11/04/2019

COD: **A110**

A110 TELECOMUNICACIONES

PRIMER EJERCICIO
SEGUNDA PRUEBA

Tiempo máximo: 120 minutos
Preguntas: 120.

MODELO / EREDUA:	**A**

- No abra el cuadernillo hasta que se le indique.
- Marque en la hoja de respuestas el modelo que le haya correspondido.
- A la finalización de la prueba recoja este cuadernillo, la copia amarilla de su hoja de respuestas y la hoja de instrucciones.
- Recuerde:
  - Aciertos: 1,00
  - Errores, nulos, dobles o blancos: no descuentan.
- La ausencia de marca o la marca incorrecta en el modelo invalida la prueba.
- No se entregarán nuevas hojas de respuesta en los últimos 5 minutos del ejercicio.
- Cuando finalice levante la mano y el personal de la organización recogerá la hoja de color blanco
- No se recogen exámenes individualmente en los últimos 3 minutos del ejercicio. Si ha finalizado permanezca en su sitio en silencio hasta la recogida final.

Gracias por su colaboración

1.- ELIJA la respuesta correcta: un equipo conectado a varias redes LAN tiene…
a) una dirección MAC estática, asignada al equipo por el fabricante
b) una dirección MAC estática por cada interface, asignada por el fabricante de la interface
c) una dirección MAC dinámica, que obtiene el equipo el conectarse
d) una dirección MAC dinámica por cada interface, que se obtiene al activar la interface

2.- ELIJA la respuesta correcta: tecnología de conexión que proporciona mejor calidad de servicio (QoS) en una red de área amplia (WAN)
a) líneas dedicadas
b) conmutación de circuitos
c) conmutación de paquetes
d) conmutación de celdas (ATM)

3.- La familia de protocolos de Internet incluye el protocolo… (Señale la opción FALSA)
a) ARP
b) FTAM
c) POP
d) SMTP

4.- ¿Cuál es el retardo máximo que se considera aceptable en VoIP?
a) 50 milisegundos
b) 150 milisegundos
c) 200 milisegundos
d) 500 milisegundos

5.- ELIJA el protocolo de VoIP más antiguo:
a) Skype
b) SIP de IETF
c) H.323 de la ITU-T
d) SCCP de Cisco

6.- ELIJA el sistema de VoIP no propietario (Open Source):
a) Alcatel-Lucent
b) Cisco
c) Asterisk
d) Avaya

7.- VPN-IPSEC. ELIJA la capa del modelo OSI en la que actúan los protocolos IPsec:
a) Capa de red (nivel 3)
b) Capa de transporte (nivel 4)
c) Capa de sesión (nivel 5)
d) Capa de aplicación (nivel 7)

8.- El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, obliga a:
a) La banca electrónica
b) Las Administraciones públicas
c) El comercio electrónico
d) A todas las transacciones electrónicas donde haya necesidad de garantizar la identidad de los participantes

9.- Para crear una SA (Security Association) de tipo dinámico entre dos equipos con Junos OS sólo es necesario:
a) Configurar IKE (Internet Key Exchange)
b) Definir el algoritmo a utilizar (MD-5, SHA)
c) Proporcionar las claves que se van a utilizar en los equipos
d) Fijar el SPI (Security Parameter Index) de la SA

10.- ELIJA la capa del modelo ISO en la que se establecen los túneles SSL (Secure Shockets Layer):
a) Capa de red (nivel 3)
b) Capa de transporte (nivel 4)
c) Capa de sesión (nivel 5)
d) Capa de aplicación (nivel 7)

11.- El protocolo SSL fue desarrollado originalmente por:
a) ARPANET
b) IBM para Internet Explorer
c) Netscape para su navegador web
d) Digital Equipment Corporation para Altavista

12.- En una conexión SSL con un servidor web (HTTPS), la información llega al navegador cifrada con claves de criptografía:
a) Simétrica
b) Asimétrica RSA
c) Asimétrica Diffie-Hellman
d) Asimétrica PSK

13.- ELIJA la respuesta correcta sobre las redes VLAN…
a) Utilizan habitualmente el protocolo de etiquetado IEEE 802.1.Q
b) Introducen un ID (identificador) en las cabeceras IP.
c) Evitan que se produzcan colisiones en un segmento de Ethernet de topología en bus
d) Sólo se pueden configurar de forma estática, asignando equipos por la dirección MAC

14.- ELIJA la respuesta correcta sobre las redes VPN
a) No existen variantes de VPN para entornos móviles (celulares, WiFi)
b) Las redes VPN se basan en conexiones punto a punto mediante túneles
c) Las conexiones VPN son siempre de nivel 3 (red), asignando al equipo una IP de la red a la que se conecta
d) El modelo de conexión a una VPN no ofrece confidencialidad, un atacante puede ver los datos transmitidos

15.- ELIJA el protocolo al que NO se puede aplicar SSL 3.0:
a) TCP
b) UDP
c) HTTP
d) SNMP

16.- SWITCHING. ELIJA la respuesta correcta: el protocolo “spanning tree” (STP) tiene como objetivo…
a) Balancear el tráfico
b) Controlar los errores en las tramas de datos
c) Evitar bucles
d) Eliminar los paquetes duplicados

17.- ELIJA la respuesta correcta: el protocolo de alta disponibilidad VRRP (Virtual Router Redundancy Protocol):
a) Es un protocolo de encaminamiento de tráfico de nivel 3 (routing)
b) Se puede implementar en un solo router físico
c) Es un protocolo propietario de CISCO
d) Utiliza multicast

18.- ELIJA la respuesta correcta sobre el protocolo PVST:
a) Se utiliza para hacer túneles punto a punto entre VLANs
b) Es un protocolo propietario de Cisco para sus switches
c) Es posterior al protocolo STP de IEEE
d) Es un protocolo de nivel 3 (transporte)

19.- El estándar para la tecnología de red SPB (Shortest Path Bridging) se denomina:
a) 802.1AQ
b) 802.1X
c) 802.1D
d) 802.1W

20.- Para identificar los equipos conectados a sus puertos, los switches utilizan:
a) El nombre de host del equipo conectado
b) La dirección IPv4 del equipo conectado
c) La dirección MAC del equipo conectado
d) La dirección IPv6 del equipo conectado

21.- El término PoE se aplica a:
a) Un sistema de cifrado de nivel de red
b) Un sistema de alimentación eléctrica sobre cable UTP
c) Un sistema de cifrado de nivel de transporte
d) Un protocolo de coordinación entre switches

22.- Para definir agregaciones de puertos en un switch se utiliza el protocolo:
a) LACP
b) HTTP
c) VRRP
d) STP

23.- De los siguientes cual NO es un método de direccionamiento de tramas:
a) Store-and-Forward
b) Cut-Through
c) Adaptative Cut-Through
d) Pass-Through

24.- Norma del IEEE para el control de acceso a red (NAC) basado en puertos:
a) 802.1D
b) 802.1X
c) 802.1Q
d) 802.1AQ

25.- Significado de las siglas DNS:
a) Dynamic Name Server
b) Data Name Server
c) Domain Name Server
d) Domain Name Storage

26.- Puerto por defecto utilizado por los servidores DNS:
a) 7
b) 22
c) 53
d) 8080

27.- Para que la modificación del valor de una entrada en el DNS tenga efecto es necesario:
a) Reiniciar el servicio DNS
b) Incrementar el valor de TTL
c) Incrementar el valor del número de serie del SOA
d) No es necesario hacer nada, basta con modificar el valor de la entrada para que este se propague

28.- En el nombre completo de dominio para un host (FQDN):
a) El nombre del host va al final
b) El valor del TLD va al final
c) El nombre del dominio va al final
d) Un número aleatorio va al final

29.- En un nombre completo de dominio (FQDN), cada elemento se separa con:
a) Un espacio en blanco
b) Una coma (,)
c) Un punto (.)
d) Un guión (-)

30.- Cuando un cliente hace una petición DHCP, la respuesta la proporciona:
a) El servidor con la IP más baja
b) El primer servidor que responda
c) El servidor que haya asignado menos direcciones
d) Siempre del mismo servidor

31.- DHCP utiliza el protocolo:
a) TCP
b) UDP
c) STP
d) RIP

32.- En una red local pueden realizar peticiones DHCP:
a) Cualquier equipo que se conecte a dicha red
b) Sólo los ordenadores de usuarios finales
c) Sólo los servidores
d) Sólo las impresoras

33.- Cual de las siguientes no es una versión de SNMP:
a) SNMPv1
b) SNMPv1c
c) SNMPv2c
d) SNMPv3

34.- Elija la correcta: el protocolo SNMP opera sobre la capa ISO:
a) Capa de red (nivel 3)
b) Capa de transporte (nivel 4)
c) Capa de sesión (nivel 5)
d) Capa de aplicación (nivel 7)

35.- El acrónimo MIB corresponde a:
a) Multi Internet Broadcast
b) Main Information Base
c) Management Information Base
d) Microsoft Internet Browser

36.- Elija la respuesta correcta:
a) Un cortafuegos puede proteger de las amenazas a las que está sometido por ataques internos
b) Un cortafuegos protege contra los ataques de ingeniería social.
c) Un cortafuegos protege sobre fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido.
d) Un cortafuegos protege aquellos ataques cuyo tráfico pasa a través de él.

37.- Los cortafuegos de tercera generación:
a) Actúan sobre la capa de aplicación del modelo OSI.
b) Sólo permiten filtrado de paquetes.
c) Sólo permiten sustituir al software antivirus.
d) Sólo permiten definir VPN.

38.- El primer documento publicado sobre tecnología firewall procede de:
a) Un grupo de la NSA
b) Un equipo de ingenieros de DEC (Digital Equipment Corporation)
c) Un equipo de investigadores de IBM
d) Se trata de un documento anónimo

39.- La topología de red más segura, en lo que respecta a fallos en alguno de los enlaces, es:
a) Topología de red en bus
b) Topología de red mallada
c) Topología de red en estrella
d) Topología de red en anillo

40.- El término “honeypot” en redes informáticas se aplica a:
a) Las impresoras en red
b) Los equipos accesibles en la red que actúan como señuelos
c) Los sistemas incluidos en la DMZ
d) Los componentes de los firewalls

41.- La DMZ está relacionada con:
a) Sistemas antivirus
b) Sistemas cortafuegos
c) Switches de la red LAN
d) Router de acceso a Internet

42.- En la DMZ de una red corporativa es donde se ubican habitualmente:
a) Las impresoras de red
b) Los equipos no protegidos por el firewall
c) Los equipos de los usuarios
d) Los servidores de correo

43.- En el estándar establecido para el cableado estructurado UTP Cat-6 por TIA/EIA, la máxima distancia recomendada para el cableado horizontal entre el panel de conexiones y la toma de pared es de
a) 70 metros
b) 80 metros
c) 90 metros
d) 100 metros

44.- Las ópticas SFP para conexiones 1000Base-LX de hasta 10 Km utilizan
a) Fibra óptica multimodo
    a. Fibra óptica monomodo en primera ventana (850 nm)
b) Fibra óptica monomodo en segunda ventana (1310 nm)
c) Fibra óptica monomodo en tercera ventana (1550 nm)

45.- Los transceptores de tipo SFP para fibra óptica, utilizados en los equipos de comunicaciones, emplean conectores…
a) FC
b) ST
c) LC
d) SC

46.- Los equipos WiFi cumplen con la normativa:
a) IEEE 802.1
b) IEEE 802.11
c) IEEE 802.2
d) IEEE 802.3

47.- Los sistemas WiFi utilizan la banda de:
a) 2 GHz
b) 3 GHz
c) 4 GHz
d) 5 GHz

48.- Para poner en marcha un radioenlace es necesario obtener un permiso de la Secretaría de Estado de Avance Digital en el que NO es necesario detallar uno de los siguientes parámetros:
a) Potencia transmitida
b) Ancho de banda
c) Banda de frecuencia
d) Longitud del vano

49.- La principal dificultad para los radioenlaces de microondas es
a) La conservación y el mantenimiento son muy costosos
b) La necesidad de visibilidad directa entre antenas (línea de vista)
c) Las regulaciones legales, sometidas a revisiones periódicas
d) Las condiciones atmosféricas, que pueden causar desvanecimientos intensos y desviaciones del haz

50.- La norma ISO 17799 sobre “Seguridad y Auditoría Informática”
a) Es una norma tecnológica
b) Considera la “Seguridad” como una competencia de la alta gerencia de una organización
c) No contempla la realización periódica de análisis de riesgos
d) No incluye una auditoría legal sobre el cumplimiento del Reglamento General de Protección de Datos

51.- Señale el enunciado FALSO sobre “hacking ético”
a) Pone a prueba la seguridad de los sistemas de protección perimetral de una empresa
b) Es totalmente altruista, se trata de una contribución para mejorar la seguridad en Internet
c) Bordea la legalidad si se hace sin consentimiento de la empresa
d) Analiza tanto la red interna como la DMZ

52.- Señale el enunciado FALSO sobre la norma ISO 17799 de “Seguridad y Auditoría Informática”:
a) Recoge la relación de controles a aplicar, pero no es certificable
b) Realiza un análisis del “control de accesos” a los equipos TIC
c) Incluye la realización de una auditoría forense
d) Analiza la gestión de “continuidad del negocio”

53.- Según la LSSI, el prestador de servicios NO está obligado a poner a disposición de los destinatarios del servicio por medios electrónico, de forma permanente, fácil, directa y gratuita, la siguiente información
a) Los datos de su inscripción en el Registro Mercantil
b) La dirección de todos sus establecimientos permanentes en España
c) Su dirección de correo electrónico
d) El NIF (Número de Identificación Fiscal) que le corresponda

54.- Entre los siguientes proveedores de servicios de intermediación, NO se aplica la LSSI a
a) Los prestadores de servicios de correo electrónico
b) Los proveedores de servicios de acceso a Internet
c) Los notarios en el ejercicio de sus funciones públicas
d) Los operadores de redes de telecomunicaciones

55.- El concepto de "smart city" NO contempla entre sus objetivos
a) La comunicación fluida de los actores entre sí: colectividades, ciudadanos, empresas, instituciones;
b) La consecución de metas especificas en materia de reducción de residuos
c) El uso compartido de bienes y servicios
d) Las cuestiones ambientales y las restricciones energéticas

56.- El concepto de IOT (Internet de las Cosas) procede del MIT, y de las investigaciones realizadas sobre
a) Redes inalámbricas de Area Personal (Bluetooth)
b) Conexión a internet de sensores en dispositivos
c) Sistemas de Identificación por Radiofrecuencia (RFID)
d) Aplicaciones para automóviles conectados

57.- Entidad que expide certificado digital de ciudadano SOLO en tarjeta física
a) FNMT
b) IZENPE (Administración vasca)
c) Camerfirma (Cámaras de Comercio)
d) ACCV (Generalitat Valenciana)

58.- Respecto de la arquitectura de switches tradicional, los switches Nexus.. (señale el enunciado FALSO):
a) Están concebidos como switches de Data Center
b) Permiten implementar VLANs
c) Permiten interfaces de fibra
d) Su uso óptimo es como switches de redes de campus

59.- Los switches NEXUS serie 9000.. (señale el enunciado FALSO):
a) permiten utilizar interfaz de línea de comando y CLI scripting
b) permiten tarjetas de puertos de hasta 40GbE
c) permite administrar SAN y LAN con la misma herramienta DataCenter Network Management
d) ejecutan sistema operativo NX-OS

60.- ¿Qué permite la secuencia de comandos siguiente?:

```
Router> enable
Router# configure terminal
Router(config)# interface s0/0/0
Router(config)# ip route 10.50.20.0 255.255.255.0 192.168.200.1
```

a) Configurar una ruta dinámica
b) Configurar una ruta estática
c) Conocer la ruta estática
d) Todas las anteriores son correctas

61.- En relación con los usos del routing estático.. (señale el enunciado FALSO):
a) Causa menor carga de CPU del router que el routing dinámico
b) Genera menos tráfico hacia otros routers
c) Puede configurarse automáticamente
d) Se puede utilizar como failsafe backup para el caso de fallo del routing dinámico

62.- Es una característica de HRRP:
a) multicast en: 224.0.0.18 – IP 112
b) Propietaria de Cisco
c) 1 router maestro y 1 o más routers de backup
d) se puede utilizar la IP real (la dirección IP más alta de la interfaz)

63.- Es una característica de VRRP:
a) 1 router maestro y 1 o más routers de backup
b) permite habilitar preempt manualmente
c) VRRP es un protocolo de routing
d) multicast en: 224.0.0.2 (ver1), multicast en: 224.0.0.102 (ver2). Ambas versiones utilizan el puerto UDP 1985

64.- RADIUS... (señale el enunciado FALSO):
a) se utiliza en esquema cliente-servidor
b) ofrece un mecanismo de autenticación de usuarios para acceder a un recurso compartido
c) requiere LDAP
d) Se pueden utilizar directorios activos o bien bases de datos que pertenezcan a aplicaciones transversales

65.- RADIUS… (Señale el enunciado FALSO):
a) encripta todos los atributos
b) garantiza el acceso restringido a las redes inalámbricas
c) ofrece un mecanismo de autenticación de usuarios para acceder a un recurso compartido
d) El período de validez de las claves está limitado en el tiempo

66.- Un servidor RADIUS se puede implementar sobre… (Señale el enunciado FALSO):
a) ciertos routers
b) un servidor
c) un Access Point
d) un firewall

67.- INTERMAPPER es… (Señale el enunciado FALSO):
a) un software de monitorización de red
b) un sistema de autenticación
c) no permite intervenir en la configuración de los dispositivos de red
d) una herramienta que permite disponer de un mapa visual de la red

68.- Funcionalidades de INTERMAPPER... (señale el enunciado FALSO):
a) reporting y datos históricos
b) interfaz visual
c) intervalos fijos de polling a los dispositivos
d) autodiscovery para los dispositivos IP

69.- Cuál de los siguientes productos de NAGIOS está especialmente diseñado para analizar, recolectar y almacenar datos de tráfico basados en especificaciones personalizadas:
a) Nagios XI
b) Nagios Log Server
c) Nagios Network Analyzer
d) Nagios Fusion

70.- Usos de NAGIOS.. (señale el enunciado FALSO):
a) Gestión de servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP).
b) Monitorización remota, a través de túneles SSL cifrados o SSH.
c) Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
d) Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.

71.- Nagios permite monitorizar el tráfico para el/los siguiente/s protocolo/s:
a) POP3, SMTP y HTTP
b) HTTPS
c) SNMP
d) Todos los anteriores

72.- SYSLOG-NG.. (señale el enunciado FALSO):
a) Es un recolector de mensajes de log
b) Permite transferir logs a un servidor central de logs
c) Permite almacenar logs en archivos o en diversas bases de datos
d) Gestiona y analiza eventos

73.- En cuanto a los mensajes enviados por SYSLOG:
a) Su longitud mínima es de 512 bytes
b) Se componen de Fecha, Prioridad, Texto
c) No hay límite de longitud para el mensaje
d) Se componen de Prioridad, Cabecera, Texto

74.- TCPDUMP... (señale el enunciado FALSO):
a) tcpdump para Windows hace uso de la biblioteca libpcap
b) En UNIX y otros sistemas operativos es necesario tener privilegios de administrador (root) para utilizar tcpdump
c) Host, net y port son filtros de tcpdump.
d) Por defecto tcpdump sólo captura los primeros 68 bytes

75.- TCPDUMP permite... (señale el enunciado FALSO):
a) capturar el tráfico entrante y saliente para una interfaz dada
b) capturar el tráfico saliente hacia una subred
c) capturar una sesión HTTP completa ensamblando los paquetes de la sesión
d) sacar el tráfico capturado a un archivo de salida

76.- Wireshark... (señale el enunciado FALSO):
a) permite visualizar el protocolo al que pertenece el paquete
b) es un IDS
c) permite examinar el contenido de los paquetes
d) permite leer datos de una captura previa almacenados en un archivo

77.- La tecnología Sandblast de Checkpoint permite detectar y eliminar malware... (señale el enunciado FALSO):
a) mediante la monitorización de la actividad de la CPU
b) mediante la emulación en el ámbito del sistema operativo
c) entregando la versión original y la versión segura del archivo
d) de archivos de Office y PDF

78.- SmartEvent permite... (señale el enunciado FALSO):
a) crear informes personalizados
b) realizar análisis forense
c) acceder desde el evento a la regla de la política que lo produce
d) acceder desde el evento a desinfectar el host

79.- El bundle Next Generation Threat Prevention (NGTP) de Checkpoint incluye... (señale el enunciado FALSO):
a) SandBlast Threat Emulation
b) URL Filtering
c) IPS
d) Antivirus

80.- El blade software para realizar URL filtering de Checkpoint... (señale el enunciado FALSO):
a) escanea y securiza el tráfico encriptado SSL/TLS que atraviesa el gateway
b) consulta una base de datos dinámica para permitir, bloquear o limitar el acceso al sitio web en tiempo real
c) permite configurar el tráfico a excluir de la inspección
d) permite definir excepciones a la inspección SSL/TLS

81.- El producto sandbox de Fortinet (FortiSandbox) puede implementarse:
a) sobre una máquina virtual
b) como un appliance
c) en cloud público
d) todas las anteriores

82.- FortiMail... (señale el enunciado FALSO):
a) abre el archivo sospechoso en entorno controlado
b) previene ataques dirigidos
c) previene ataques por volumen
d) dispone de antispam y antimalware

83.- ¿Cuál de los productos utiliza el concepto "Security Rating Score"?:
a) SmartEvent
b) FortiAnalyzer
c) Ambos
d) Ninguno

84.- El gestor de eventos SmartEvent de Checkpoint ofrece las siguientes ventajas... (señale el enunciado FALSO):
a) filtrado de eventos por IP, protocolo y fecha
b) correlación de eventos
c) acceso a documentación para resolver una infección
d) visualización del panel de control desde dispositivos móviles

85.- ¿Cómo se configura e implementa URL Filtering en Checkpoint?: (Señale el enunciado FALSO):
a) Se activa con un clic en cualquier Security Gateway
b) Se integra de forma transparente con SmartEvent
c) Fuerza a la inspección SSL/TLS del tráfico HTTPS
d) Permite configurar manualmente listas blancas y negras

86.- SmatEvent proporciona información sobre... (señale el enunciado FALSO):
a) resultado de la acción correctiva que ha realizado
b) localización física del origen del ataque (país)
c) usuario afectado
d) nombre del ataque

87.- En SmartEvent los ataques detectados pueden resolverse de las siguientes maneras... (señale el enunciado FALSO):
a) resolución automática del problema que causa el evento
b) acceso a la documentación de resolución ThreatWiki
c) modificación de una regla de la política para evitar el ataque
d) reconfiguración de los parámetros de un blade

88.- Una empresa con una sola sede dispone de FortiGate implantado. Se desea incorporar FortiSandbox. ¿Cuál es la modalidad de implementación más adecuada de FortiSandbox?:
a) Independiente
b) FortiGate integrado
c) FortiGate distribuido integrado
d) Todas las anteriores son igualmente adecuadas

89.-¿Cuál de las siguientes utilities pueden configurarse en alta disponibilidad?
a) FortiAnalyzer
b) FortiMail
c) FortiGate
d) Todas las anteriores

90.- SmartEvent respecto de los LOG tradicionales tiene como ventajas... (señale el enunciado FALSO):
a) filtrado de eventos por diversos criterios
b) panel de control visual configurable
c) navegación hasta la regla asociada al evento
d) creación y planificación de informes personalizados

91.- El blade de Antispam & E-mail security de Checkpoint tiene las siguientes funcionalidades... (señale el enunciado FALSO):
a) Protección IPS del email
b) Apertura del archivo infectado en entorno emulado
c) Protección zero-hour
d) Antispam por reputación IP

92.- Un radioenlace se compone de diversos elementos... (señale el enunciado FALSO):
a) Antenas
b) Estaciones terminales
c) Gateway VoIP
d) Estaciones repetidoras intermedias

93.- ¿Qué técnicas y sistemas garantizan la alta disponibilidad y confiabilidad de un radioenlace? Señale el enunciado FALSO:
a) Redundancia de equipos frente a averías
b) Técnicas de diversidad frente a desvanecimientos
c) Transmisión de señales auxiliares de telemando
d) Estaciones repetidoras intermedias

94.- Aruba Airwave, mediante sus distintos módulos, permite... (señale el enunciado FALSO):
a) Analizar la experiencia de usuario al conectarse a la red
b) Monitorizar el comportamiento de los clientes de red
c) Configurar alertas personalizadas
d) Configurar Access Points de cualquier fabricante

95.- Aruba AirWave, mediante sus distintos módulos, permite... (señale el enunciado FALSO):
a) Bloquear automáticamente por política sitios de alto riesgo en base al comportamiento del tráfico
b) Monitorizar infraestructuras cableadas e inalámbricas
c) Reproducir mapas de calor RF
d) Medir tiempos de respuesta de conexión a redes WiFi

96.- La herramienta Aruba ClearPass permite... (señale el enunciado FALSO):
a) Crear, definir y reforzar una política consistente de acceso de qué dispositivos pueden conectarse a qué elementos de la organización
b) Controlar los dispositivos conectados mediante autenticación y/o autorización
c) Basarse en RADIUS y otros protocolos de seguridad de acceso
d) Suspender o desconectar dispositivos maliciosos a nivel de red

97.- Aruba ClearPass se utiliza para... (señale el enunciado FALSO):
e) Identificar dispositivos
f) Aplicar políticas de control de acceso
g) Proteger los recursos mediante controles de políticas dinámicos
h) Realizar el aprovisionamiento manual de dispositivos desde el departamento de TI

98.- Aruba ClearPass en sistemas WIFI... (señale el enunciado FALSO)::
a) incluye opciones de encriptado del login y el tráfico para redes públicas
b) debe utilizarse en organizaciones de más de 25 usuarios
c) soporta BYOD
d) permite la aplicación automática de políticas y controles de calidad del servicio

99.- Los controladores WIFI: se utilizan para... (señale el enunciado FALSO):
a) facilitan la gestión de la red inalámbrica
b) facilitan el acceso de los usuarios a la red inalámbrica
c) aumentan la eficiencia de la red inalámbrica
d) garantizan la cobertura inalámbrica completa mediante su funcionalidad y la de los puntos de acceso

100.- Un documento de plan de contingencia de comunicaciones debe incluir... (señale el enunciado FALSO):
a) la relación de los recursos humanos y materiales disponibles
b) el procedimiento técnico a ejecutar para restablecer el servicio a su nivel original
c) los pasos a ejecutar para la activación del plan de contingencia
d) información general sobre los sistemas y elementos críticos

101.- Son objetivos de la gestión de incidencias de comunicaciones... (señale el enunciado FALSO):
a) documentar la investigación para la resolución de la incidencia
b) minimizar el impacto negativo de la incidencia en la organización
c) restablecer el servicio lo antes posible
d) preservar la disponibilidad del servicio

102.- Forman parte ineludible del proceso de gestión de incidencias de seguridad... (señale el enunciado FALSO):
a) el registro de la incidencia
b) la categorización de la incidencia
c) el escalado de la incidencia
d) el cierre de la incidencia

103.- La primera acción a tomar ante una incidencia de seguridad registrada es:
a) asignar y escalar
b) analizar
c) comunicar a INCIBE
d) registrar las acciones de investigación de la incidencia

104.- Un plan de contingencia de seguridad... (señale el enunciado FALSO):
a) permitirá evitar la improvisación ante incidentes de seguridad
b) deberá colaborar a mitigar el impacto financiero y de imagen producido por el incidente
c) en lo posible deberá evitar la interrupción de la actividad de la organización
d) en su alcance deberá incluir todos los procesos y sistemas de la organización

105.- Los siguientes recursos, metodologías y actuaciones colaboran en la prevención de incidencias de seguridad: Señale el enunciado FALSO:
a) formación y concienciación del personal
b) elaboración de un plan de contingencia
c) implantación de buenas prácticas de gestión de sistemas de información
d) implantación del Esquema Nacional de Seguridad

106.- AlienVault UMS... (señale el enunciado FALSO):
a) detecta amenazas
b) categoriza las alarmas en 5 tipos de riesgos
c) recolecta y analiza información de seguridad de entornos locales y cloud
d) prioriza la respuesta a incidentes

107.- Un media gateway permite... (señale el enunciado FALSO):
a) conectar la red VoIP de la organización a una red IP
b) operar en un entorno mixto IP / analógico, utilizando el media gateway como traductor
c) comunicar sedes remotas que tienen implantadas distintas tecnologías (PBX y VoIP)
d) empaquetar una conversación para su transmisión por una red VoIP

108.- APN: Señale el enunciado FALSO:
a) Debe ser resuelto por DNS (Resolución de APN)
b) Puede permitir el acceso a una red pública o a una red privada
c) Requiere configurar de forma obligatoria el Identificador de red (Network Identifier) y el Identificador de Operador (Operator Identifier)
d) Indica al dispositivo por qué camino conectarse a Internet

109.- En cuanto a la configuración de APN:
a) Existe una configuración única para cada país
b) Requiere idénticos parámetros que la configuración de una VPN
c) Debe estar configurado cualquiera que sea el operador que se utilice
d) Debe modificarse para poder utilizar roaming

110.- En el marco de un hacking ético... (señale el enunciado FALSO):
a) Se pueden utilizar técnicas de ingeniería social
b) Se permite el uso de herramientas de hacking "no ético"
c) Puede enfocarse a las IP internas o externas
d) Se deben aplicar todos los métodos de Pentesting disponibles

111.- El Esquema Nacional de Interoperabilidad está orientado a... (señale el enunciado FALSO):
a) la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones Públicas
b) la eficacia y la eficiencia de las Administraciones Públicas
c) garantizar a la ciudadanía el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos
d) definir los servicios y aplicaciones que las Administraciones Públicas deben ofrecer a la ciudadanía

112.- Policy Based Routing (PBR) versus Load Balancing (LB)... (señale el enunciado FALSO):
a) Ambos permiten optimizar recursos al distribuir el tráfico por distintas vías
b) Ambos requieren la selección de un algoritmo determinado
c) PBR requiere la configuración manual de las rutas
d) LB se puede implementar por paquete (per-packet) o por destino (per-destination)

113.- El Esquema Nacional de Seguridad se implementa en una organización mediante... (señale el enunciado FALSO):
a) La implantación del nivel de madurez máximo para todos los sistemas
b) El establecimiento de un marco organizativo
c) La promulgación de una política y una normativa de seguridad
d) El establecimiento de medidas de control de acceso

114.- Los servicios ofrecidos por el CCN-CERT contemplan... (señale el enunciado FALSO):
a) Sistema de alerta temprana (SAT)
b) Formación y sensibilización
c) Informes de buenas prácticas
d) Auditoría de certificación en ENS

115.- La Guía de seguridad de las TIC (guía CCN-STIC 811) ... (señale el enunciado FALSO):
a) Es de aplicación para interconectar sistemas adscritos al ENS con otros sistemas, estén o no adscritos al ENS
b) Establece la aplicación de los principios de mínimo privilegio, nodo auto protegido y mínimo despliegue
c) Exige la redundancia de la frontera para todo tipo de arquitectura de protección del perímetro
d) Requiere un Acuerdo de Seguridad de la Interconexión

116.- En cumplimiento del RGPD... (señale el enunciado FALSO):
a) Es necesario disponer de una base legítima para poder tratar datos del interesado
b) Se aplican los principios de privacidad por defecto y privacidad por diseño
c) Es obligatorio declarar los tratamientos a la Agencia Española de Protección de Datos
d) Es obligatorio disponer de un registro de actividades de tratamiento

117.- Un firewall WAF…
a) protege a clientes
b) protege contra ataques cross side scripting
c) se despliega para proteger una red corporativa
d) filtra tráfico entre servidores

118.- Un IPS... (señale el enunciado FALSO):
a) identifica actividades sospechosas
b) desinfecta archivos maliciosos
c) bloquea ataques conocidos
d) reporta al administrador

119.- Un IPS... (señale el enunciado FALSO):
a) bloquea el tráfico basándose en su origen, destino y puerto utilizado
b) se ubica entre dos redes y controla el tráfico entre ellas
c) protege de exploits a las que la red es vulnerable
d) registra la actividad maliciosa en logs

120.- Las funcionalidades del Blade IPS de Checkpoint incluyen la detección y prevención de... (señale el enunciado FALSO):
a) intentos de tunneling que pueden indicar fuga de datos
b) exploits conocidos específicos
c) vulnerabilidades
d) accesos a URL maliciosas por parte de usuarios de la LAN

Ayuntamiento de Vitoria-Gasteiz
Vitoria-Gasteizko Udala

OPE2017-18
A110 11/04/2019
1. Ariketa- 2. Proba / 1. Ejercicio 2ª. Prueba
A/D–B Ereduko Behin-behineko Txantiloia – Plantilla provisional. Modelo A/D Y B

Nº	A
1	B
2	A
3	B
4	B
5	C
6	C
7	A
8	B
9	A
10	B
11	C
12	A
13	A
14	B
15	B
16	C
17	D
18	B
19	A
20	C
21	B
22	A
23	D
24	B
25	C
26	C
27	C
28	B
29	C
30	B

Nº	A
31	B
32	A
33	B
34	D
35	C
36	D
37	A
38	B
39	B
40	B
41	B
42	B
43	C
44	C
45	C
46	B
47	D
48	B
49	B
50	B
51	B
52	C
53	B
54	C
55	B
56	C
57	B
58	C
59	B
60	B

Nº	A
61	C
62	B
63	A
64	A
65	D
66	B
67	B
68	C
69	B
70	A
71	D
72	D
73	D
74	A
75	C
76	B
77	C
78	D
79	A
80	C
81	D
82	A
83	B
84	B
85	C
86	A
87	A
88	B
89	D
90	A

Nº	A
91	B
92	C
93	D
94	D
95	A
96	C
97	D
98	B
99	C
100	B
101	A
102	C
103	A
104	D
105	B
106	D
107	A
108	C
109	C
110	D
111	D
112	B
113	A
114	D
115	C
116	C
117	B
118	B
119	A
120	D

17/09/2019

A110.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.

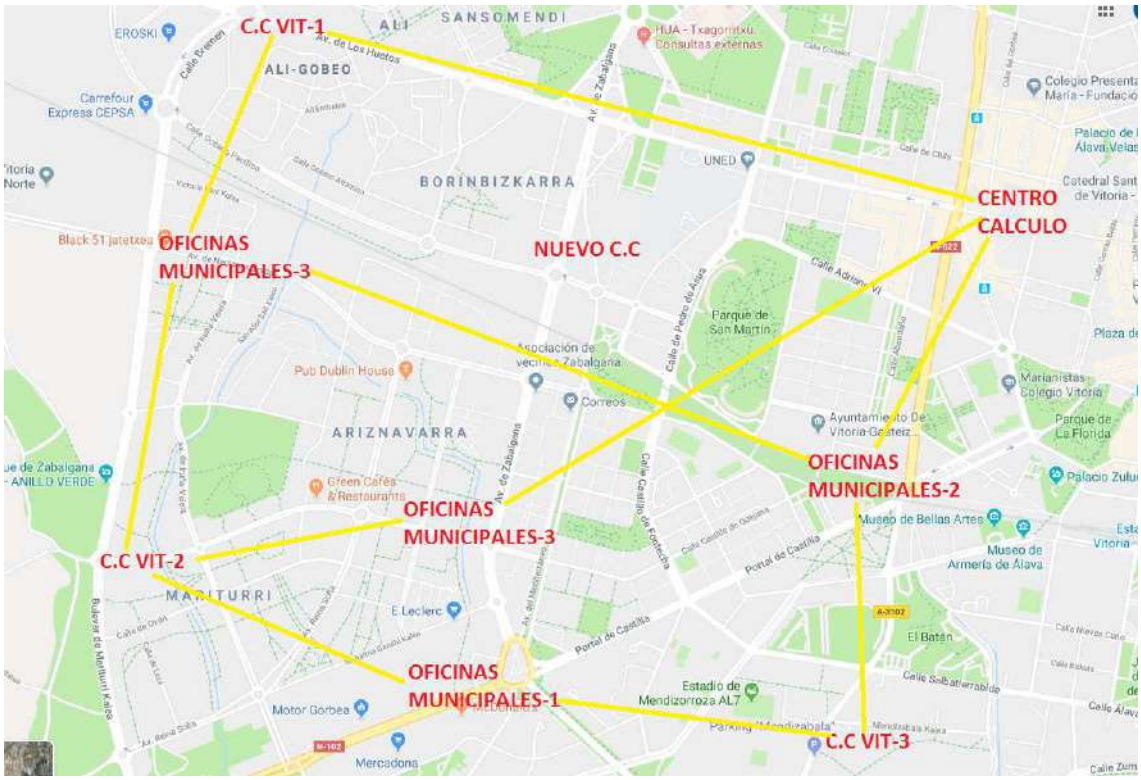
- **Móviles apagados** y, al igual que los relojes, pulseras de actividad y similares, retirados de la mesa. Botellas de agua, estuches y similares pueden tenerse accesibles pero no sobre la mesa.
- Si no hay reloj en la sala, se informará por voz del tiempo que falta para la realizar la prueba: 60-30-15-10-5 y último minuto.
- Sobre la mesa exclusivamente cuadernillo de preguntas, hoja de identificación personal, DNI y bolígrafo (azul o negro). No se permite la utilización de rotuladores de color, si 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 (A111)**
  - **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-110	OP9999ZZZZZ	1	1 / 4
A-110	OP9999ZZZZZ	1	2 / 4
A-110	OP9999ZZZZZ	2	3 / 4
A-110	OP9999ZZZZZ	3	4 / 4

SUPUESTO 1: PROYECTO DE CONEXIÓN CON FIBRA OPTICA DE UN EDIFICIO DEL AVG (400 puntos)

Introducción

El AVG va a abrir un **Centro Cívico** nuevo (**NUEVO C.C**) en el punto que se indica en el plano de Vitoria-Gasteiz.



En este mapa se aprecia la ubicación del **NUEVO C.C** y el trazado actual del entramado de la Red Corporativa de Fibra Óptica del AVG .

Es voluntad del AVG que, dada la importancia del Centro Cívico y siguiendo la línea municipal de conectar estos centros a la **red de fibra corporativa**, contratar un tendido de fibra en alta disponibilidad para la prestación de los servicios de telecomunicaciones de voz y datos de dicho Centro e **integrarlo** en dicha Red Corporativa a **nivel físico y lógico**

Datos de partida

El Centro Cívico tendrá servicios de Intervención Social, Deportes, Atención Ciudadana, Biblioteca, Zona de Lectura y otras zonas de uso público, con préstamo de libros y WIFI municipal.

Los servidores que albergan las aplicaciones necesarias para estos servicios mencionados residen en el **CENTRO DE CÁLCULO** y se sirven por la Red Corporativa de Fibra Óptica del AVG .

Se deberán tener en cuenta los servicios domotizados de mantenimiento del edificio: control de accesos, cuenta personas, video vigilancia, control de temperatura y alarmas, que deben reportar señales de control, de vídeo y de sensórica diversa a Policía y a un SCADA de Mantenimiento (todo ello en la Red Corporativa municipal).

La telefonía corporativa del edificio será VoIp, que es el estándar municipal, teniendo la central telefónica IP centralizada en el **CENTRO DE CÁLCULO.**

Se solicita:

1.1.- Definición del Proyecto y pasos previos a la instalación (120 puntos)

1. Definir los objetivos que queremos lograr en cuanto a las comunicaciones de datos del edificio nuevo:

   - Integración en la red municipal: servicios que, a su juicio, deben integrarse.
   - Servicios que no deben integrarse y ser independientes: Medios a desplegar en estos casos.

2. Uso de recursos propios: redes propias …
3. Puede servir nuestra instalación para terceros (otros organismos)? O , hay servicios de terceros que podamos usar? Ponderación de costes versus beneficios.
4. Definir los objetivos y características que, a su criterio, debe cumplir esta instalación de fibra: seguridad, redundancia, velocidad, tipo de fibra, tipo de conexión, donde y como conectar a red corporativa. (Topòlogía). Motivarlo.
5. Definición de los aspectos técnicos de la instalación: tipo de fibra, de conexión, de cable, del fusionado, con o sin empalmes intermedios razonar el porqué, racks, método de tendido de la fibra.
6. Ponderar los objetivos previstos en base a la realidad de la instalación: ubicación del edificio, tamaño y si algunos podrán o no cumplirse por razones de viabilidad o economía.

   - Replanteo de la instalación; trazado, vías alternativas, caminos redundantes, alta disponibilidad de fibra y del servicio asociado.
   - Servicios afectados o que se van a cubrir: como se sabrían estos datos? Relaciones a tener en cuenta.
   - Trabajos colaterales Mandrilado, Obra civil necesaria: ponderación de lo necesario: costes versus beneficios

1.2 - Contratación de la instalación de fibra (50 puntos)

Tras la definición del proyecto, se debe sacar a licitación, que constituye un paso muy importante por la criticidad que la adecuada elaboración del expediente puede suponer

Definir esquemáticamente un expediente de contratación de la conexión de comunicaciones por fibra óptica para este edificio. Como mínimo que abajo se indican.

1. Aspectos a tener en cuenta para contratar: categorías de empresa, hay obra civil o no, cuanta obra civil y quien puede hacerlo
2. Proceso de contratación: plazos y proceso. De una manera muy somera.
3. Cumplimiento de normativa municipal.
4. Coordinación de gremios: si hay obra civil, con terceros de otras obras...
5. Pliegos Técnico y Administrativo: criterios de valoración y Acuerdo de Calidad de Servicio. (muy esquemático)

1.3 - Seguimiento de la instalación (30 puntos)

Como lo harías?: Visitas, Reuniones, Certificaciones …

1.4 - Verificación de la instalación e Integración en Red Municipal (200 puntos)

- Recepción de documentación de la instalación: que se debe exigir y para qué?
- Verificación de lo instalado: como ?
- Instalación y configuración de la electrónica necesaria para la operativa para la cual se hace el proyecto.
- Aspectos a tener en cuenta a la hora de incluirlo en la red Corporativa: distintos servicios, seguridad, alta disponibilidad…
- Integración y despliegue de servicios en el nuevo centro: interacciones o aislamiento entre los diversos servicios, con quien se comunican, seguridad…
- Descripción técnica de los pasos a dar en la integración: a nivel de Routing, de Switching y de Seguridad. Problemas que pueden surgir, resolución de éstos…
- Pruebas: indicar cuales y para qué se harían.
- Documentación de la instalación:
- Planimetría a entregar.

SUPUESTO 2: PROYECTO DE CONVERGENCIA DE UN NUEVO ENTORNO OT CON UNO IT YA EXISTENTE (400 puntos)

Introducción

El AVG cuenta con una extensa red Corporativa en la que hay numerosos centros conectados, cada uno con sus servicios…

Esta conectividad se consigue en base a una red de fibra óptica propia para ser usada según las necesidades: transmisiones de VoIp, datos varios, vídeo..

El entorno OT lo vamos a ver como un acercamiento al Internet de las Cosas, es decir, las tecnologías y comunicaciones necesarias para poder gestionar verticales de múltiples tipos: electricidad, climatización, tráfico, sondas de diversos tipos… de cara a la obtención de unos usos y rendimientos lo más eficaces posibles, así como para la recolección de datos de interés para un uso inmediato o, tras su correspondiente almacenaje, un uso futuro.

Así, entenderemos por entorno OT el formado por :sondas, dispositivos de control de elementos industriales (válvulas, relés…) que, a través de una red de comunicaciones, envían información a un dispositivo central a través de uno o más protocolos (industriales o más estándares de la pila IP), y en este dispositivo central se podrá almacenar la información proveniente de estos dispositivos para su posterior procesado (transmisión unidireccional), o incluso, con algoritmos predeterminados, generar ordenes de vuelta a esos dispositivos (transmisión bidireccional).

La red de calle no está desarrollada a nivel OT en su totalidad. Se llega a dispositivos tales como controladores de alumbrado (no a todos), pero no se ha desarrollado un proyecto de integración que permita obtener los objetivos mencionados de:

- Enviar información desde los dispositivos de calle a un dispositivo central receptor de la información (tipo SCADA por ejemplo)
- Generar ordenes de vuelta desde el SCADA a esos dispositivos de calle.

Es decir, no se llega a TODAS partes en caso de querer implantar un proyecto concreto de aplicación para un servicio de esas características.

En el caso particular del Ayuntamiento de Vitoria-Gasteiz, entenderemos como entorno IT el de la red Corporativa con sus usos tradicionales de aplicaciones municipales y accesos a Internet: un entorno de comunicaciones informático tradicional.

La red de comunicaciones actual cumple a la perfección con los requerimientos IT, es decir, los usuarios del Ayto accede y usan las aplicaciones albergadas en servidores, almacenan los datos en BBDD con unos estándares de calidad altos.

Exposición del proyecto:

- Como ejemplo de un servicio OT, el Servicio de Tráfico necesita conectar una serie de elementos de calle como son las centrales semafóricas, los radares y las espiras de control de velocidad repartidas por la ciudad.

- Se desea que todo este entramado esté gobernado por un software denominado EKOTRAFIX que se alberga en servidores dedicados conectados a la Red Corporativa municipal.

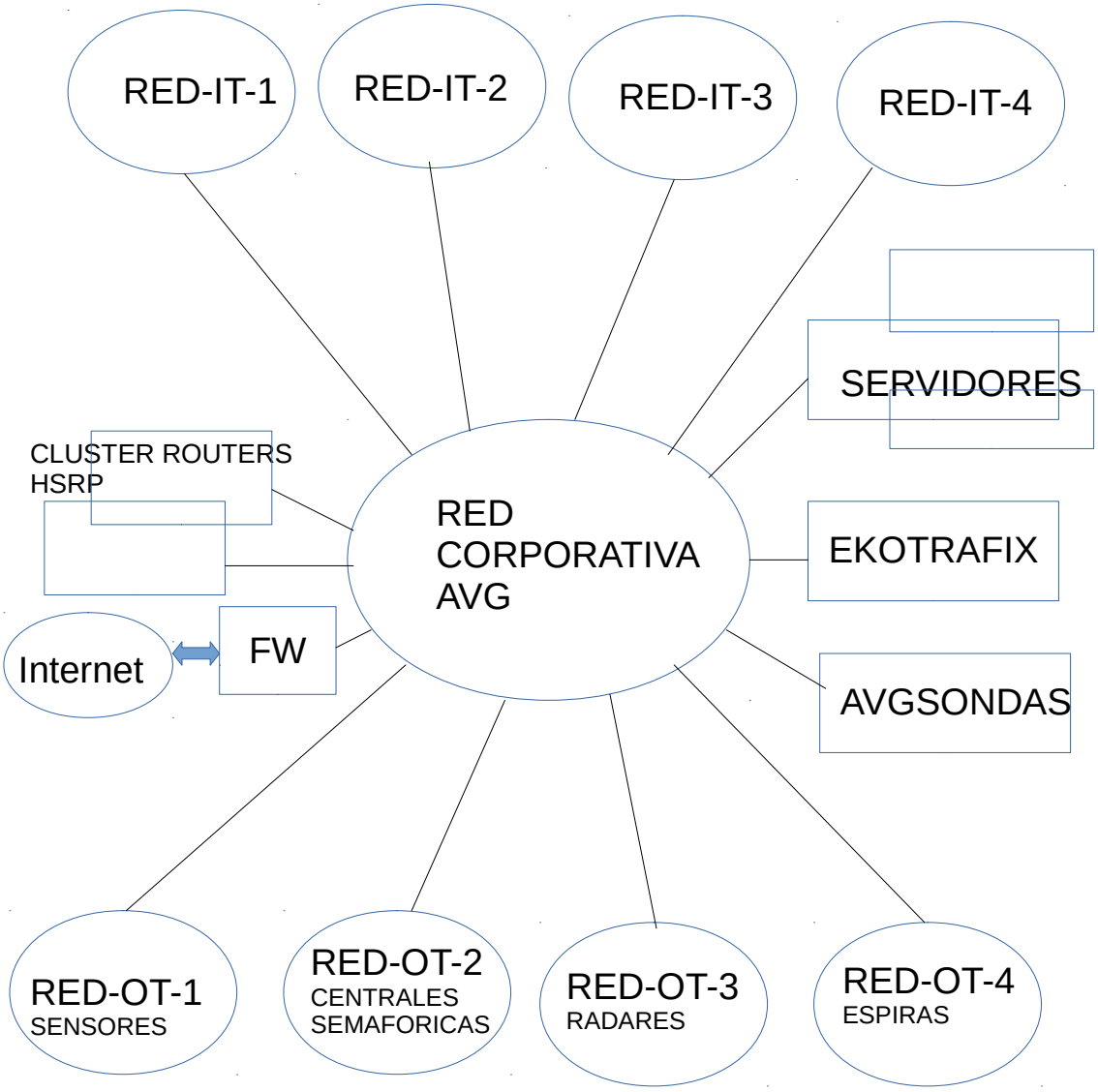
- Paralelamente, se despliegan sensores de contaminación, ruido y conteo de vehículos en múltiples puntos de la ciudad. Se desea que estos sensores reporten a una plataforma denominada AVGSONDAS aunque en este caso su tratamiento será diferente y esos datos se almacenarán en BBDD para tratar los datos y exponerlos a la ciudadanía a través de la Web municipal.

- Dada la variada casuística de los elementos mencionados en cuanto a su tipología, perfil de uso, fabricantes y de los tipos de tráfico de comunicaciones generado, así como de los usos que de dichos elementos hacen en cada servicio, lo englobaremos TODO ello bajo el paraguas de elementos OT y por ello serán objeto del trabajo.

- La conectividad de todos estos elementos la unificaremos en la red corporativa de fibra óptica municipal.

- Tanto las sondas, elementos terminales, servidores, herramientas de gestión y usuarios, estarán conectados a la Red Corporativa del Ayuntamiento de Vitoria-Gasteiz.

Esquema de situacion actual y de los elementos nuevos



- Las Redes IT-1,2,3 y 4 son redes ya existentes y en producción en la Red Corporativa. Son Layer 2 y se comunican entre ellas y con los servidores vía Routing. El routing lo proporcionan una pareja de routers en Alta Disponibilidad.
- Estas redes se conectan a los servidores para correr aplicaciones municipales.
- Las Redes OT-1,2,3 y 4 son las del nuevo entorno a conectar e integrar. Podrán ser Layer 2 o 3.
- Las redes RED-OT-2,3 y 4 se conectan al EKOTRAFIX.
- La red RED-OT-1 se conecta al servidor AVGSONDAS.
- La conexión a Internet se controla con un Firewall (FW).

Objeto del ejercicio:

La dispersión de estos elementos hace complejo el éxito en el alcance de los objetivos por lo que se plantea un proyecto de integración de los elementos OT con la estructura IT ya existente bajo el paraguas de la red corporativa que actuará como nexo de unión, siempre que sea posible con las tecnologías de dicha red, o con la implantación de las tecnologías de comunicaciones que se consideren adecuadas implantar.

El ejercicio a desarrollar deberá tener en cuenta los recursos existentes (Red Corporativa y entorno IT), las redes a integrar)entorno OT) los posibles recursos a implantar, analizar los objetivos y los elementos a integrar, buscar la mejor solución para cada tipo y hacer una planificación de acciones para conseguir dicha integración.

- Conexión de TODO este universo de elementos dispares a la red corporativa de una manera ordenada, eficaz y segura.
- Asegurar la obtención de datos para su posterior análisis mediante la elección de las tecnologías de comunicaciones más adecuadas para todos y cada uno de los servicios o tipos de tráfico, teniendo en cuenta la especial casuística de los entornos OT en cuanto a protocolos, tipos de tráfico,etc y motivando la elección.
- Conexionado de los elementos de Tráfico para su reporte a la plataforma EKOTRAFIX de cara a la toma de decisiones.
- Conexionado de las sondas para su análisis en la plataforma AVGSONDAS de gestión y su reporte a una organización externa de las Naciones Unidas (Vía Internet).
- Integrar y homogeneizar, en la medida de lo posible, los entornos a nivel de: equipamiento, mantenimiento, tecnologías, protocolos..
- Contemplar todo el proyecto desde el punto de vista de un entorno seguro, introduciendo, o modificando, si así se considera necesario, los elementos necesarios para ello.

Se solicita:

2.1. Análisis de necesidades (30 Puntos)

2.2. Perfiles /protocolos de tráfico: definición, volumen, análisis de necesidades con atención a la casuística y características de los entornos OT. (30 Puntos)

2.3. Análisis de posibilidades de conectividad a la red corporativa: pros, contras, viabilidad de cada una, compatibilidad con la base tecnológica existente, costes asociados. (50 Puntos).

2.4. Elección motivada de la / las soluciones a implantar. (50 Puntos).

2.5. Modelo de integración a nivel Físico y Lógico (hasta nivel de Red.), incluido el modelo de seguridad si se considera oportuno. (170 Puntos)

2.6. Modelo de gestión a nivel de herramientas de monitorización y de prevención o resolución de incidentes, si procede.(para ambos entornos) (30 Puntos)

2.7. Pruebas a realizar / Validación de la solución. 40 Puntos)

SUPUESTO 3: PASOS A DAR PARA LA INSTAURACIÓN DEL ENS EN UNA ADMINISTRACIÓN LOCAL (200 PUNTOS)

Introducción y precedentes

El Ayuntamiento de Vitoria-Gasteiz, (en adelante AVG) siguiendo una línea de trabajo orientada a la prestación de servicios digitales al ciudadano, en algunos de los cuales la seguridad en el manejo de los datos, en uno y otro sentido, cobra especial relevancia.

Es por ello que, siguiendo los requerimientos legales que las leyes 39 y 40 nos obliga a cumplir, se plantea como reto el cumplimiento de los preceptos del Esquema Nacional de Seguridad (ENS) dentro del área de actuación del AVG.

Se solicita:

3.1. Razonar, brevemente, las causas por las que el AVG debe cumplir el ENS (14 puntos)

3.2. Objetivos que el ENS persigue y que, en nuestro caso, serían objetivo para el AVG. (16 puntos)

3.3. ¿Cuales serían los elementos básicos y/o ámbitos de actuación del ENS en el AVG? (20 puntos)

3.4. Enumerar los principales Roles o Figuras que aparecen en la Organización, atendiendo a la responsabilidad que tienen en la especificación, supervisión y operación de la seguridad de la información en el AVG. (10 puntos)

3.5. Definir, de una manera esquematizada, las Fases a desarrollar y , dentro de cada una de ellas, las subfases y/o acciones a implementar. (140 puntos)