25/09/2019

A205. INFORMATICA-TELECOMUNICACIONES

SEGUNDO EJERCICIO
Tiempo máximo: 140 minutos
Pd Max: 1.000 puntos
Puntuación prueba: 30 puntos

No abra el cuadernillo hasta que se le indique y lea atentamente las instrucciones de esta portada.

- **Móviles apagados** y, al igual que los relojes, pulseras de actividad y similares, retirados de la mesa. Botellas de agua, estuches y similares pueden tenerse accesibles pero no sobre la mesa.
- Si no hay reloj en la sala, se informará por voz del tiempo que falta para la realizar la prueba: 60-30-15-10-5 y último minuto.
- Sobre la mesa exclusivamente cuadernillo de preguntas, hoja de identificación personal, DNI y bolígrafo (azul o negro). Se permite la utilización de rotuladores de color y de TIPEX® o similares.
- Utilice en su ejercicio un tipo **de letra que permita su lectura** por el Tribunal.
- Si se le ha facilitado una **hoja de identificación** con una CLAVE rellénela con su DNI, nombre, apellidos y código/denominación de la prueba.
- **Escriba la CLAVE en las hojas de respuesta** que vaya a utilizar. NO escriba su nombre, DNI o firme la prueba ya que es causa de NO CORRECCIÓN. Utilice ambas caras del folio. Numere folios, no páginas.
- La Hoja de Identificación se recogerá transcurridos los primeros minutos de la prueba.
- Si desea un **certificado de asistencia** solicítelo en el momento en el que se le realice el control de presencia.
- Las respuestas deberán ser concretas y precisas. La corrección se realizará conforme a criterios predeterminados. La valoración máxima de cada pregunta, en el caso de ser diferentes, viene señalada en el enunciado de la misma.
- Si ha finalizado antes de tiempo levante la mano para que se le recoja la hoja de respuestas. No se recogen exámenes individualmente en los últimos 3 minutos del ejercicio y si ha finalizado en este plazo permanezca en su sitio, en silencio, hasta la recogida final,
- No olvide indicar en todas sus hojas de respuestas:
  - **Código OPE (A205)**
  - **Clave** identificación
  - **Caso/supuesto. (Iniciar cada supuesto en una hoja nueva**)
  - **Número de hoja** / **total** de hojas utilizadas
- Ejemplo CABECERA:

COPE Zuzentzeko kodea / Clave de corrección	Kasua-Ustezkoa / Caso-Supuesto	Ariketaren orria - Hoja / Guztira - Total hojas prueba
A-205	OP9999ZZZZZ	1	1 / 4
A-205	OP9999ZZZZZ	1	2 / 4
A-205	OP9999ZZZZZ	2	3 / 4
A-205	OP9999ZZZZZ	2	4 / 4

SUPUESTO 1: PROYECTO DE MIGRACION DE UNA RED DE COMUNICACIONES ENRUTADA (LAYER 3) A LAYER 2 (600 puntos)

En el marco de una organización compleja como el Ayuntamiento de Vitoria-Gasteiz (en adelante AVG), tenemos una arquitectura de conmutación en varios niveles (backbone, acceso) con dos routers en HSRP para obtener la alta disponibilidad en el routing. El routing, en una organización, permite la conectividad Inter-redes.

Todas las redes del AVG son IP´s de clase C, con default gateways a un cluster de routers que actúan en modo activo-activo.

PLANTEAMIENTO DEL EJERCICIO

Debido a diversos factores tales como:

- Dispersión geográfica de los diferentes servicios que componen el AVG
- Mejora del rendimiento de los trabajadores al poder desempeñar su trabajo en varias sedes.
- Flexibilidad de las instalaciones.
- Implantación masiva de tecnología Voz Ip.
- Futuro IoT inminente

Se plantea un cambio de arquitectura de conmutación de la Red Corporativa de Datos del Ayuntamiento de Vitoria-Gasteiz de la actual a capa 3 a una más flexible a capa 2 basado en VLAN´s. Permitirá dotar a la red Corporativa del AVG de una gran flexibilidad en sus implantaciones, obteniendo las **siguientes mejoras:**

- Conexión de redes lógicas en cualquier punto de la red Corporativa.
- Dotar de calidad de servicio – QOS- a las comunicaciones.
- Redes disgregadas multisede.
- Creación y mantenimiento sencillo.
- Seguridad embebida si la arquitectura así lo contempla.

ARQUITECTURA ACTUAL

NODO-1, NODO-2 y NODO-3 son los nodos principales de una red de backbone de la cual cuelgan nodos secundarios, conformando entre todas la estructura de Red Corporativa del Ayuntamiento de Vitoria-Gasteiz.

Estos NODOS están conectados al Cluster de Routers (2) que funcionan entre si en HSRP.

Conectados a la Red Corporativa, pero ajenas a ésta (se separan por Firewalls o routers, hay conexiones a Redes Externas (proveedores, otras organizaciones…).

Por otro lado, y de manera análoga, existe una barrera perimetral de protección hacia Internet donde también tenemos conexiones VPN, SSL´s, la propia conexión a Internet…

La arquitectura actual tiene además las siguientes características:

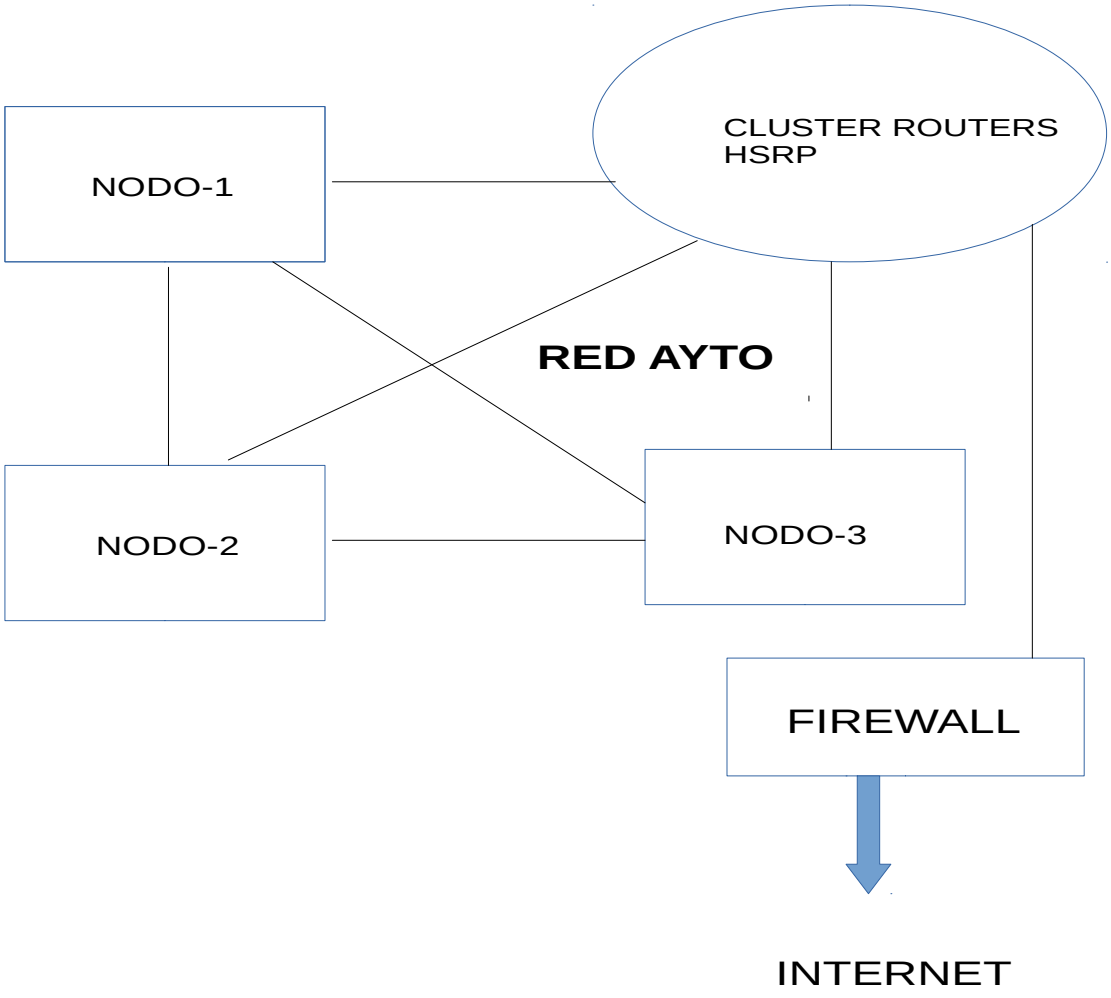
- Todos los nodos que forman parte de la red AYTO están unidos entre sí a nivel 3, incluyendo los Conmutadores de BackBone Cisco . Esto quiere decir que las redes definidas en cada nodo o rama está aislada a ese nodo o rama.
- La manera de proporcionar alta disponibilidad entre los distintos caminos que enlazan los nodos entre sí es mediante un proceso de routing dinámico OSPF.

La principal limitación de esta arquitectura es que las subredes definidas en cada uno de los nodos están confinadas a dichos nodos o ramas. No es posible extender alguna de estas subredes a más de un nodo o rama, impidiendo poder extender las subredes.

La **RED AYTO** incluye todas las subredes de trabajo de los trabajadores del Ayuntamiento de Vitoria-Gasteiz, las redes de servidores (en los CPD´s). Estas subredes se distribuyen entre 3 nodos o ramas:

- NODO-1
- NODO-2
- NODO-3

Además de las subredes internas, desde la AYTO se accede a INTERNET tal y como se muestra en la figura.

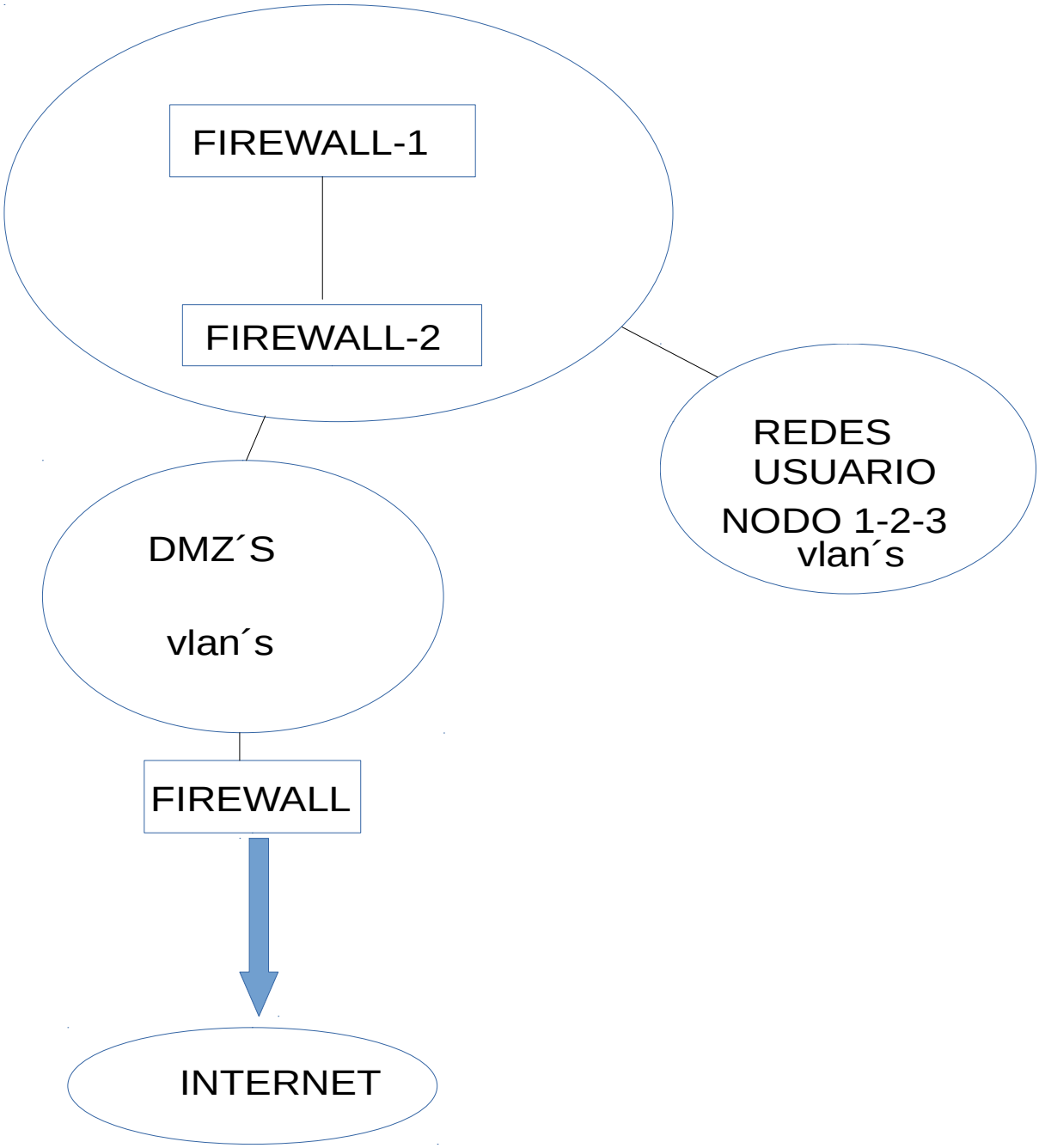


ARQUITECTURA FINAL

El nivel de routing permite la comunicación entre las distintas subredes que integran la arquitectura lógica de la la infraestructura de comunicación de datos.

La arquitectura futura se basa en la sustitución del modelo de conmutación, asociado con un cambio de los nodos de enrutamiento, pasando, de ser routers clásicos, a un cluster de Firewalls, consiguiendo , de este modo, una seguridad nativa.

Con ello se pretende que el cambio de conmutación de Nivel 3 a 2 vaya asociado, a un modelo de routing seguro. En este sentido, se deben tener en cuenta los accesos Inter.- VLAN´s.



- Los NODOS: 1, 2 y 3 basados en Switches Cisco ya no se comunicarán entre ellos a nivel 3. Lo harán a nivel 2 y a nivel de VLANs, que serán y estarán accesibles desde todos los nodos de la red troncal

- Se permitirá, si así se desea, que se puedan extender sin problemas las subredes del CPD de producción en el CPD de backup y viceversa.

- Las puertas de enlace de todas las subredes internas de la red AYTO serán la IP virtual de un cluster de FW´s (s firewalls)

- Desaparece el routing dinámico OSPF. La alta disponibilidad entre los enlaces que unen los distintos nodos de la red AYTO se hará mediante enlaces de fibra redundantes (recálculos de spanning tree).

Objeto del ejercicio

- Plantear un proyecto de migración por fases. Puntuación: 420 puntos
    - Planteamiento general de la Arquitectura. Futura: Gráfico de la arquitectura final
    - Proyecto de migración.
        - Reorganización y Definición de VLANS..
        - Elección de switches y otros elementos del universo Layer 2..
        - Configuración de las VLAN´s. Criterios a seguir.
        - Fases de configuración de las máquinas: paso a paso.
    - Migración de las redes: físicas a VLAN: paso a paso. Hacer referencia a los comandos más importantes para ello, (sin detalle).
    - Somero planteamiento del QoS: como y donde se implementaría
    - Arquitectura de routing;: donde y como se hace el routing interVLAN y hacia Internet, seguridad unificada, y las implantaciones necesarias para conseguirlo.

- Señalar que aporta esta arquitectura con respecto a la de Layer 3. Pros y contras. Motivarlo y poner ejemplos concretos. Puntuación: 90 puntos

- Señalar que problemas que pueden aflorar en una red multicamino (enlaces redundantes entres sedes) y las soluciones a implementar en cada caso. Puntuación: 90 puntos

SUPUESTO 2: DISEÑO DE UNA SOLUCIÓN DE COMUNICACIONES POR RADIO ENLACE. (200 puntos)

Situación de partida

La Depuradora de Araka, dependiente de AMVISA (Aguas Municipales de Vitoria), y sita en el "monte de Araka", no dispone de una conexión de datos de calidad a la red municipal . En la actualidad se "sale del paso" con conexiones 3G / 4G que resultan lentas y caras para los fines previstos. La Depuradora se halla ubicada en terreno militar y a un cota de 650 metros de altura.

Se plantea la necesidad de , al tratarse de una instalación estratégica, conectar dicha Depuradora a la red municipal de comunicaciones de datos en las condiciones que dicha catalogación exigen en cuestiones tales como integridad, disponibilidad..

Por su situación elevada y a 4 Kilómetros en línea recta del casco urbano, la posibilidad de echar fibra óptica hasta sus instalaciones es poco posible técnicamente y muy cara.

Por ello, se plantean alternativas de conectividad, que cumplan con una serie de requisitos técnicos, económicos y de calidad.

La Depuradora de Araka, alberga una serie de servicios que necesitan el uso de soluciones tecnológicas que, a su vez, necesitan comunicarse con la Red Corporativa Municipal , con la cual mantiene una serie de servicios activos:

- Telefonía Ip, servida por la centra de VoIp municipal sita en la Red Corporativa
- Aplicaciones municipales, que trabajan contra servidores centralizados en la Red Corporativa
- Conexión Centralizada a Internet para los usuarios corporativos.
- Conexión independiente a Internet del propio edificio de Depuradora para ciertos sensores que conectan con empresas y organismos externos de control.
- Transmisión desde diversos sensores a un SCADA sito en las oficinas centrales de AMVISA, en la calle Puerto Rico, conectadas a red municipal).

PLANO GENERAL – ARAKA – CASCO URBANO DE VITORIA-GASTEIZ. En el Plano de Vitoria con Araka a la vista se aprecia la distancia de la Depuradora al Casco Urbano de Gasteiz y, por lo tanto, al entramado de fibra óptica que conforma la Red Corporativa uniendo edificios de servicios municipales. **(anexo I)**

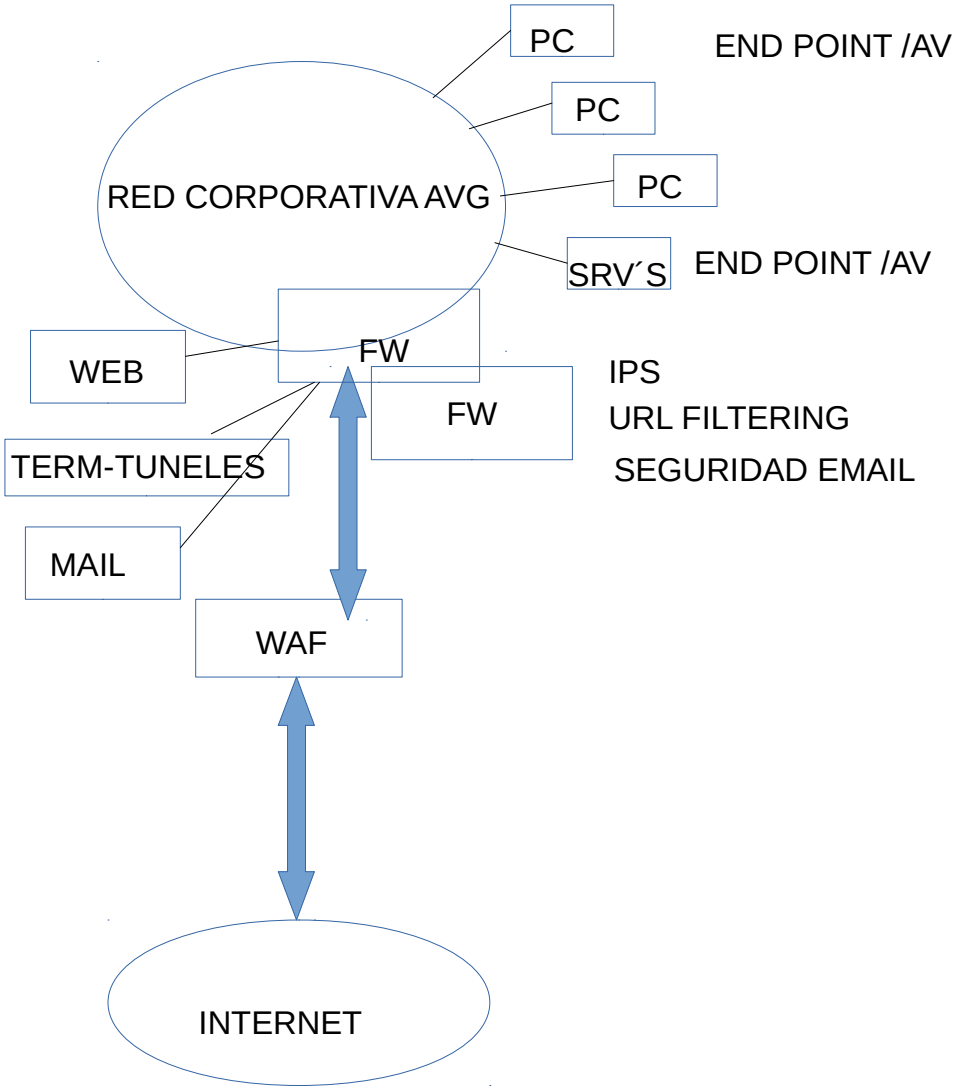
PLANO ESPECIFICO- GASTEIZ – EDIFICIOS – FIBRA. En este Plano de Vitoria se aprecian diferentes edificios municipales (propiedad municipal y susceptibles de ser usados para montar infraestructuras). Las líneas amarillas marcan los ramales de fibra óptica que unen dichos edificios y conforman la red de datos municipal. **(anexo II)**

Objeto del ejercicio

- Motivación de uso de la tecnología de radio enlace sobre otras tecnologías (20 puntos)
- Uso de banda licenciada o libre: motivación. Cuidados especiales a tener en cuenta en este apartado. (14 puntos)
- Seguridad aplicable en la transmisión de los datos (si procede). (20 puntos)
- Diseño físico de la solución. Montaje, antenas, alimentación, transceivers, conmutación. (50 puntos)
- Diseño lógico: teniendo en cuenta que TODOS los servicios de datos son servidos desde la Red de Comunicaciones Corporativa del Ayuntamiento de Vitoria-Gasteiz, en la cual se hallan las salidas a Internet Corporativo, los servidores de Aplicaciones municipales y el SCADA. En el diseño lógico se incluirá QoS si se considera necesario (52 puntos)
- Integración en la red municipal. Como se llevaría a cabo? Pasos, aspectos a tener en cuenta, problemática, soluciones (30 puntos)
- Pruebas a realizar. Relación sin entrar en detalle. (8 puntos)
- Documentación a elaborar. Relación sin entrar en detalle. (6 puntos)

SUPUESTO 3: ARQUITECTURA DE UNA VERTICAL DE SEGURIDAD HOMOGENEA. (200 puntos)

En el marco de una organización compleja , como el Ayuntamiento de Vitoria-Gasteiz (en adelante AVG), se han detectado, tras una auditoría de seguridad, diversos posibles vectores de ciber ataque: correo electrónico, dispositivos de almacenamiento externo,, Web, los puestos de trabajo (usuario final o estaciones de trabajo-servidores) y un terminador de túneles IPSEC, que pueden poner en peligro la integridad de la organización



.

Esta organización dispone de diversos elementos de protección: firewalls, anti virus, sondas, IPS… que se han ido integrando en la estructura de seguridad a lo largo del tiempo.

La información que obtenemos de todos estos elementos es grande y variada, aportando los datos necesarios para llevar a cabo las modificaciones necesarias para cubrir las necesidades, en lo que a seguridad se refiere, del AVG:

En este marco, la necesidad de tener una gestión integrada homogénea de todos los dispositivos, herramientas o sistemas de seguridad se hace imprescindible para una adecuada resolución de problemas y una prevención proactiva adecuada.

La diversidad de productos de seguridad, formatos de datos, protocolos , así como el hecho de que dichos datos sean , en ocasiones, referentes a productos concretos con fabricantes distintos, hace que la disparidad de dichos datos haga difícil un tratamiento homogéneo, y, por lo tanto, la obtención de conclusiones del cruce de dichos datos para la toma de decisiones que nos permitan un rendimiento óptimo (proactivo incluso).

Con la falta de coherencia y de homogeneidad en los productos, la arquitectura, los datos, y por lo tanto de los resultados de la conjunción de todos los datos extraíbles de estos dispositivos (hard y soft) no son comparables o inteligibles entre ellos.

En aras de una mayor efectividad y simplificación de los procesos de seguridad interna y periférica se pretende construir una arquitectura de seguridad sólida y homogénea que nos permita tener un punto central de control de la seguridad de la organización (tipo SIEM).

Para ello, se pretende unificar en criterios, productos y formatos de datos todas las protecciones de la Organización para todos y cada uno de los vectores posibles de ataque y en toda la vertical:

- La protección del puesto de trabajo: sea con una herramienta de end point, anti virus, ambas combinadas etc… Seguridad física – USB´s..
- Seguridad perimetral: con todo lo que puede conllevar: Sand Box, IPS, IDS…
- WAF (si se estima necesario).
- Seguridad Correo Electrónico: Alternativas?
- …

Objeto del ejercicio

- Plantear una arquitectura de seguridad unificada y homogénea teniendo en cuenta, como mínimo, los vectores indicados. Puntuación: 100 puntos,
- Definir las interrelaciones de datos entre cada elemento de la arquitectura. Puntuación: 30 puntos
- Plantear las herramientas de gestión, control, logging y monitorización. Poner ejemplo concreto de herramienta/s. Puntuación: 20 puntos,
- ¿Como la homogeneidad de tecnologías/productos ayudaría a la proactividad? Poner un ejemplo concreto. Puntuación: 20 puntos,
- En cada elemento, explicar muy someramente las amenazas (sin llegar a un nivel técnico profundo del tipo de amenaza) de las que protegería. Puntuación: 20 puntos,
- Herramientas o tecnologías que aporten un valor añadido: uso de tokens, doble factor de autenticación u otros. En que punto y para qué? Puntuación: 10 puntos.