepto **Security Fabric**que proporciona una amplia protección y visibilidad para cada segmento de red, dispositivo y appliance. La solución ofertada sincroniza automáticamente los recursos de seguridad para hacer cumplir las políticas, coordinar respuestas automatizadas a amenazas detectadas en cualquier lugar de la red, además de proporcionar una administración fácil de toda la plataforma Fortinet.

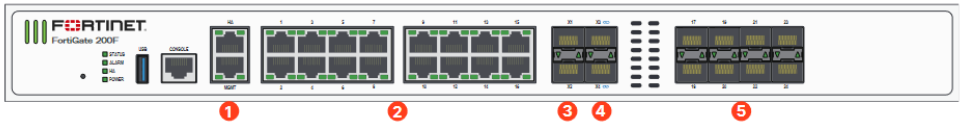
Los cortafuegos propuestos para el centro de datos son los equipos Fortinet FortiGate 201F que se integrarán en el Security Fabric de la red segura de Diputación de Cáceres, es decir, estos equipos proporcionarán una protección y visibilidad centralizada de todas las entidades. Los equipos FortiGate 201Fson capaces de realizar firewalling a 27 Gbps y además incorporan puertos de 10 GbE lo que los hace altamente potentes y escalables para añadir más entidades si fuese necesario.

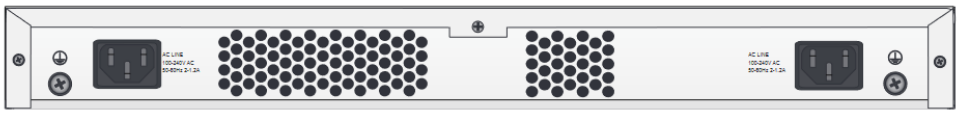
Por otro lado, los equipos FortiGate 201F incorporan un disco SSD de 480 GB que permite realizar optimización WAN para maximizar el rendimiento de la WAN, proporcionar una gestión inteligente del ancho de banda y un rendimiento de seguridad consolidado inigualable. La optimización WAN reduce la sobrecarga de la red y elimina el tráfico innecesario para una mejor experiencia de rendimiento general. El uso eficiente del ancho de banda y un mejor rendimiento de las aplicaciones eliminarán la necesidad de costosas actualizaciones de enlaces WAN en el centro de datos de Diputación de Cáceres y otras soluciones costosas para el crecimiento del tráfico de la red.

El **Fortinet Security Fabric** proporciona una amplia protección y visibilidad para cada segmento de red, dispositivo y appliance, ya sea virtual, en la nube o en el lugar. La solución ofertada sincroniza automáticamente los recursos de seguridad para hacer cumplir las políticas, coordinar respuestas automatizadas a amenazas detectadas en cualquier lugar de la red y administración fácil de la plataforma FortiGate, FortiAnalyzer, FortiSandbox y FortiWeb por medio de la tecnología Security Fabric.



La plataforma NGFW Centralizado del Centro de Datos de Diputación estará formada por equipos de seguridad perimetral Fortinet FortiGate 201F:





Interfaces

1. 2x GE RJ45 HA / MGMT Ports
2. 16x GE RJ45 Ports
3. 2× 10 GE SFP+ Slots
4. 2× 10 GE SFP+ FortiLink Slots
5. 8x GE SFP Slots

Hardware Features

No se va a proceder a describir las características técnicas de este producto puesto que son las mismas que las descritas en el punto 3.1 Cortafuegos de nueva generación.

4.1.1 Especificaciones técnicas

Las características técnicas de los equpos Fortigate 201F están en el **Anexo I.**

4.2 Plataforma de gestión centralizada

4.2.1 Descripción de la solución Fortimanager.

La solución diseñada para la administración global de los dispositivos suministrados consiste en la instalación y configuración de un sistema de gestión centralizada, en formato virtual, que permita la configuración, mantenimiento, actualización de todos los dispositivos de la red de forma ágil y centralizada. Se propone su ubicación en nuestro Centro de Datos.

FortiManager es una plataforma integrada para la administración centralizada de productos en una infraestructura de seguridad de Fortinet. FortiManager proporciona gestión centralizada de la implantación, configuración y actualización para dispositivos FortiGates, FortiSwitch y FortiAP.

Para reducir latencias en la red y el uso del acceso a Internet, FortiManager también puede funcionar como servidor de distribución de FortiGuard (FDS) para que los dispositivos gestionados puedan descargar las firmas de seguridad directamente desde Fortimanager.

Desde un FortiManager se pueden administrar hasta 5.000 dispositivos y virtual domains (VDOMS) y todos ellos desde una única interfaz de gestión.
El uso de un FortiManager en una infraestructura de seguridad Fortinet puede ayudar a minimizar los costes tanto de los despliegues como de la operación. Permite una rápida provisión de dispositivos, seguimiento detallado de versiones y una minuciosa auditoría.

4.2.1.1 Equipamiento y características técnicas

En este apartado se presentan y describen las características técnicas del FortiManager ofertado en la presente propuesta.

FortiManager VM

El sistema de gestión centralizada a instalar será un producto del fabricante Fortinet denominados FortiManager, en formato virtual.

A continuación, se indican algunas de las funcionalidades de FortiManager:

- Control y seguimiento de configuraciones. El FortiManager guarda y mantiene el historial de todos los cambios de configuración que se hacen a lo largo del tiempo. Estos cambios se pueden programar para que se apliquen de forma automática.
- Gestión centralizada. FortiManager puede gestionar de forma centralizada la configuración de múltiples equipos desde una misma consola. Las configuraciones se pueden compilar en un repositorio centralizado y desplegar en múltiples dispositivos cuando sea requerido.
- Dominios de administración. FortiManager puede dividir la administración de grandes entornos agrupando equipos en dominios de administración a nivel geográfico o funcional.
- Provisión local del servicio FortiGuard. Un FortiGate puede utilizar un FortiManager

para optimizar el rendimiento en la búsqueda de clasificaciones y la descarga de definiciones y firmas para antivirus, IPS, web filtering y email filtering.

- Gestión de firmwares. FortiManager puede gestionar de forma centralizada imágenes de firmware y programar la actualización de dispositivos gestionados.
- Scripting. FortiManager soporta scripts de CLI o TCL para simplificar el despliegue de configuraciones.
- Informes y logging. FortiManager también se puede utilizar para logar tráfico de los equipos administrados y generar informes basados en consultas SQL. El FortiManager también incluye las características de logs e informes de FortiAnalyzer.
- Gestión del ciclo de vida de dispositivos Fortinet. Las tareas de administración de dispositivos Fortinet siguen un ciclo de vida típico: Despliegue, monitorización, mantenimiento y actualización.

4.2.1.2 Especificaciones técnicas

Las características técnicas de éste equipamiento están en el **Anexo I.**

4.3 Plataforma de gestión y salvaguarda de logs y accesos FortiAnalyzer.

4.3.1 Descripción de la solución

La solución diseñada para centralizar y mantener los logs a largo plazo consiste en la instalación y configuración de un sistema de gestión de logs, en formato virtual. Se propone su ubicación en nuestro Centro de Datos.

La familia de productos FortiAnalyzer extiende las capacidades de visibilidad, gestión de alarmas y eventos de las plataformas FortiGate, FortiCarrier, FortiAP, FortiWeb, FortiMail, FortiCache, FortiSandbox, FortiManager, FortiDDOS y FortiClient, así como de otros dispositivos de terceros compatibles con Syslog.

Un conjunto de informes fácilmente configurables permite analizar, reportar y almacenar eventos de seguridad, tráfico de red, contenido web y mensajes para medir el cumplimiento de políticas de una organización.

4.3.1.1 Equipamiento y características técnicas

En este apartado se presentan y describen las características técnicas del FortiAnalyzer ofertado en la presente propuesta.

FortiAnalyzer VM

El sistema de gestión centralizada a instalar será un producto del fabricante Fortinet denominados FortiAnalyzer, en formato virtual.

A continuación, se indican algunas de las funcionalidades de FortiAnlyzer:

- Más de 550 informes y gráficos configurables ayudan a monitorizar y mantener identificados patrones de ataques, políticas de uso aceptable y a demostrar el cumplimiento de políticas.
- Informes de capacidad y utilización de la red, que permiten gestionar las redes de forma planificada y eficiente.
- Arquitectura escalable que permite al dispositivo funcionar en modo colector o analizador, para optimizar el procesamiento de logs.
- Funcionalidades avanzadas, tales como la correlación de eventos, análisis forense y vulnerabilidades de los activos, proporcionan herramientas esenciales para una defensa en profundidad en redes complejas.
- Agregación segura de datos desde múltiples dispositivos de seguridad, que proporciona visibilidad completa de la red.
- Integración completa con FortiManager, como punto centralizado de comando, control, análisis e informes.

- Segmentación de la información generada por los dispositivos en dominios administrativos permitiendo modelos de delegación basados en roles o tipo MSSP.
- Ciclo completo de gestión de la información que abarca los procesos de recolección, normalización, clasificación, correlación y explotación en modo de alertas e informes.
- Gran capacidad para almacenar logs, así como elegir entre diferentes niveles de RAID (0, 1, 5, 6, 10, 50 y 60), discos en "spare", e intercambio de discos en caliente, permiten asegurar los datos para cumplir con las necesidades de la organización.
- Soporte IPv6, tanto para la recepción de logs como para el acceso de administración a la plataforma.
- Ejecución de diferentes utilidades de diagnóstico, tales como: ping, traceroute y visor de logs.
- Posibilidad de despliegue de la plataforma en diversas plataformas de virtualización.
- Servicios de integración web desde terceras aplicaciones con Web Services.
- Múltiples usuarios de administración con diferentes perfiles de gestión administrativa basada en roles.

4.3.1.2 Especificaciones técnicas

Las caracteríisticas técnicas del equipo FortiAnlyzer están en el **Anexo I.**

4.4 Equipo de monitorización y gestión de eventos de la seguridad de red Ariolo Alienvault USM SIEM 360.

Ariolo USM SIEM Premium 360 ®

El sistema *Ariolo SIEM Premium* ® tiene la capacidad de realizar auditorías automáticas y periódicas al obtener, normalizar, correlar, agrupar y analizar eventos de seguridad de red que determinan si el sistema de información salvaguarda el activo empresarial. Su ubicación será el Centro de Datos de Diputación.

Los ingenieros de Ariadnex S.L. analizarán mediante el sistema *Ariolo SIEM Premium* ® las alertas recabadas con la herramienta y valorarán las alarmas indicando los posibles puntos de fallo y de mejora de la infraestructura.

El Sistema de Monitorización y Gestión de Eventos de Seguridad es un producto que permite, entre otras funciones, verificar el comportamiento de un equipo en un determinado entorno. El sistema propuesto integra diferentes herramientas del mundo del Software Libre como son Nagios, Nesus/OpenVas, p0f, Snort/Suricata, Spade, Arpwatch, nmap, entre otras. La inteligencia *Ariolo SIEM Premium* ® realiza la **correlación activa de logs y la generación de informes desde un único interfaz** que facilita el acceso, la configuración y la gestión de la información de seguridad por los operadores.

- Identificación de ataques en tiempo real.
- Sistema de gestión integral de incidentes.
- Análisis orientado a riesgos.
- Monitorización de disponibilidad y recursos.
- Inventariado automático de activos.
- Cuadro de mandos flexible y personalizable.
- Informes sobre cumplimiento de normativas.
- Análisis y generación de informes en tiempo real.
- Arquitectura multi-nivel y multi-cliente.

Para instalar y gestionar este tipo de soluciones, la empresa Ariadnex, S.L. se apoya en los estándares para llegar a la configuración más contrastada. La utilización de estándares, y más concretamente una metodología, asegura que todos los aspectos acerca de la seguridad quedan contemplados.

4.4.1 Producto Ariolo SIEM Premium ®

La aportación del Sistema de Monitorización y Gestión de Eventos de Seguridad nos permitirá realizar una correlación inteligente contextual que se adapta a las necesidades de la seguridad de la organización, además de al cumplimiento de las normativas y regulaciones existentes: LOPD, LSSICE, PCI, ISO, SOX, FISMA, HIPAA, etc. Este sistema tiene la capacidad de correlar, priorizar y medir el riesgo a partir de los datos recogidos, mejorando la fiabilidad y sensibilidad de los eventos detectados.

El producto incorpora un conjunto de herramientas, todas ellas Open Source que permiten complementar la información recibida de los logs de los sistemas y aplicaciones a monitorizar para ofrecer una seguridad unificada.

Concretamente, como sistema de análisis de vulnerabilidades, el producto incorpora OpenVAS. La consola de gestión permite la selección de los sistemas a analizar, tipo de análisis a realizar, forma de ejecución, planificación de la ejecución.

El producto integra las bases de datos de vulnerabilidades para que sean accesibles desde el portal web, pudiéndose hacer búsquedas sobre las mismas, enlazarlas con el gestor de incidencias o la base de datos de conocimiento. Además, la información proporcionada por estas bases de datos se utiliza por los motores de correlación para identificar activos afectados por las vulnerabilidades así como para asignar un valor de riesgo a las incidencias encontradas.

Las bases de datos de vulnerabilidades son actualizadas cada 15 días para mantener su funcionalidad y preservar la integridad y la seguridad de la plataforma auditada.

La integración de los análisis de vulnerabilidades, bases de datos, y otras herramientas, dan valor al conjunto de la plataforma, permitiendo obtener información más rica y completa en cuanto a la seguridad de la red, al tiempo de obtener indicadores, métricas, informes y pudiendo gestionar las incidencias encontradas.

La plataforma, así como las herramientas que la componen, aportan las siguientes funcionalidades:

- Realizar análisis de vulnerabilidades automáticos con OpenVas de forma programada. Estos dan lugar a informes específicos para cada activo escaneado con detalles de las vulnerabilidades encontradas así como respuestas recomendadas para cada una de ellas. Se podrán, a su vez, definir diferentes tipos de análisis en función de la agresividad de los mismos y los servicios susceptibles de ser probados.
- Cruzar los datos de las vulnerabilidades recogidas con CVE, OSVDB. En base a los identificadores de las mismas, los informes de vulnerabilidades serán completados con información referida a las vulnerabilidades encontradas, en las bases de datos mencionadas. Esto permite elaborar informes con el máximo nivel de detalle técnico y soluciones posibles a una determinada vulnerabilidad.
- Generar incidencias en referencia a los activos analizados con diferentes niveles de prioridad y riesgo.

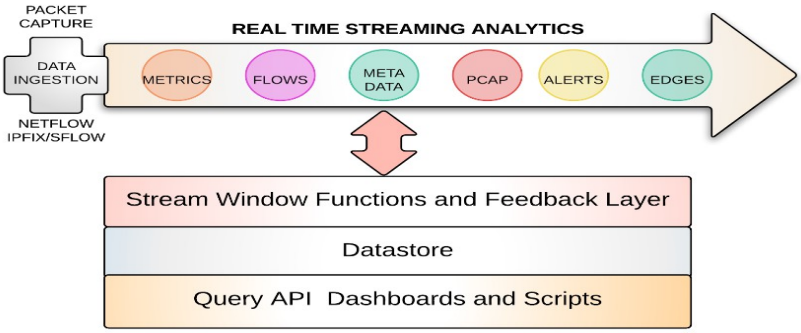
La herramienta también permite la personalización. Es decir, se permite crear dashboards específicos en base a campos como tipo de vulnerabilidad, sistema al que afecta, fabricante, gravedad, parche, etc.

A su vez se definen una serie de métricas a utilizar para monitorizar el estado de seguridad. Estas métricas permiten, al personal especializado, conocer el grado de exposición a amenazas externas de los servicios escaneados.

4.4.2 Ariolo SIEM Premium ® de Análisis y Monitorización de todo el tráfico de Red

Las organizaciones necesitan cada vez mayor visibilidad de la red, monitorización de la seguridad de la red, capturar amenazas, y capacidades de respuesta a incidentes. El sistema de análisis del tráfico y monitorización de seguridad en la red funciona capturando los paquetes de la red o mediante tecnología Netflow para proporcionar visibilidad en tiempo real y analítica histórica. El sistema utiliza algoritmos de analítica para dar respuesta en tiempo real en lugar de las soluciones tradicionales basadas en bases de datos. La imagen que se muestra a continuación presenta los seis bloques que tiene el sistema: métricas de tráfico, flujos de red, metadatos, alertas de seguridad, y almacenamiento de paquetes en formato RAW.

Métricas de ancho de banda y tráfico: visibilidad en profundidad



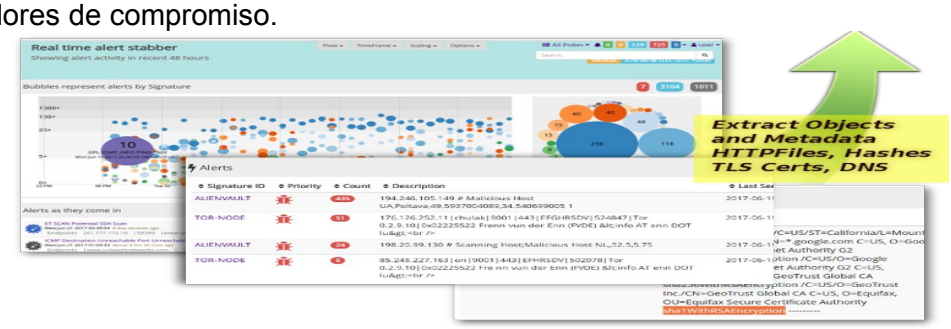
El sistema trae la mejor visibilidad en tráfico de red de su clase. Mientras procesa los paquetes en formato RAW continuamente extrae métricas de más de 200 tipos de tráfico en alta resolución (en menos de 100 msec). Además, el sistema tiene habilitado por defecto las métricas avanzadas como los contadores de cardinalidad (por ejemplo aplicaciones únicas por equipo) y snapshots Top-N. El administrador puede crear también métricas personalizadas usando una API. Algunas de las más de 200 métricas incluyen Equipos, Aplicaciones, Puertos, Números de Sistema Autónomo, MAC, VLAN, Métricas de Capa 2, SSL Orgs, Certificados, Algoritmos de Cifrado, Códigos de Respuesta HTTP, perfiles de tráfico de Redes Sociales, categorías de URL, etc. Las métricas en tiempo real permiten visualizar el tráfico en tiempo real de cualquier métrica. Esto permite una rápida respuesta a incidentes.

Análisis de Flujos: base de datos de flujos altamente escalable para investigación

Un flujo representa una conversación IP. El sistema reconstruye los flujos a partir de los paquetes, los indexa y los almacena en una base de datos personalizada y diseñada para escalar a billones de flujos con tiempos de respuesta de milisegundos. La herramienta de exploración de flujos nos permite realizar peticiones a la base de datos de flujos usando cualquier criterio. El sistema tiene un algoritmo llamado Flow Tracker que realiza “fotos instantáneas” de varios flujos interesantes como por ejemplo de flujos sospechosos o flujos de transferencias de ficheros fuera de la organización. Todos los flujos se almacenan para poder ser analizados durante el proceso de investigación de incidentes.

Metadatos: extrae objetos del tráfico de red

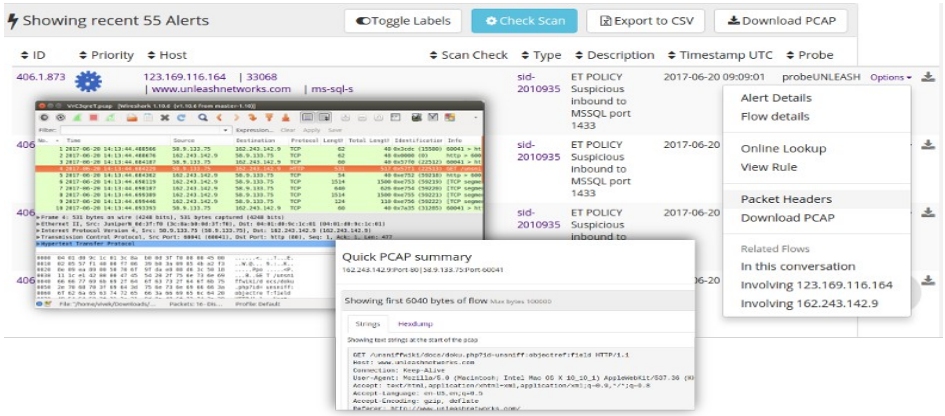
El sistema extrae varios tipos de objetos de los paquetes que se almacenan como Recursos y como Documentos FTS (Full Text Search). Algunos ejemplos son los registros de DNS, URLs HTTP, certificados SSL, hashes de ficheros, archivos binarios, y cabeceras HTTP. Estos objetos se pueden consultar en la fase de investigación o analizados como indicadores de compromiso.



Análisis de Seguridad: integración con IDS y sistemas inteligentes de amenazas

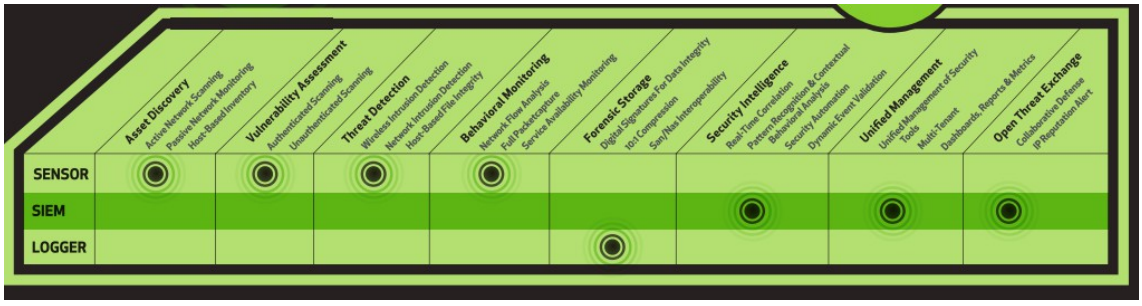
La plataforma se integra con sistemas IDS y procesos de alertas a través del mismo canal de análisis. Esto permite una estrecha correlación entre las alertas de intrusión y otros tipos de datos. Por ejemplo, se puede etiquetar los flujos para generar alertas de prioridad 1 para su posterior análisis. Además, el sistema incluye un plugin llamado Badfellas que automáticamente actualiza las firmas de inteligencia y analiza el tráfico contra ellas. El módulo de alertas en tiempo real es un cuadro de mandos de alertas en tiempo real que permite mostrar claramente las alertas.

Análisis de Paquetes: análisis de los paquetes en profundidad desde cualquier contexto



El sistema indexa y analiza todos los paquetes en formato cifrado. El sistema permite analizar los paquetes para obtener los flujos, alertas, tráfico, o cualquier otro dato en un intervalo de tiempo específico. Además, las políticas de poda permiten que el tráfico innecesario se almacene en el sistema aumentando así el intervalo de retención.

El equipo suminsitrado integrará todas las funciones y capacidades en u modelo todo en uno.



4.4.2.1 Especificaciones técnicas

Las características técnicas del equipamiento SIEM USM Alienvault / Ariolo 360 están en el **Anexo I.**

5 Gestión del Servicio

En un escenario ideal, los servicios y sistemas funcionan con normalidad pero cuando los problemas aparecen, y llegado el caso tiene lugar una degradación o pérdida de servicio, las empresas y fabricantes debemos demostrar empatía y capacidad de respuesta. Para ello se dispondrá de un soporte por parte del fabricante disponible en horario adecuado al servicio.

Además, las plataformas estarán suscritas a un servicio de actualizaciones de firmas, firmware y software para mantener los sistemas actualizados.

Más allá del cumplimiento formal de los niveles de calidad de servicio, **Ariadnex proveerá un servicio de gestión y resolución de incidencias y peticiones de servicio con el fin de garantizar la plena disponibilidad de los sistemas y servicios.** Ariadnex se compromete a cumplir los niveles de calidad de servicio exigidos en el pliego, y que así son requeridos por la Diputación Provincial de Cáceres.

Ariadnex S.L. mantendrá y pondrá a disposición de la Diputación Provincial de Cáceres un repositorio donde se almacenarán los ficheros de configuración de los dispositivos de red, además, se mantendrá un histórico con todos los cambios efectuados sobre la configuración de los equipos indicando la fecha de realización.

Ariadnex S.L. se compromete de llevar a cabo el mantenimiento, puesta al día y control de actualizaciones de toda la plataforma en cualesquiera que sean las circunstancias incluso de forma proactiva en todo el ciclo de vida del servicio.

5.1 Gestión de incidencias y consultas

A continuación se describe la metodología y las tareas y el compromiso de Ariadnex S.L. con Diputación Provincial de Cáceres en el proceso de gestión de incidencias y consultas:

Tareas del Centro de Gestión

Ariadnex S.L., se compromete a implementar y evidenciar la exigencia del pliego del modelo “UNA SOLA LLAMADA” es decir que todas las incidecias y peticiones de

servicio se resolverán o encauzarán en una sola primera llamada, sin centros de de recepción que reasignen las llamadas, ni locuciones, ni otro tipo de mecanismos que obliguen a los usuarios y técnicos a realizar varias llamadas o interaccciones.

- Para la consulta y gestión de incidencias, Ariadnex dispone de un centro de atención personalizada por ingenieros de la plataforma ofertada. Además, Ariadnex S.L., cuenta con un ingeniero certificado en **CISM de ISACA** que estará a disposición durante toda la duración del contrato Director y Gestor del proyecto y la entrega del servicio.
- Ariadnex S.L. se encuentra ubicada en Extremadura donde se dispone de laboratorios y del centro de Soporte y control y gestión del Servicio. Al tener oficina en Extremadura tiene la posibilidad de acudir a las entidades locales en cuestión de horas si así se requiere.
- El servicio que ofrece Ariadnex S.L. incorpora la posibilidad de presentar y explicar la incidencias y consultas que Diputación Provincial de Cáceres estime conveniente por un Ingeniero en Seguridad.
- Ariadnex S.L., dispone y pondrá a disposición del servicio de de un sistema de ticketing que permite abrir incidencias y consultas a través de correo electrónico, teléfono o vía web y también por la herramienta Telegram. Esta herramienta permite documentar todas las incidencias realizadas así como calcular tiempos de espera y resolución de cada ticket. La herramienta de ticketing permite a la Diputación Provincial de Cáceres comprobar si se están cumpliendo los acuerdos de nivel de servicio (SLA) exigidos en el pliego.
- Ariadnex también ofrece un servicio de notificaciones proactivas, por teléfono o mediante correo electrónico, para comunicar al técnico o personal asignado por la Diputación Provincial de Cáceres de aspectos que puedan impactar sobre el rendimiento o el adecuado funcionamiento del sistema de seguridad perimetral. Por ejemplo, la comunicación de vulnerabilidades o bugs sobre el sistema de seguridad perimetral.
- Ariadnex S.L., realizará revisiones periódicas de la configuración de los equipos para proponer mejoras de configuración.
- Ariadnex S.I. se aplicará, como servicio gestionado, las recomendaciones de configuración destinadas a mejorar el rendimiento de los sistemas.
- Ariadnex S.L., pondrá a disposición de Diputación de Cáceres un servicio para personalizar informes según los requerimientos que determine el cliente.

Compromiso del Centro de Gestión

Ariadnex S.L., se compromete al mantenimiento preventivo, correctivo y adaptativo de todas las actuaciones necesarias, tanto sobre la red, como sobre el equipamiento, destinadas a evitar la aparición de incidencias. Se realizarán los controles, análisis,

estudios, pruebas y operaciones necesarias para minimizar la probabilidad de averías y cortes del servicio, incrementando así la vida útil de los sistemas.

Mantenimiento preventivo:

- Análisis de las incidencias con fallos repetitivos y propuesta de un plan de acciones para que no se repitan.
- Revisión de los elementos en los que se hayan producido incidencias repetitivas.
- Realización de pruebas periódicas que permitan verificar el cumplimiento de los valores ópticos comprometidos.

Mantenimiento Correctivo:

- Este servicio consiste en la asignación, seguimiento y control de las actividades encaminadas a resolver las posibles anomalías detectadas por la Diputación Provincial de Cáceres y notificadas en la herramienta de ticketing, por correo electrónico o por teléfono y/o Telegram.
- Una vez detectada la incidencia, el personal operativo procederá a diagnosticar la posible causa, iniciando las acciones necesarias para proceder a subsanarla en el menor plazo de tiempo posible.
- Cuando resulte factible, la resolución de las anomalías será llevada a cabo mediante la conexión remota o en el caso contrario se procederá a trasladar personal técnico a las dependencias donde se encuentre el sistema que presente las anomalías.
- Durante toda vida activa de la incidencia y en cualquier momento la entidad local podrá disponer de la información del estado de resolución de la misma mediante contacto directo con Ariadnex S.L.
- Una vez solucionada la incidencia, Ariadnex S.L. verificará, a través de las herramientas necesarias el funcionamiento del servicio, así como entregar un informe de la resolución de la incidencia si así lo requiere la entidad local.

El centro de gestión de Ariadnex tiene los recursos necesarios para monitorizar los servicios ofrecidos y poner a disposición de Diputación Provincial de Cáceres la información resultante de sus análisis, entregando informes y estadísticas sobre los resultados de dichas medidas de tal forma que se pueda comprobar el cumplimiento del nivel de servicio.

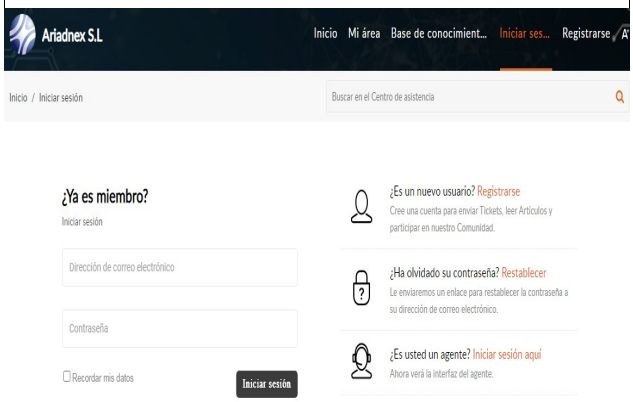
Para aquellos trabajos que supongan una interrupción parcial o total de los servicios prestados, Ariadnex S.L., se compromete a realizar dicho trabajo fuera del horario laboral siempre de conformidad con Diputación Provincial de Cáceres. Presentando un plan específico de trabajo que refleje las tareas a realizar, el equipamiento y servicios afectados y los mecanismos de recuperación.

Dicho plan deberá ser verificado y aprobado por Diputación o la entidad local como requisito previo e indispensable para su ejecución.

La disponibilidad de los servicios estará garantizada a excepción de los periodos de interrupción imprescindibles para el desarrollo de los trabajos programados. Además, se preverán mecanismos de recuperación con un tiempo máximo de vuelta atrás de 12 horas.

6 Soporte Técnico

Ariadnex dispondrá, aparte de un teléfono centralizado, de los recursos necesarios para satisfacer el buen funcionamiento de los sistemas de la **Diputación Provincial de Cáceres**, adecuando una herramienta de comunicación para la gestión de tickets o incidencias, una dirección de correo, un teléfono de contacto y un sistemas de creación de tickets mediante la herramienta de mensajería instantánea Telegram para cualquier tipo de necesidad por parte de las entidades locales o de **Diputación Provincial de Cáceres**.

Notificación WEB	Notificación Telegram
	

Diputación Provincial de Cáceres y las entidades locales dispondrán de toda la información necesaria de los fabricante/s para cualquier tipo de gestión que estime necesaria, como por ejemplo un RMA al día siguiente hábil cuando el fabricante acepta el reemplazo.

Ariadnex S.L., siempre velara por un equipamiento actualizado en seguridad y en sistemas, e informará en todo momento a **Diputación Provincial de Cáceres** de intervenciones futuras para mejorar el funcionamiento y optimización de manera proactiva. Asesorará al cliente buscando siempre el mejor rendimiento de todos los equipos utilizados.

Todas las plataformas ofertadas estarán suscritas a un servicio de actualizaciones por el período determinado.

Se contará con el soporte del fabricante Fortinet donde toda su familia de productos y servicios disponen de un soporte online para poder acceder y resolver todo tipo de dudas que puedan surgir con el servicio, equipamiento, licencias, etc. Ariadnex se encargará de interactuar de forma directa con el fabricante y se facilitarán a la Diputación Provincial de Cáceres los datos de acceso a los portales web del fabricante para la gestión del equipamiento y licencias así como a las bases de conocimiento y herramientas de soporte para consultas o gestión de incidencias.

Las incidencias abiertas a través de la herramienta serán respondidas y resueltas dentro de los márgenes de tiempo especificados por personal técnico cualificado, entendiendo por cualificado personal con títulos superiores.

Ariadnex S.L., ofrecerá un servicio personalizado de soporte técnico con diferentes niveles:

- **Técnicos de Soporte de Primer nivel.**

Técnicos e ingenieros que diagnostican y resuelven las incidencias, o bien determinan la necesidad de escalar ante circunstancias determinadas para ser atendidas por el siguiente nivel, bien por la propia dificultad o complicación de la misma o sencillamente por criticidad o prioridad.

- **Técnicos de Soporte de Segundo nivel.**

Son un grupo de ingenieros de alto nivel disponibles para dar soporte a los técnicos de campo en el diagnóstico y resolución de las incidencias recibidas en el Centro de Atención al Cliente, que requieran una respuesta experta. Los ingenieros de soporte tienen conocimientos profundos de todas las soluciones de comunicaciones y seguridad comercializadas por Ariadnex, que actualizan por medio de un proceso de formación continua.

- **Gestor del servicio.**

Será un ingeniero o una ingeniera encargado/a de dirigir el proyecto y de tanto coordinar como supervisar todas las tareas a realizar en todas las fases que conforman el proyecto.

En el caso de los elementos de terceros fabricantes, el servicio técnico de Ariadnex se encargará del diagnóstico, localización y resolución de fallos cuando el cliente lo demande.

En el caso que la resolución de los incidentes no sea posible por medio de los técnicos de Ariadnex, ya que se puede tratar de un bug o anomalía del sistema o plataforma, Ariadnex se encargará del reporte de los mismos al fabricante.

6.1 Clasificación de Incidencias

Las incidencias serán clasificadas en función de la gravedad de la siguiente manera:

- Prioridad ALTA: serán aquellas consideradas como tal por el personal de la entidad local o la Diputación Provincial de Cáceres y que supongan una pérdida o una grave degradación del servicio, incluyendo en esta categoría todas las incidencias de avería hardware de cualquier dispositivo.
- Prioridad MEDIA: serán aquellas que degraden el servicio permitiendo su uso con funcionalidades alteradas o restringidas.
- Prioridad BAJA: serán aquellas que afecten al servicio pero no lo degraden ni influyan en capacidades y funcionalidades esenciales. En esta categoría se incluyen las peticiones de cambio y las consultas sobre el uso, procedimientos y cambios de la plataforma.

Ariadnex S.L., ofrecerá una cobertura horaria, entendiéndose como tal la franja horaria en la que las entidades locales o la Diputación Provincial de Cáceres podrán realizar una consulta que será atendida en tiempo y forma.

Los niveles de servicio serán, como mínimo, los siguientes:

SLA SERVICIO DE SOPORTE ADJUDICATARIO DESDE LAS 8:00 HASTA LAS 18:00 HORAS.	
PARÁMETRO	VALOR
Cobertura horaria de atención	10 x 5
Tiempo de intervención incidencias	P. Alta: Máximo 2 horas. (To + 2h) P. Media: Máximo 4 horas. (To + 4h) P. Baja: Máximo 8 horas. (To + 8h)
Tiempo de resolución incidencias	P. Alta: Máximo 4 horas. (To + 4h) P. Media: Máximo 8 horas. (To + 8h) P. Baja: Máximo 24 horas. (To + 24h)
Tiempo de intervención consultas	Máximo 24 horas (To + 24 horas)

Para asegurar que se cumplen los tiempos señalados, Ariadnex S.L., dispondrá de, como mínimo un 3% de los dispositivos suministrados de cada tipo en stock, es decir, de equipamiento perimetral, de equipamiento wifi y de equipamiento de switching.

7 Garantía Ariadnex S.L.

Ariadnex, S.L. proveerá durante al menos 1 año de un servicio de garantía en toda su extensión y en todos los elementos suministrados tanto de software como de hardware.

Nuestra empresa asumirá todos los compromisos de mantenimiento y actualizaciones de todos lo elementos que se suministren así como de la mano de obra y servicio por el tiempo exigido en el pliego.

Asi mismo, y en virtud de cumplir con los mencionados compromisos, nuestra empresa contratará todos los servicios y mantenimientos necesarios con terceros para poder asegurar que se cumplen los tiempos de reparación, mantenimiento, actualizaciones, etc., y que están reflejados en los apartados correspondientes de nuestra oferta.

Entendiendo la evidente complejidad en cuando a prestaciones y funcionalidades de la plataforma, resulta especialmente relevante poder disponer de los acuerdos de niveles de servicio con los proveedores para poder asegurar que se cumplen todos y cada uno de los compromisos con Diputación de Cáceres.

Para el aseguramiento de la garantía y calidad de servicio en los términos exigidos en el pliego, Ariadnex S.L., asegurará los mismos en virtud de los acuerdos necesarios con los proveedores, fabricantes y socios especializados propuestos.

De acuerdo a la siguiente tabla:

Fabricante	Tipo Equipamiento	Garantía de atención Hw	Tipo soporte Fab	Mantenimiento Ariadnex
	Firewalll de las entidades y en CPD Diputación.	*NBD*	*24x7*	*24x7 Español*
	Puntos de Acceso de las entidades	*NBD*	*24x7*	*24x7 Español*
	Switches de las entidades	*NBD*	*24x7*	*24x7 Español*
	FortiAnalyzer	*NBD*	*24x7*	*24x7 Español*
	Fortimanager	*NBD*	*24x7*	*24x7 Español*
	Appliance SIEM en CPD Diputación.	*NBD*	*Ardnx partners 24 x 7*	*24x7 Español*
	Appliances Hw y Sw Centro de Datos propio	< 2 hr	24 x 7	*24x7 Español*

Las garantías y mantenimientos de productos y servicios cumplirán en todos los casos las condiciones necesarias que permitan atender y resolver en tiempo y forma cualquier incidencia dentro de la plataforma. Nuestros acuerdos incluyen, y no sólo, los siguientes:

Equipamiento de seguridad de perímetro, Wifi , switching, gestión de logs y Manager

- Servicio FortiCare, 24 horas del día, los 7 días de la semana, Se cubre durante todo el día, siempre que necesite cobertura de soporte técnico. Incluye soporte vía web, chat y teléfono para nuestro equipo global. Los reemplazos de hardware se envían al siguiente día hábil de envío, antes de recibir el dispositivo original. Se incluyen las suscripciones fundamentales de FortiGuard para políticas dinámicas. Se suministra en la opción UTP.

	A-la-carte	ATP	UTP	ENT
24×7 Support	✓	✓	✓	✓
Content Security AV, AI powered Cloud Sandbox +	✓	✓	✓	✓
Web Security AI-Powered Web, Video, DNS Filtering +	✓		✓	✓
Device Security IoT, OT security & compliance tools	✓			✓
Advance SOC/NOC Tools SOC as a Service, Cloud Delivered Management & Analytics +	✓			

- Equipamiento de correlación de eventos y seguridad de la información.
  - El cliente recibirá las actualizaciones tanto de las versiones como las *minor releases* de la versión profesional de Ariolo / AlienVault USM. Estas versiones son lanzadas cada 6 meses normalmente. Así mismo el fabricantet ofrece dos niveles de soporte Estandar y Premium para asegurar que nuestro cliente recibe el servicio que necesita en el memento que lo necesita.

Cada uno de los niveles ofrece las siguientes características

Support Feature	Standard	Premium
Product Updates*	Yes	Yes
Online Ticket Submission/Tracking	Yes	Yes
Access to Knowledgebase	Yes	Yes
Response Type	Phone/Email/Web	Phone/Email/Web
Contract Coverage Hours/Day	8 hours	24
Coverage Days/Week	5	7
# Supported Contacts Allowed **	5	10
# Support Requests Allowed (Annually)	Unlimited	Unlimited
Holiday Coverage	No (see Section 12)	Yes

**Includes version Updates (major & minor), hot fixes, etc.*
*** Eligibility to become a designated support contact requires AlienVault certification*

Independientemente de las necesidades de servicio de atención sobre las garantías de los productos y servicio Ariadnex S.L pone un único PUNTO DE CONTACTO DE SERVICIO que es el reseñado en el apartado Soporte Técnico.

8 Actualización

FortiGuard Labs, la organización de investigación e inteligencia de amenazas de Fortinet, desarrolla, innova y mantiene uno de los sistemas de aprendizaje automático e inteligencia artificial más reconocidos y experimentados de la industria. Fortinet utiliza esto para brindar protección, visibilidad y continuidad comercial incomparables y comprobadas en todo el Fortinet Security Fabric, protegiendo a los clientes contra la amplia gama de amenazas sofisticadas y en constante cambio.

Esta plataforma ingiere y analiza 100 mil millones de eventos todos los días, en promedio, para entregar más de mil millones de actualizaciones de seguridad diarias para proteger a todos los clientes contra amenazas nuevas y desconocidas en todas las implementaciones de Security Fabric.

Por otro lado, AlienVault y, entre otros, su servicio OTX ofrece mecanismos para la actualización de las bases de datos de firmas, con el objetivo de mantener el sistema actualizado y detectar de forma rápida y ágil cualquier intento de ataque y/o intrusión.

La suscripción de firmas ofrece la actualización continua de los elementos de Ariolo USM SIEM permitiendo tener la plataforma permanentemente preparada ante nuevas vulnerabilidades y ataques.

La plataforma integra un sistema que permite actualizar las bases de datos de vulnerabilidades de forma automática. Entre otras cosas, también se actualizan plugins para hacer escaneos, reglas de IDS y directivas de correlación. Todo ello necesario para la adecuada explotación del sistema.

La Suscripción está desarrollada por el VRT (Vulnerability Research Team) que analiza continuamente los nuevos ataques y genera nuevas directivas de correlación (Reglas de Correlación) y los elementos necesarios para que estas sean efectivas (firmas de snort, plugins de nessus, etc.).

La suscripción se realiza a través de un feed automático que es recogido por el management server y reenviado a cada sensor si es necesario.

El feed incluye la actualización y los siguientes objetos:

- Directivas de Correlación
- Plugins de Colección
- Firmas de análisis
- Plugins de analizadores.
- Tablas de correlación cruzada e inventario
- Grupos de políticas

Ariadnex se compromete a actualizar, durante al menos un año, todas las licencias, bases de datos y firmas de las distintas plataformas.

Así mismo, Ariadnex se compromete a actualizar, durante al menos un año, el firmware de todos los equipos a la última versión estable publicadas por cada fabricante.

9 Dotaciones Opcionales

Aunque en una primera aproximación al proyecto no preveemos disponer de dotaciones adicionales con excepción de las púramente de servicios, es decir, incorporación de recursos y medios tantos como sean necesarios para la consecución exitosa del mismo queremos reseñar que en nuestro compromiso con Diputación de Cáceres estaremos en disposición de habilitar el equipamiento y recursos necesarios, dentro de lo razonable, aunque no se haya reflejado expresamente en la presente oferta.

10 Plan de trabajo y cronograma

A continuación se reflejan los procedimientos de trabajo, cronograma, recursos asignados y planificación de tareas.

10.1 Planificación de los trabajos

Ariadnex se compromete a realizar la instalación y puesta en marcha en un plazo de 6 meses desde la firma del contrato.

A continuación se describen las tareas que realizará Ariadnex durante el transcurso del proyecto. Todas las tareas de coordinación y dirección del proyecto realizadas por Ariadnex

siempre serán puestas en conocimiento y comunicadas a la Diputación Provincial de Cáceres.

El proyecto está compuesto principalmente por las cuatro fases que se describen a continuación. Como punto de partida, tenemos que destacar el arranque del proyecto.

10.1.1 Proceso de iniciación

Arranque del Proyecto

Desde el inicio del proyecto, Ariadnex tendrá comunicación directa con el cliente para realizar la Dirección del Proyecto. Al inicio se presentará el equipo del proyecto, formado por ingenieros de Ariadnex, se explicará el alcance y las fases del proyecto, además de los plazos y calendario de las tareas a realizar durante toda la extensión del servicio.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Sistema de seguridad y acceso a Internet seguro para entidades locales**	**128,86 días**	**vie 01/10/21**	**mié 30/03/22**
2	**Procesos de iniciación**	**0,25 días**	**vie 01/10/21**	**vie 01/10/21**
3	**Arranque del proyecto**	**0,25 días**	**vie 01/10/21**	**vie 01/10/21**
4	Reunión inicial de arranque de proyecto	1,5 horas	vie 01/10/21	vie 01/10/21
5	Elaboración del calendario del proyecto	30 mins	vie 01/10/21	vie 01/10/21
6	Entrega del calendario del proyecto	0 días	vie 01/10/21	vie 01/10/21

10.1.2 Procesos de Análisis y Diseño

En esta fase Ariadnex liderará la recopilación de información especialmente para el despliegue de la solución técnica. Ariadnex dinamizará las actividades para que, con la colaboración e implicación de los técnicos de la Diputación Provincial de Cáceres, disponga de toda la información del entorno y pueda, a nivel de detalle, diseñar la instalación y configuración de la plataforma.

Procesos de Análisis

Este proceso consiste en obtener la arquitectura actual de la infraestructura para diseñar la instalación de la plataforma de seguridad y la migración de los servicios de producción.

7	**Procesos de análisis y diseño**	**0,63 días**	**vie 01/10/21**	**vie 01/10/21**
8	**Proceso de análisis**	**0,13 días**	**vie 01/10/21**	**vie 01/10/21**
9	Análisis de la arquitectura actual	30 mins	vie 01/10/21	vie 01/10/21
10	Análisis de los sistemas actuales	30 mins	vie 01/10/21	vie 01/10/21

Proceso de Diseño

En esta tarea se diseñará la arquitectura final que tendrá la plataforma, además de definir y diseñar el método y procesos de migración de las conexiones, siempre priorizando la dispo-

nibilidad de los servicios en producción y con procedimientos de vuelta atrás o rollback para ser ejecutados ante cualquier imprevisto.

11	**Proceso de diseño**	**0,5 días**	**vie 01/10/21**	**vie 01/10/21**
12	Diseño de la arquitectura	2 horas	vie 01/10/21	vie 01/10/21
13	Diseño de la implantación	2 horas	vie 01/10/21	vie 01/10/21

10.1.3 Proceso de ejecución y control

Dotación del centro de datos centralizado

En esta fase se efectuará el registro de los dispositivos además de llevar a cabo el licenciamiento de los mismos. Se entregará una documentación con todos la información relacionada con los procesos de instalación de los diferentes productos.

➔ *Plataforma de gestión centralizada*

En esta tarea se desplegará el sistema de gestión centralizado en el CPD Ariolo, para ello, se configurarán los segmentos de red necesarios y se configurará el acceso. Una vez se hayan desplegado los sistemas necesarios se configurarán los informes que se enviarán de forma periódica.

14	**Proceso de ejecución y control**	**126,8 días**	**vie 01/10/21**	**mar 29/03/22**
15	**Dotación del centro de datos centralizado**	**3,19 días**	**vie 01/10/21**	**jue 07/10/21**
16	**Plataforma de gestión centralizada**	**0,48 días**	**vie 01/10/21**	**lun 04/10/21**
17	Instalar y desplegar el sistema en CPD Ariolo	2 horas	vie 01/10/21	lun 04/10/21
18	Configuración de red	30 mins	lun 04/10/21	lun 04/10/21
19	Configuración de visibilidad (NOC/SOC)	15 mins	lun 04/10/21	lun 04/10/21
20	Configuración de notificaciones y alertas	20 mins	lun 04/10/21	lun 04/10/21
21	Configuración de Security Fabric	15 mins	lun 04/10/21	lun 04/10/21
22	Configuración y planificación de informes	30 mins	lun 04/10/21	lun 04/10/21

➔ *Plataforma de gestión y salvaguarda de logs y accesos*

En esta tarea se desplegará el sistema de gestión y salvaguarda de logs y accesos e el CPD Ariolo, para ello, se configurarán los segmentos de red necesarios. Posteriormente se establecerán los niveles de análisis para la generación de informes que periódicamente se enviarán a la Diputación Provincial de Cáceres.

23	**Plataforma de gestión y salvaguarda de logs y accesos**	**0,44 días**	**lun 04/10/21**	**lun 04/10/21**
24	Instalar y desplegar el sistema en CPD Ariolo	2 horas	lun 04/10/21	lun 04/10/21
25	Configuración de red	30 mins	lun 04/10/21	lun 04/10/21
26	Configuración de política de Analítica y Archivado	15 mins	lun 04/10/21	lun 04/10/21
27	Configuración de Security Fabric	15 mins	lun 04/10/21	lun 04/10/21
28	Configuración y planificación de informes	30 mins	lun 04/10/21	lun 04/10/21

➔ *Cortafuegos de nueva generación*

En esta tarea se llevará a cabo la instalación física de los cortafuegos en el CPD de la Diputación Provincial de Cáceres, una vez instalado se actualizarán a la última versión estable recomendada por el fabricante y se configurará los parámetros de red necesarios para poder establecer la comunicación. Posteriormente se configurará la alta disponibilidad entre los dispositivos en modo Activo – Pasivo. Se configurarán los perfiles de seguridad y políticas de que permitirán la navegación. Además, se procederá a configurar el túnel IPSec contra el SOC.

La última fase que se realizará en esta tarea serán las pruebas de alta disponibilidad.

29	**Cortafuegos de nueva generación**	**0,59 días**	**lun 04/10/21**	**mar 05/10/21**
30	Instalar cortafuegos en CPD de la Diputación	2 horas	lun 04/10/21	mar 05/10/21
31	Actualizar firmware	15 mins	mar 05/10/21	mar 05/10/21
32	Configuración de red de los cortafuegos	30 mins	mar 05/10/21	mar 05/10/21
33	Configuración de Alta Disponibilidad (Activo/Pasivo)	10 mins	mar 05/10/21	mar 05/10/21
34	Configuración de Security Fabric	15 mins	mar 05/10/21	mar 05/10/21
35	Configuración de perfiles de seguridad	15 mins	mar 05/10/21	mar 05/10/21
36	Configuración de Políticas IPv4	15 mins	mar 05/10/21	mar 05/10/21
37	Definición y Configuración de Pre-Filtros Sandbox	15 mins	mar 05/10/21	mar 05/10/21
38	Configuración de VPN IPsec contra SOC	30 mins	mar 05/10/21	mar 05/10/21
39	Pruebas de Alta Disponibilidad	20 mins	mar 05/10/21	mar 05/10/21

➔ *Plataforma de monitorización y gestión de eventos de la seguridad*

En esta tarea se llevarán a cabo la instalación del tenant de monitorización y seguridad en CPD Ariolo, también se desplegará en las las instalaciones de la Diputación de Cáceres la sonda que, tras ser configurada y haber valorado los activos y las redes a monitorizar, se establecerá el reenvío de eventos al tenant donde se adaptarán los plugins y se definirán las políticas iniciales.

40	**Plataforma de monitorización y gestión de eventos de la seguridad**	**1,68 días**	**mar 05/10/21**	**jue 07/10/21**
41	Instalar tenant de monitorización y seguridad en CPD Ariolo	1 hora	mar 05/10/21	mar 05/10/21
42	Instalar Sonda en CPD de la Diputación	2 horas	mar 05/10/21	mar 05/10/21
43	Configuración inicial de la plataforma	30 mins	mar 05/10/21	mar 05/10/21
44	Definición de activos y redes a monitorizar	15 mins	mar 05/10/21	mar 05/10/21
45	Definición de servicios a monitorizar	15 mins	mar 05/10/21	mar 05/10/21
46	Determinar sistemas que reenviará eventos	15 mins	mar 05/10/21	mar 05/10/21
47	Definición de puerto en SPAN	30 mins	mar 05/10/21	mar 05/10/21
48	Definición y valoración de activos	30 mins	mar 05/10/21	mié 06/10/21
49	Integración de elementos con la plataforma de monitorización	2 horas	mié 06/10/21	mié 06/10/21
50	Configurar herramienta de monitorización de la disponibilidad	30 mins	mié 06/10/21	mié 06/10/21
51	Configurar reenvío de eventos	1 hora	mié 06/10/21	mié 06/10/21
52	Adaptar plugins	2 horas	mié 06/10/21	mié 06/10/21
53	Configurar monitorización de red	20 mins	mié 06/10/21	mié 06/10/21
54	Definir políticas iniciales	1 hora	mié 06/10/21	mié 06/10/21

Id	Nombre de tarea	Duración	Comienzo	Fin
55	Planificar análisis de vulnerabilidades	1 hora	mié 06/10/21	jue 07/10/21
56	Configurar cuadros de mando	20 mins	jue 07/10/21	jue 07/10/21
57	Registrar y licenciar equipos	15 mins	lun 22/11/21	lun 22/11/21
58	Documentar instalación	2 horas	lun 22/11/21	mar 23/11/21

Dotación de los Ayuntamientos

Previamente a proceder al despliegue de la plataforma de seguridad en las entidades locales, se requiere efectuar varias tareas, estas tareas se definen a continuación.

También se efectuará el registro de los dispositivos además de llevar a cabo el licenciamiento

- ➔ *Armarios rack de comunicaciones*

  Se llevará a cabo un estudio previo para determinar la ubicación del armario rack y el tamaño.

- ➔ *Cortafuegos de nueva generación (91 firewall)*

  Se establecerá la configuración inicial en los 91 cortafuegos, entendiéndose así a la actualización de firmware a la última versión estable, establecimiento de perfiles de seguridad que se aplicarán a las políticas que filtrarán las conexiones y se definirán los filtros iniciales para el envío de datos a FortiSandbox.

- ➔ *Infraestructura de equipos de red (91 switches)*

  Se establecerá la configuración básica de red, se integrarán con la controladora para poder llevar a cabo la actualización de firmware y establecer los perfiles NAC.

- ➔ *Infraestructura inalámbrica (182 APs)*

  Se estudiará el entorno donde se instalarán los puntos de accesos para determinar su ubicación definitiva.

  Se establecerá la configuración básica de red, se integrarán con la controladora para poder llevar a cabo la actualización de firmware y definirán los perfiles de configuración.

59	**Dotación de los Ayuntamientos**	**90,63 días**	**mar 23/11/21**	**mar 29/03/22**
60	**Tareas Previas**	**28,69 días**	**mar 23/11/21**	**vie 31/12/21**
61	**Armarios racks de comunicaciones**	**5,63 días**	**mar 23/11/21**	**mar 30/11/21**
62	Estudio previo para su ubicación y tamaño	45 horas	mar 23/11/21	mar 30/11/21
63	**Cortafuegos de nueva generación (91 firewall)**	**7 días**	**mar 30/11/21**	**jue 09/12/21**
64	Configuración de red inicial	20 horas	mar 30/11/21	vie 03/12/21
65	Actualizar firmware	10 horas	vie 03/12/21	lun 06/12/21
66	Configuación de Security Fabric	6 horas	lun 06/12/21	mar 07/12/21
67	Configuración de perfiles de seguridad	8 horas	mar 07/12/21	mié 08/12/21
68	Configuración de Políticas IPv4	8 horas	mié 08/12/21	jue 09/12/21
69	Definición y Configuración de Pre-Filtros Sandbox	4 horas	jue 09/12/21	jue 09/12/21
70	**Infraesctructura de equipos de red (91 switches)**	**6,31 días**	**jue 09/12/21**	**vie 17/12/21**
71	Configuración de red (IP, DNS, VLAN, etc)	20 horas	jue 09/12/21	mar 14/12/21
72	Integración de switch con la controladora de red	3,5 horas	mar 14/12/21	mar 14/12/21
73	Actualización de firmware del switch	11 horas	mar 14/12/21	mié 15/12/21
74	Configuración de Security Fabric	8 horas	mié 15/12/21	jue 16/12/21
75	Definición de perfiles NAC	8 horas	jue 16/12/21	vie 17/12/21
76	**Infraestructura inalámbrica (182 APs)**	**9,25 días**	**vie 17/12/21**	**vie 31/12/21**
77	Replanteo de los puntos de accesos	45 horas	vie 17/12/21	lun 27/12/21
78	Configuración básica (IP, DNS, País, etc)	10 horas	lun 27/12/21	mar 28/12/21
79	Integración de puntos de accesos con la controladora WiFi	3,5 horas	mar 28/12/21	mié 29/12/21
80	Actualización de firmware de los puntos de accesos	3,5 horas	mié 29/12/21	mié 29/12/21
81	Configuración de Security Fabric	4 horas	mié 29/12/21	jue 30/12/21
82	Definición de perfiles de configuración	8 horas	jue 30/12/21	vie 31/12/21
83	Registrar y licencias equipos	4 horas	vie 31/12/21	vie 31/12/21

Entidad Local 1 (Piloto)

Antes de empezar con la instalación de los dispositivos en las diferentes entidades locales, se llevará a cabo una instalación piloto en uno de los Ayuntamientos, una vez finalizada la instalación y haber efectuados las pruebas oportunas, Ariadnex facilitará un documento con los datos.

➔ *Armarios racks de comunicaciones*

El armario de comunicaciones, en función de la entidad local será de armario o de suelo, el proceso de instalación consistirá en colgarlo o bien ubicarlo.

➔ *Cortafuegos de nueva generación (1 firewall)*

Se instalará el cortafuegos dentro del armario y se realizarán las pruebas de conectividad para asegurar el correcto funcionamiento del mismo.

➔ *Infraestructura de equipos de red (1 switch)*

Se instalará el switch dentro del armario y se realizarán las pruebas de conectividad para asegurar el correcto funcionamiento del mismo.

➔ *Infraestructura inalámbrica (2 Aps)*

Se efectuará la instalación física de los puntos de accesos, posteriormente, se realizarán pruebas de cobertura para asegurar la calidad del servicio y se llevarán a cabo pruebas de conexión y funcionamiento de la red inalámbrica.

84	**Entidad Local 1 (Piloto)**	**1 día**	**mar 30/11/21**	**mié 01/12/21**
85	**Armarios racks de comunicaciones**	**0,25 días**	**mar 30/11/21**	**mar 30/11/21**
86	Instalación de armario (colgado o de suelo)	2 horas	mar 30/11/21	mar 30/11/21
87	**Cortafuegos de nueva generación (1 firewall)**	**0,19 días**	**mar 30/11/21**	**mié 01/12/21**
88	Instalar cortafuegos en el armario rack	1 hora	mar 30/11/21	mié 01/12/21
89	Pruebas de conectividad	30 mins	mié 01/12/21	mié 01/12/21
90	**Infraestructura de equipos de red (1 switch)**	**0,19 días**	**mié 01/12/21**	**mié 01/12/21**
91	Instalar switch en el armario rack	1 hora	mié 01/12/21	mié 01/12/21
92	Pruebas de conectividad	30 mins	mié 01/12/21	mié 01/12/21
93	**Infraestructura inalámbrica (2 APs)**	**0,38 días**	**mié 01/12/21**	**mié 01/12/21**
94	Instalación física de los puntos de accesos	2 horas	mié 01/12/21	mié 01/12/21
95	Pruebas de cobertura inalámbrica	30 mins	mié 01/12/21	mié 01/12/21
96	Pruebas de funcionamiento	30 mins	mié 01/12/21	mié 01/12/21
97	Documentar instalación	2 horas	mié 01/12/21	mié 01/12/21

Entidad Local 2 – 91

La metodología empleada para llevar a cabo las instalaciones en los Ayuntamientos restantes será idéntica que en la instalación de la entidad local piloto.

Una vez finalizadas las instalaciones, se llevará a cabo una transferencia de conocimientos sobre el estado de la plataforma así como los conocimientos necesarios para diagnosticar los problemas que puedan darse en la misma.

98	**Entidad Local 2 - 91**	**83,75 días**	**mié 01/12/21**	**mar 29/03/22**
99	**Armarios racks de comunicaciones**	**18,75 días**	**mié 01/12/21**	**mar 28/12/21**
100	Instalación de armario (colgado o de suelo)	150 horas	mié 01/12/21	mar 28/12/21
101	**Cortafuegos de nueva generación (90 firewall)**	**16,88 días**	**mar 28/12/21**	**jue 20/01/22**
102	Instalar cortafuegos en el armario rack	90 horas	mar 28/12/21	mié 12/01/22
103	Pruebas de conectividad	45 horas	mié 12/01/22	jue 20/01/22
104	**Infraestructura de equipos de red (90 switch)**	**16,88 días**	**jue 20/01/22**	**lun 14/02/22**
105	Instalar switch en el armario rack	90 horas	jue 20/01/22	vie 04/02/22
106	Pruebas de conectividad	45 horas	vie 04/02/22	lun 14/02/22
107	**Infraestructura inalámbrica (180 APs)**	**31,25 días**	**lun 14/02/22**	**mar 29/03/22**
108	Instalación física de los puntos de accesos	160 horas	lun 14/02/22	lun 14/03/22

Id	Nombre de tarea	Duración	Comienzo	Fin
109	Pruebas de cobertura inalámbrica	45 horas	lun 14/03/22	mar 22/03/22
110	Pruebas de funcionamiento	45 horas	mar 22/03/22	mar 29/03/22
111	Documentar instalación	90 horas	lun 14/03/22	mar 29/03/22
112	Transferencia de conocimientos	1 día	mar 29/03/22	mié 30/03/22

10.1.4 Procesos de cierre

Una vez finalizado el proceso de despliegue de la infraestructura tendrá lugar una reunión de cierre de proyecto con el personal responsable de la Diputación de Cáceres con el objetivo de poder validar el proyecto.

113	**Procesos de cierre**	**0,19 días**	**mié 30/03/22**	**mié 30/03/22**
114	Reunión de cierre de proyecto	1,5 horas	mié 30/03/22	mié 30/03/22
115	Validación global del proyecto	0 días	mié 30/03/22	mié 30/03/22

11 Otra información de interés

Nuestra empresa pone a disposición de Diputación de Cáceres toda la documentación necesaria, de cualquier tipo para evidenciar toda la información que se refleja y que ampara la presente oferta.

Queremos además reflejar la ventaja que su pone una solución completamente integrada y gestionada como la que proponemos, que permite disponer de una infraestructura eficiente y escalable a todas las entidades locales con muy poco impacto ni sobrecarga sobre la estructura de recursos de Diputación de Cáceres, puesto que posee un algo grado de autonomía e independencia precisamente por ser una solución integrada y completamente gestionada.

12 Anexo I

12.1 Características Técnicas Productos Ofertados.

12.1.1 Características Técnicas Fortigate 40F

Las características técnicas de Fortinet FortiGate 40F son la siguientes:

	FORTIGATE 40F	FORTIWIFI 40F
Interfaces and Modules		
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	
Hardware Accelerated GE RJ45 Internal Ports	3	
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	
Hardware Accelerated GE RJ45 PoE/+ Ports	0	
Wireless Interface	0	Single Radio (2.4GHz/5GHz) 802.11 /a/b/g/n/ac-W2
USB Ports	1	
Console Port (RJ45)	1	
Onboard Storage	0	
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	1 Gbps	
NGFW Throughput [2, 4]	800 Mbps	
Threat Protection Throughput [2, 5]	600 Mbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps	
Firewall Latency (64 byte, UDP)	2.97 µs	
Firewall Throughput (Packet per Second)	7.5 Mpps	
Concurrent Sessions (TCP)	700,000	
New Sessions/Second (TCP)	35,000	
Firewall Policies	5,000	
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	250	
SSL-VPN Throughput	490 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55,000	
Application Control Throughput (HTTP 64K) [2]	990 Mbps	
CAPWAP Throughput (HTTP 64K)	3.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	8	
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8	
Maximum Number of FortiTokens	500	

	FORTIGATE 40F	FORTIWIFI 40F
Dimensions and Power		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160	
Weight	2.2 lbs (1 kg)	
Form Factor	Desktop	
Input Rating	12Vdc, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz	
Power Consumption (Average / Maximum)	13.4 W / 15.4 W	14.6 W / 16.6 W
Current (Maximum)	100V AC / 0.2A, 240V AC / 0.1A	
Heat Dissipation	52.55 BTU/h	56.64 BTU/h
Redundant Power Supplies		
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	
Radio Specifications		
Multiple (MU) MIMO	0	3 × 3
Maximum Wi-Fi Speeds	0	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	0	20 dBm
Antenna Gain	0	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz

12.1.2 Características Técnicas Punto de Acceso Pliego

	FORTIAP C24JE
Maximum Likelihood Demodulation (MLD)	Yes
Maximum Ratio Combining (MRC)	Yes
A-MPDU and A-MSDU Packet Aggregation	Yes
MIMO Power Save	Yes
Short Guard Interval	Yes
Wireless Monitoring Capabilities	
Rogue Scan Radio Modes	Background, Dedicated
WIPS / WIDS Radio Modes	Background, Dedicated
Packet Sniffer Mode	No
Spectrum Analyzer	No
Dimensions	
Length x Width x Height	6.69 × 4.04 × 1.08 inches 170 × 102.5 × 27.5 mm
Weight	1.3 lbs (0.6 kg)
Package (shipping) Weight	1.6 lbs (0.74 kg)
Mounting Options	Wall Plate, Optional Desk Mount FAP-MNT-WJ-20
Included Accessories	Mounting kit for Wall Plate
Environment	
Power Supply	GPI-115, GPI-130, or SP-FAP400-PA
Power Consumption (Maximum)	Depends on PoE connected
Humidity	5–90% non-condensing
Operating / Storage Temperature	32–104°F (0–40°C) / -4–158°F (-20–70°C)
Directives	Low Voltage Directive • RoHS
UL2043 Plenum Material	No
Mean Time Between Failures	>10 Years
IP Rating	—
Surge Protection Built In	—
Hit-less PoE Failover	No
Certifications	
Wi-Fi Alliance Certified	No
DFS	No
Warranty	
Limited Lifetime Warranty	Yes

* Frequency selection and power may be restricted to abide by regional regulatory compliance laws.

	FORTIAP C24JE
Maximum Likelihood Demodulation (MLD)	Yes
Maximum Ratio Combining (MRC)	Yes
A-MPDU and A-MSDU Packet Aggregation	Yes
MIMO Power Save	Yes
Short Guard Interval	Yes
Wireless Monitoring Capabilities	
Rogue Scan Radio Modes	Background, Dedicated
WIPS / WIDS Radio Modes	Background, Dedicated
Packet Sniffer Mode	No
Spectrum Analyzer	No
Dimensions	
Length x Width x Height	6.69 × 4.04 × 1.08 inches 170 × 102.5 × 27.5 mm
Weight	1.3 lbs (0.6 kg)
Package (shipping) Weight	1.6 lbs (0.74 kg)
Mounting Options	Wall Plate, Optional Desk Mount FAP-MNT-WJ-20
Included Accessories	Mounting kit for Wall Plate
Environment	
Power Supply	GPI-115, GPI-130, or SP-FAP400-PA
Power Consumption (Maximum)	Depends on PoE connected
Humidity	5–90% non-condensing
Operating / Storage Temperature	32–104°F (0–40°C) / -4–158°F (-20–70°C)
Directives	Low Voltage Directive • RoHS
UL2043 Plenum Material	No
Mean Time Between Failures	>10 Years
IP Rating	—
Surge Protection Built In	—
Hit-less PoE Failover	No
Certifications	
Wi-Fi Alliance Certified	No
DFS	No
Warranty	
Limited Lifetime Warranty	Yes

* Frequency selection and power may be restricted to abide by regional regulatory compliance laws.

12.1.3 Características Técnicas Switches de Red

	FORTISWITCH 108F	FORTISWITCH 124F
Hardware Specifications		
Total Network Interfaces	7x GE RJ45, 1x GE/POE-PD RJ45, and 2x GE SFP	24x GE RJ45 and 4× 10GE SFP+
Dedicated Management 10/100 Port	0	0
RJ-45 Serial Console Port	1	1
Form Factor	Desktop	1 RU Rack Mount
Power over Ethernet (PoE) Ports	0	0
PoE Power Budget	0	0
Mean Time Between Failures	> 10 years	> 10 years
System Specifications		
Switching Capacity (Duplex)	20 Gbps	128 Gbps
Packets Per Second (Duplex)	30 Mpps	190 Mpps
MAC Address Storage	8 K	32 K
Network Latency	4 µs	< 1µs
VLANs Supported	4 K	4 K
Link Aggregation Group Size	8	8
Total Link Aggregation Groups	8	16
Packet Buffers	512 KB	2 MB
DRAM	256 MB DDR3	512 MB DDR3
FLASH	32 MB	64 MB
ACL	768	768
Spanning Tree Instances	16	16
Dimensions		
Height x Depth x Width (inches)	1.18 × 4.72 × 7.09	1.73 × 9.06 × 12.99
Height x Depth x Width (mm)	30 × 120 × 180	44 × 230 × 330
Weight	1.36 lbs (0.62 kg)	4.48 lbs (2.03 kg)
Environment		
Power Required	100–240V AC, 50/60 Hz / PoE-PSE(a	100–240V AC, 50-60 Hz
Power Supply	12V/1A DC power adapter included, PoE-PD Built in	AC built in
Redundant Power	No	No
Power Consumption	6.2 W	24.8 W / 26.3 W
Heat Dissipation	21.142 BTU/h	89.683 BTU/h
Operating Temperature	32–113°F (0–45°C)	32–113°F (0–45°C)
Storage Temperature	-49–158°F (-40–70°C)	-4–158°F (-20–70°C)
Humidity	5–95% non-condensing	10–90% non-condensing
Air-Flow Direction	side-to-back	side-to-back

12.1.4 Características técnicas Firewalls Centro de Datos Diputación.

	FORTIGATE 200F	FORTIGATE 201F
Interfaces and Modules		
GE RJ45 Ports	16	
GE RJ45 Management / HA	1 / 1	
GE SFP Slots	8	
10 GE SFP+ FortiLink Slots (default)	2	
10 GE SFP+ Slots	2	
USB Port	1	
Console Port	1	
Onboard Storage	0	1× 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	5 Gbps	
NGFW Throughput [2, 4]	3.5 Gbps	
Threat Protection Throughput [2, 5]	3 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	27 / 27 / 11 Gbps	
Firewall Latency (64 byte, UDP)	4.78 µs	
Firewall Throughput (Packet per Second)	16.5 Mpps	
Concurrent Sessions (TCP)	3 Million	
New Sessions/Second (TCP)	280,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) [1]	13 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	16,000	
SSL-VPN Throughput	2 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	4 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	3,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	300,000	
Application Control Throughput (HTTP 64K) [2]	13 Gbps	
CAPWAP Throughput (HTTP 64K)	20 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel)	256 / 128	
Maximum Number of FortiTokens	5,000	
High Availability Configurations	Active, Active-Active, Passive, Clustering	

	FORTIGATE 200F	FORTIGATE 201F
Dimensions and Power		
Height x Width x Length (inches)	1.73 × 17.01 × 13.47	
Height x Width x Length (mm)	44 × 432 × 342	
Weight	9.92 lbs (4.5 kg)	10.14 lbs (4.6 kg)
Form Factor (supports EIA/non-EIA standards)	Ear Mount, 1 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	101.92 W / 118.90 W	104.52 W / 121.94 W
Current (Maximum)	100V / 2A, 240V / 1.2A	
Heat Dissipation	405.70 BTU/h	436.98 BTU/h
Redundant Power Supplies	Yes	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	20–90% non-condensing	
Noise Level	49.9 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6	

12.1.5 Características técnicas equipo de gestión de dispositivo Fortimanager.

FORTIMANAGER VIRTUAL APPLIANCES	FMG-VM-100-UG
Capacity	
Devices/VDOMs (Maximum)[1,3]	100 +
Storage Capacity	1 TB
GB/Day of Logs[2]	5
Chassis Management	✓
Virtual Machine	
Hypervisor Support	Up-to-date hypervisor support can be found in the release notes for each FortiManager version. Visit https://docs.fortinet.com/product/fortimanager/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiManager [version] support" → "Virtualization"
vCPU Support (Minimum / Maximum)	4 / Unlimited
Network Interface Support (Min / Max) [4]	1 / 4
Storage Support (Minimum / Maximum)	100 GB / 16 TB
Memory Support (Minimum / Maximum)	8 GB / Unlimited for 64-bit
High Availability Support	Yes

12.1.6 Características técnicas equipamiento de análisis y gestión de logs Fortianalyzer.

FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB5
Capacity	
GB/Day of Logs	+5
Storage Capacity	+3 TB
Devices/VDOMs Maximum	10,000
Chassis Management	✓
Virtual Machine	
FortiGuard Indicator of Compromise (IOC)	✓
SOC Subscription	✓
Virtual Machine	
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"
vCPU Support (Minimum / Maximum)	4 / Unlimited
Network Interface Support (Min / Max) [5]	1 / 4
Memory Support (Minimum / Maximum)	8 GB / Unlimited for 64-bit

12.1.7 Características técnicas SIEM USM Alienvault Ariolo 360.

Seguridad ARIOLO	USM ALL-IN-ONE						USM PREMIUN 360		
	AIO 25A	AIO 75A	AIO 150A	AIO Standard (Sensor Disabled)	AIO Standard (Sensor Enabled)	Remote Sensor[1]	Server	Logger	Sensor
Device Performance									
Max Assets	25	75	150	–	–	–	–		
Max Data Collection (eps)	1,000			2,500	1,000	500	–	15,000	2,500
Max Data Correlation (eps)	1,000			2,500	1,000	–	5,000	–	–
IDS Throughput (Mbps)	100			–	100	100	–	–	1,000
Hardware Specifications									
Form Factor	1U						1U		
Length x Width x Height (In)	26.6 x 17.2 x 1.7					11.3 x 17.2 x 1.7	26.6 x 17.2 x 1.7		
Weight (lb)	42					11	42		
Power Supply	2 x 700 / 750W					1 x 700/750W	2 x 700 / 750W		
Network Interfaces	6 x 1GbE					2 x 1GbE	2 x 1GbE		6 x 1GbE 2 x 10GbE (option)
CPU	2 x Intel Xeon MIN 2.4GHz 8 Cores					1x Intel Xeon MIN, 3.1 MHz 4 Cores	2 x Intel Xeon MIN 2.4 GHz 12 Cores		
Storage Capacity (TB) Compressed[4] / Uncompressed	9.0 /1.8					5.0 / 1.0	6.0 / 1.2	9.0 / 1.8	6.0 /1.2
Disk Array Configuration	RAID 10					No	RAID 10		
Memory (GB)	24					8	24		
Redundant Power Supply	Yes					No	Yes		
IPMI Interface	Yes						Yes		
Max Heat Dissipation (BTU/hr)	439.55					27.30	846.18	815.47	667.05 (6x1 option) 684.11 (2x10 option)
Max Power Consumption (kVA)	0.1288					0.1052	0.2480	0.2390	0.1955 (6x1 option) 0.2005 (2x10 option)

Remote Sensor device ships with feet for desktop deployment. Rack mount not required.
Enterprise Server ships with 2 x 1U devices. One device is the Enterprise Server and one is the Enterprise DB
Enterprise Sensor provides IDS capabilities only. It does not include data collection capabilities
5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.

12.2 Descripción de la metodología empleada proyecto Diputación Cáceres.

A continuación se detallan las metodologías que serán de aplicación en el proyecto resultante, siempre que la dirección del proyecto del cliente lo estime oportuno.

12.2.0.1 Métrica V3

La planificación, desarrollo, análisis, e implantación objeto de la presente propuesta se ajustará a lo dispuesto por Métrica V3 (Metodología de Planificación y Desarrollo de Sistemas de Información).
Métrica es una metodología de propósito generalista, promovida por el Consejo Superior de Informática (CSI, dependiente del Ministerio de Administraciones Públicas del Estado Español), como producto de su línea estratégica para la "Mejora de la calidad y la productividad en el desarrollo de software".
La principal característica de Métrica es su flexibilidad, ya que se adapta a gran variedad de sistemas y ciclos de vida. Su carácter público y abierto ha permitido su utilización en departamentos informáticos de las Administraciones Públicas y de empresas privadas.

12.2.0.2 Magerit

Como actividad imbricada en las actividades del Proyecto se prestará especial atención a aquellos aspectos relacionados con la seguridad.
Los esfuerzos afines a este objetivo estarán dirigidos según el uso de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), metodología propuesta por el Ministerio de Administraciones Públicas y elaborada por un equipo interdisciplinario del Comité Técnico de Seguridad de Información y Tratamiento Automatizado de Datos Personales del Consejo Superior de Informática.
La aplicación de MAGERIT aporta racionalidad en el conocimiento del estado de seguridad de los sistemas de información y ayuda a garantizar una adecuada cobertura en extensión y en intensidad para el dominio considerado:
Analizando los riesgos, identificando las amenazas que acechan a los distintos activos pertenecientes o relacionados con los sistemas de información en estudio y determinando su vulnerabilidad ante esas amenazas, permitiendo, de esta forma, estimar el impacto que una seguridad incorrectamente dimensionada puede ocasionar en el desarrollo, implantación y explotación de los sistemas.

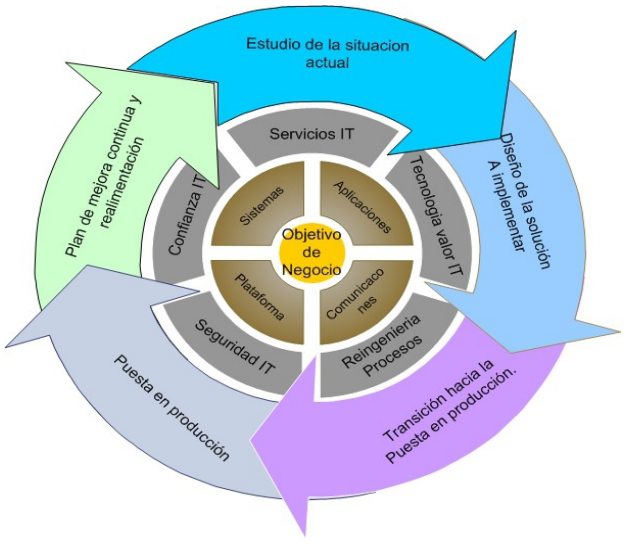
Gestionando los riesgos que soportan dichos sistemas y su entorno, seleccionando y proponiendo la implantación de las salvaguardas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.
Para poder construir proyectos específicos de seguridad, MAGERIT posee interfases básicas de enlace con Métrica. Como método de seguridad de tercera generación (es decir, adaptado a unas amenazas crecientemente intencionales que usan, cada vez, más recursos lógicos), MAGERIT permite añadir la consideración de los requerimientos de seguridad, sin interferir en las técnicas de Métrica, pero utilizándolas para identificar y documentar los procedimientos y productos de aseguramiento. Estas interfases tienen ventajas inmediatas, entre las que destacan el análisis de la seguridad de los sistemas con anterioridad a su desarrollo y el control de consistencia sostenido a lo largo de todo el ciclo de vida.

12.2.0.3 ITIL v3

En la situación actual de las infraestructuras de TI y debido a su grado de complejidad es necesario una actualización constante no sólo de los conocimientos que nos posibilitan conocer y controlar en profundidad todos los parámetros técnicos de la misma sino que además es necesario un reestudio de la forma y la filosofía con la que se realiza la gestión de todos y cada uno de los componentes esenciales de la plataforma.

Así Nace IT Infraestructure Library ITIL que ya su Versión 3 sigue recogiendo un conjunto de “mejores prácticas” en este caso enfocado al servicio desde el punto de vista de su ciclo de vida. Teniendo en cuenta el servicio como una forma fundamental de entregar valor facilitando el resultado podemos gestionar, controlar y modificar el impacto de nuestro trabajo en nuestra organización.

Así pues, asimilando en este caso el concepto de servicio y enfocándolo a su ciclo de vida, nuestros consultores certificados proponen una metodología ITIL V3.0 para enfocar el despliegue y desarrollo del presente proyecto tomando como referencia nuestro conocimiento de la infraestructura a implementar y las soluciones a adoptar.Proponemos un diagrama conceptual como el siguiente:



Donde hemos tomado como base la metodología ITIL de última generación y donde podemos destacar las fases dedicadas al control del ciclo de vida de la provisión de seguridad.

- ✔ Estudio de la situación actual, incluyendo parte de la plataforma que pudiera estar necesitando el servicio.
- ✔ Diseño de la solución a implementar o mantener, tomando como referencia las posibilidades tanto actuales como futuras en cuanto a necesidades del servicio
- ✔ Proceso de Transición hacia la puesta en producción, desde el punto de vista de la viabilidad de uso, prestaciones logradas, facilidades de implementación, asistencia al cambio ,.etc,.
- ✔ Puesta en producción y operación, control de la plataforma, operativa ordinaria, uso adecuado de recursos, estudios de disponibilidad,.
- ✔ Plan de Mejora continua, que arrope una experiencia de uso satisfactoria y que estructure un plan eficaz de reestudio de la propia plataforma para alcanzar esos objetivos de mejora continua.

12.2.0.4Plan de Calidad

La empresa Ariadnex cuenta con experiencia de las normas ISO 27001 y 20000, no en vano fue la primera certificada en ambas normas en Extremadura en el año 2013.
A partir de ahí hemos seguido conservando una fuerte implicación en la metodología de la seguridad y el control de la entrega de servicios TI.

Así toda la organización utiliza y aplica la Best Practices de ambas certificaciones en todos sus procesos.

Toda tarea a realizar se notificará en la herramienta como ticket para que todo el Centro de Datos de Ariadnex S.L., y Diputación de Cáceres puedan tener conocimiento de toda tarea futura a realizar.

Toda acción a realizar por Ariadnex S.L. deberá quedar documentada y en plena comunicación con el Diputación de Cáceres para que en futuras acciones a realizar siempre se pueda valorar todos los posibles riesgos a tener en cuenta.

Desde Ariadnex S.L. se asegura que toda gestión tendrá su procedimiento y política para asegurar la seguridad en los procesos de la organización

En Ariadnex S.L. se valora, analiza y evalúanlos riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicionalmente se da un tratamiento a los riesgos de la seguridad de la información.

En Ariadnex S.L. la mejora es nuestro sello de identidad, por ello las no conformidades conllevaran acciones correctivas y a la mejora continua el tiempo que se mantenga la relación como proveedor con Diputación de Cáceres.

12.2.0.5 Específica para este proyecto

Gestión de Problemas.

La gestión de problemas investiga la infraestructura y registros disponibles para identificar causas reales y errores potenciales en la provisión de los servicios.

La gestión de problemas garantiza que:

- Se identifiquen, documenten y rastreen los errores a largo plazo.
- Se documenten los síntomas y soluciones permanentes o temporales de los errores.
- Se realizan las peticiones de cambio pertinentes para modificar la infraestructura.
- Se prevengan nuevos incidentes
- Se elaboran informes de calidad de la infraestructura y procesos.

Gestión de Infraestructuras.

Con el objeto de ofrecer un mejor servicio al cliente se incluye un servicio de gestión de las infraestructuras, Ariadnex pone a disposición del cliente un técnico especialista con el objeto de realizar las siguientes actividades:

- Mantenimiento Preventivo, que incluye comprobación del correcto funcionamiento del suministro, recopilación y revisión de logs con el objeto de detectar comportamientos anómalos de la red.
- Gestión de Cambios, con el objeto de incorporar pequeños cambios en las configuraciones actuales de las infraestructuras.
- Gestión de Versiones, con el objeto de aplicar los últimos parches y updates fiables en los firmware y software implantados en la red.

Estas actividades serán ejecutadas In Situ por Ariadnex .

Gestión de cambios

La Gestión de Cambios coordina el proceso de modificaciones a realizar y limita el número de incidentes relacionados con las mismas. incluye:

- Evoluciones sobre la situación actual.
- Medidas Correctivas.

Las actividades incluidas en la Gestión de Cambios son:

- Registro.
- Aceptación, filtrado de las RFCs (Request for Changes).
- Clasificación, por categoría y prioridad.
- Planificación, consolidar los cambios y planificar su implantación.
- Coordinación.
- Implantación de los cambios
- Evaluación para determinar si el cambio tuvo éxito.

Gestión de versiones

Es objetivo de Gestión de Versiones garantizar la calidad del entorno de producción utilizando procedimientos formales y verificar cuándo se implementan nuevas versiones. A diferencia de Gestión de Cambios que se ocupa de la verificación, Gestión de Versiones se encarga de la implantación.
En el presente proyecto estará vinculado especialmente con la evolución o Roadmap, puesto que será el proceso que gestione y documente la implementación de las versiones aceptadas de microcódigo de los productos (Firmware)

12.3 Gestión de Incidentes

La gestión de incidentes es una actividad reactiva cuyo objetivo es asegurar que el cliente disponga del servicio lo más pronto posible. Los incidentes se registran, se clasifican y se les asignan especialistas adecuados. Posteriormente se controlan y por último se resuelven y se cierran. El estrecho contacto con los usuarios lo lleva a cabo el Centro de Servicios que sirve de oficina de entrada a las áreas especialistas.

La Gestión de Incidentes se basa en la codificación de un incidente por prioridad basado en el impacto (o grado de desviación sobre la operativa normal, en términos de número de usuarios afectados o procesos de negocio afectados) y la urgencia del incidente (o la demora aceptable para el usuarios o proceso de negocio).

En caso de no poder resolver la incidencia en primera línea de soporte en el tiempo acordado, se procede a su escalado jerárquico o funcional.

La definición de la ruta de los incidentes y su valoración en cuanto a urgencia y prioridad son responsabilidad de este grupo.

Las actividades incluidas en esta área son:

- Admisión y Registro de los incidentes.
- Clasificación (Categoría, Prioridad, Servicio, Grupo de Soporte, Tiempo Estimado, Número de referencias del incidente, estado del incidente en el proceso).
- Comparación (investigación de incidentes similares).
- Investigación y Diagnóstico por el grupo de soporte.
- Resolución y Recuperación.
- Cierre, tras la implementación de una solución satisfactoria.
- Seguimiento de progreso y monitorización. El Centro de Servicios como responsable de los incidentes ofrece feedback a los usuarios.

La Gestión de Incidentes se apoya en los siguientes servicios:

- Monitorización proactiva 7x24
- Asistencia OnSite 7x24
- Soporte Técnico
- Servicio de Reparación y Reposición
- Stock de Repuestos.

12.3.1 Monitorización proactiva 24x7x365

Ariadnex realizará una Monitorización proactiva 7x24 del estado de los equipos desde su Centro de Operaciones, siempre que la operativa funcional y el cumplimiento normativo así lo permita.

Esta actividad ejecutará un proceso d escalado inmediato al Centro de Servicios quien pondrá en marcha los procedimientos establecidos de recuperación.

También permitirá un análisis de los recursos absorbidos por cada servicio para preveer y planificar posibles necesidades de crecimiento.

Los recursos disponibles son:

- - Operadores de Gestión de Red 7x24
- - Herramienta de Gestión de Red

12.3.2 Asistencia Onsite 7X24X2

Este módulo de servicio regula la realización de servicios para todas las intervenciones de mantenimiento In-Situ en los sistemas y soluciones de red y seguridad.

El tiempo de inicio de los trabajos para la eliminación de averías por parte del técnico de servicio de Ariadnex en las dependencias del cliente, depende del tiempo de respuesta acordado para asistencia In-Situ y de la prioridad indicada al notificar la avería. Los trabajos de mantenimiento se realizan, dentro del periodo de servicio indicado en el contrato.

Este módulo de servicio incluye gastos tales como, tiempo de desplazamiento, preparación y tiempo de trabajo de mantenimiento dentro del periodo de servicio acordado.
Servicios incluidos.

- Diagnosis de una anomalía notificada por el cliente o detectada In-Situ.
- Eliminar fallos en el HW que se hayan producido como consecuencia del uso normal del mismo.
- Introducción del proceso de logística para el suministro de repuestos, acordado con el cliente.
- Sustitución de componentes defectuosos, módulos o equipos terminales sin suministro de HW.
- Incorporación en el ámbito local de parches de SW (Microcódigo) según criterio de Ariadnex .
- Realización de instalación, desmontaje y trabajos de reactivación necesarios para realizar el mantenimiento.

- Realizar las pruebas de funcionalidad y seguridad al finalizar los trabajos In-Situ.

12.3.3 Gestión de Problemas.

La gestión de problemas investiga la infraestructura y registros disponibles para identificar causas reales y errores potenciales en la provisión de los servicios.

La gestión de problemas garantiza que:

- Se identifiquen, documenten y rastreen los errores a largo plazo.
- Se documenten los síntomas y soluciones permanentes o temporales de los errores.
- Se realizan las peticiones de cambio pertinentes para modificar la infraestructura.
- Se prevengan nuevos incidentes
- Se elaboran informes de calidad de la infraestructura y procesos.