ACTUALIZACIÓN DE MEDIDAS DE CIBERSEGURIDAD EN LA RED DE EXPLOTACIÓN DE ETS

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

ÍNDICE

1 OBJETO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES 1

2 RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES 2

3 DESARROLLO GENERAL DE LOS TRABAJOS 3

3.1 CONTROL DE LOS TRABAJOS 3

3.2 PROGRAMA DE TRABAJOS 3

4 ANTECEDENTES, DOCUMENTOS DE REFERENCIA Y PLANTEAMIENTO GENERAL 4

4.1 ANTECEDENTES 4

4.2 OBJETIVO 4

4.3 DOCUMENTACIÓN Y NORMATIVA DE REFERENCIA 5

4.4 PLANTEAMIENTO GENERAL 5

4.5 POLÍTICAS Y PROCEDIMIENTOS 6

4.6 SEGURIDAD PERIMETRAL Y SEGURIDAD EN RED 8

4.7 SEGURIDAD EN DATOS. ANTIVIRUS 9

4.8 DOMINIO Y ACTUALIZACIONES DE SISTEMA OPERATIVO 9

5 TRABAJOS A REALIZAR POR EL CONTRATISTA 11

5.1 TRABAJOS PREVIOS 11

5.2 ANÁLISIS DE LA SITUACIÓN ACTUAL 12

5.3 MEDIDAS DE CIBERSEGURIDAD EN LA RED OT 12

5.4 ACTUALIZACIÓN DE LAS POLÍTICAS SEGURIDAD ETS 27

5.5 CONTROL DE RESULTADOS 29

5.6 DOCUMENTACIÓN Y FORMACIÓN 29

5.7 SOPORTE DEL ADJUDICATARIO 30

6 GARANTÍA 33

7 CERTIFICACIONES 34

8 PLAZO DE EJECUCIÓN DE LOS TRABAJOS 35

9 PRECIOS DE CONTRATO 36

10 VALORACIÓN Y ABONO DE LOS TRABAJOS REALIZADOS 37

11 PRESUPUESTO DEL CONTRATO 38

12 ANEJO: CUADRO DE PRECIOS 39

1 OBJETO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

El objeto del presente Pliego de Prescripciones Técnicas Particulares es el de establecer las condiciones técnicas que han de regir la adjudicación y, en su momento, del servicio para la actualización de medidas de ciberseguridad en la red de explotación de ETS y para proporcionar su posterior soporte tecnológico.

2 RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES

A los efectos de fijar las relaciones contractuales se definen las siguientes figuras jurídicas:

PROPIEDAD.- ETS, Ente Público del Gobierno Vasco.

RESPONSABLE DEL PROYECTO.- ETS designará un Responsable del Contrato, bajo la supervisión de la Dirección de Instalaciones Y Mantenimiento. Dada la complejidad de los trabajos, el Responsable del Contrato podrá rodearse del equipo técnico necesario que le asesorará y en su caso podrá actuar por delegación del mismo.

CONTRATISTA.- Licitador Adjudicatario del contrato de prestación de servicio, persona natural o jurídica que adquirirá esa condición a la firma del Contrato.

DELEGADO/A DEL CONTRATISTA.- Técnico Superior, designado por el Contratista para hacerse cargo de la coordinación técnica de los trabajos y representar a éste frente a ETS. Todo el equipo del Contratista dependerá del Delegado, quien informará directamente y cuantas veces sea requerido al Responsable del Proyecto.

3 DESARROLLO GENERAL DE LOS TRABAJOS

3.1 CONTROL DE LOS TRABAJOS

Al menos una vez por mes, el Contratista informará por escrito al Responsable del Proyecto sobre el estado de los trabajos hasta entonces realizados, y solicitará de él las instrucciones pertinentes para la continuación o nueva presentación de aquellos.

Siempre que el Contratista solicite alguna instrucción o decisión, deberá proponer a su vez, aquélla que a su entender considere como más apropiada. En cualquier momento el Equipo Técnico del Responsable del Proyecto, podrá inspeccionar la marcha de los trabajos, en la oficina del Contratista.

Las observaciones o prescripciones que se deriven de la inspección serán comunicadas al Contratista a través del Responsable del Proyecto.

De todas las reuniones que se mantengan entre el Equipo Responsable del Proyecto y el Contratista se levantarán ACTAS donde se recojan las propuestas, modificaciones, instrucciones y conclusiones que se adopten.

3.2 PROGRAMA DE TRABAJOS

Completada la revisión de los documentos y datos básicos, el Contratista hará entrega al Responsable del Proyecto del Programa de trabajo, que detallará a nivel operativo el Plan de Trabajo que hubiese sido presentado en la proposición.

El programa de trabajos contendrá los siguientes elementos:

- La metodología pormenorizada según la cual se propone al Contratista realizar los trabajos, desarrollada a nivel operativo y acompañada de las justificaciones pertinentes.
- La organización del equipo del Contratista para el desarrollo de los trabajos, incluyendo la relación de personas, la relación de medios materiales y la descripción organizativa del equipo.
- El Plan de Trabajo, incluyendo Cronograma completo para la ejecución de los trabajos de redacción que sea compatible con lo establecido en el presente Pliego y acorde con lo indicado en la propuesta económica

4 ANTECEDENTES, DOCUMENTOS DE REFERENCIA Y PLANTEAMIENTO GENERAL

4.1 ANTECEDENTES

En ETS coexisten dos redes de comunicaciones bien diferenciadas. La red corporativa, sistemas u ofimática y la red de explotación o multiservicio.

La primera red está gestionada por el departamento de sistemas y en ella se encuentran los servidores y ordenadores donde se ejecutan las aplicaciones corporativas (correo electrónico, intranet, SAP, aplicaciones de gestión, almacenamiento etc.) así como los PC de trabajo de cada usuario de ETS. Esta red dispone de sus sistemas de seguridad tanto perimetrales (firewall) como a nivel de usuario final (endpoint) dado que se relaciona con redes externas.

La segunda red está gestionada por el departamento de mantenimiento y sobre ella se soportan todos los sistemas relacionados con la explotación ferroviaria. Esto incluye sistemas críticos como son los relacionados con la señalización ferroviaria, telemandos de energía e instalaciones, sistemas de seguridad, etc. Esta red dispone de accesos punto a punto a ciertas máquinas, así como de conexión con la red corporativa de ETS y con la red de Euskotren a través de un router XSR (Enterasys) en Atxuri. En el año 2019, ETS caracterizó y auditó la seguridad de esta red con el objetivo de determinar su estado y de las mejoras a acometer en la red, para protegerla frente a amenazas y riesgos informáticos.

4.2 OBJETIVO

El objetivo de este servicio es la ejecución de las medidas necesarias para dotar de seguridad a la red de explotación de ETS, materializando las acciones identificadas en este documento como resultado de la auditoría de la red de explotación realizada en el año 2019.

La red de explotación está compuesta por equipos y tecnologías heterogéneas (IP, MPLS, DSL), medios de transmisión de fibra óptica y cobre y los sistemas ferroviarios que permiten la operación del servicio y que se soportan sobre la red de explotación, no siendo objeto de este pliego las medidas de ciberseguridad a implantar en los servidores y equipos de los sistemas ferroviarios que se materializarán en el ámbito de su correspondiente contrato de mantenimiento. En cambio sí que es objeto del presente pliego la actualización de las políticas de seguridad de ETS para incorporar las medidas de protección y seguridad de los sistemas ferroviarios.

4.3 DOCUMENTACIÓN Y NORMATIVA DE REFERENCIA

Los trabajos objeto del presente concurso comprenderán todas las labores necesarias para la "Actualización de medidas de ciberseguridad en la red de explotación de ETS", tendrán como referencia la siguiente documentación:

- Auditoría de Seguridad de la Red de Explotación de ETS (2019)

La ejecución de los trabajos deberá realizarse conforme a la siguiente normativa:

- ISO/IEC 27001 que proporciona las directrices en los controles de seguridad para el Sistema de Gestión de la Seguridad de Información (Información Security Management System).
- ITU-T X.805 que proporciona las directrices para analizar los requisitos de seguridad de los sistemas de comunicación extremo a extremo.
- Se deberán seguir practicas recomendadas que tengan aplicabilidad en los equipos industriales de control que están bajo en alcance de la normativa ISA/IEC 62443.

4.4 PLANTEAMIENTO GENERAL

El objetivo del conjunto de medidas y sistemas de ciberseguridad es el de proteger la información procesada, almacenada y transmitida y monitorizada en el ámbito de la red de explotación de ETS.

El planteamiento de este conjunto de medidas se basa, de forma general, en el enfoque de *defensa en profundidad (Defense in Depth)* que está estratificado en diferentes capas para la aplicación de políticas, medidas y soluciones de ciberseguridad en cada una de las capas.

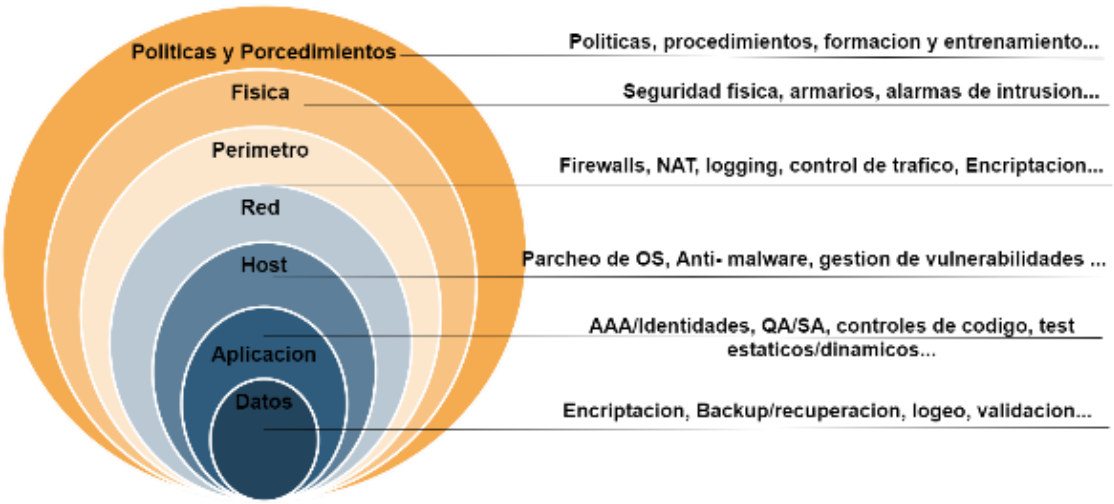


Figura 1: Arquitectura de defensa en profundidad

Este enfoque supone la superposición de una serie de mecanismos defensivos, medidas y soluciones para proteger equipos, sistemas y datos e información valiosos.

Si un mecanismo falla, otro actúa inmediatamente para frustrar un ataque sin que afecte a más capas. Este enfoque de múltiples capas con redundancias intencionadas aumenta la seguridad de un sistema en su conjunto y aborda muchos vectores de ataque diferentes.

De esta manera las soluciones propuestas y adoptadas en un proyecto de ciberseguridad deberán ser evaluadas y seleccionadas en función de la criticidad de los activos, focalizando las inversiones en ciberseguridad en aquellas medidas y soluciones que impidan la materialización de vectores de ataque que afecten directamente a los sistemas y activos más importantes y críticos para la operación. Estos sistemas y activos más importantes deberán ser identificados en un análisis de riesgos realizado inicialmente.

4.5 POLÍTICAS Y PROCEDIMIENTOS

El Comité de Seguridad Lógica y Física de ETS es el órgano ejecutivo y consultivo que trata de resolver de forma corporativa y transversal dentro de la organización los aspectos relativos a la Protección de las Infraestructuras Sensibles, tanto en la vertiente de la seguridad física como de la seguridad lógica y de ciberseguridad.

Este Comité asume todas las funciones previstas para el Comité de Seguridad de la Información en la Política y Procedimientos de Seguridad de la Información basadas en la ISO 27001:2013.

ETS realizó la auditoría de seguridad de su red de explotación en el año 2019 que culminó con un conjunto de medidas a aplicar para disminuir el riesgo de comprometer la disponibilidad de sus sistemas de explotación.

Las tareas de implantación definidas en este pliego para la actualización de las medidas de ciberseguridad de la red OT de ETS, se llevarán a cabo cumpliendo la Política de Seguridad de la Información de ETS ultima versión de Mayo 2021, revisando los procedimientos actuales y proponiendo aquellas modificaciones que se requieran realizar para poder cumplir los requisistos de los nuevos sistemas implantados.

4.5.1 SEGURIDAD EN HOST

Todos los equipos de la red de explotación deberían estar configurados de la forma más segura posible ya que pueden ser el origen de una intrusión, además de ser utilizados para realizar movimientos laterales por los posibles atacantes.

Estas medidas podrían incluir aspectos como:

- Bastionado y configuración que maximice la seguridad de servidores y equipos de acuerdo con las políticas de ciberseguridad definidas.

- Estudio para la identificación de necesidades de renovación de equipos con sistemas operativos o aplicativos de operación sin soporte del fabricante, de actualizaciones de ciberseguridad y/o de parches de actualizaciones.
- Configuración de un sistema de autenticación centralizada (AD, LDAP, RADIUS o similar)
- Medidas de seguridad para el control de dispositivos:
    - Planificación y programa para la Instalación de seguridad parches
    - Desactivación de cualquier funcionalidad innecesaria (servicio)
    - Activación exclusiva de protocolos seguros (cifrados / autenticados)
    - Activación de registros
    - Sincronización horaria
- Metodología para gestión de usuarios y permisos
    - Cambio de contraseñas para usuarios locales
    - Cifrado de protección de contraseña local
    - Contraseña y Política de sesión
    - Mecanismo Single Sign On (SSO)
- Gestión de cuentas locales
    - Eliminación de usuarios innecesarios

La implantación de medidas de seguridad en host no es objeto de este servicio sino que corresponden al mantenedor de la máquina del correspondiente sistema ferroviario.

En cambio, sí se incluye la actualización de las políticas de seguridad de ETS con todas las medidas identificadas en este servicio, así como las instrucciones técnicas especificas que describan al detalle la configuración de los equipos a nivel de sistema operativo, dominio, antivirus, aplicación, etc

También se deberá incluir la definición de cómo deberá ejecutar cada mantenedor el backup de los datos de cada uno de los subsistemas, incluyendo una política de backup manual.

4.5.2 SEGURIDAD EN APLICACIONES

A nivel de aplicación se deberá maximizar y procurar la utilización de protocolos seguros (o versiones revisadas) por parte de todos los subsistemas que se integran en la red de explotación.

Esta medida es complementaria a la funcionalidad recogida en los apartados anteriores y su aplicación corresponde al desarrollador/mantenedor de cada subsistema. Aunque adicionalmente se reviará y actualizará el procedimiento actual.

4.6 SEGURIDAD PERIMETRAL Y SEGURIDAD EN RED

La seguridad perimetral hace referencia a la seguridad que afecta a la frontera de una red de datos, como es el caso de la red de explotación de ETS. Esta frontera está formada por el conjunto de máquinas y dispositivos (Firewalls) que interactúan con el exterior y con otras redes. Esta seguridad perimetral junto con la segmentación de las redes limita en gran medida el área de superficie de ataques en la red, realizando análisis y filtrado de tráfico.

Los dispositivos de seguridad perimetral permiten integrarse en redes multiprotocolo y aplicar las funcionalidades de seguridad más actuales, como son:

- Funcionalidades el sistema de detección y prevención de intrusiones (IDS / IPS)
- Filtrado en múltiples capas OSI.
- La inspección profunda de paquetes incluso en la capa de sockets seguros (SSL).
- La protección automatizada contra amenazas.
- Sincronización de tiempos, para permitir que los equipos y sus logs estén sincronizados en base a un equipo altamente seguro.
- Sistema de prevención de fugas de datos (DLP) para evitar que los datos confidenciales entren o salgan de la red.

En el caso concreto de la red OT de ETS, ésta cuenta con conexión con la red IT de ETS y con la red de Euskotren a través de un router XSR (Enterasys) en Atxuri.

ETS no cuenta con accesos radio (WiFi, TETRA) a la red de explotación, por lo que no se incluirá ninguna actuación en dichas redes.

Los firewalls suministrados serán los encargados controlar y filtrar el acceso a las redes IT y a las redes de Euskotren, las redes OT de salto y los servicios separados en subredes de la red OT. La segmentación de la red OT existente, junto con los nuevos firewalls, permitirá identificar y controlar todo el tráfico entre segmentos de la red, ya que para su apertura será necesaria la solicitud, justificación y autorización de todos los flujos de datos. Esto, a su vez, limitará en gran medida el área de superficie de ataques a la red y especialmente los movimientos laterales entre equipos, por un atacante.

El análisis y aplicación de las medidas en la red OT correspondientes para garantizar la seguridad de los accesos remotos desde la red IT son objeto de este servicio. Un ejemplo de estas medidas puede ser la aplicación de doble factor de autenticación basado en el nombre de usuario / contraseña y el token para los accesos habituales.

La aplicación de las medidas de seguridad en estos puntos de conexión es objeto de este servicio, siendo muy importante que en cualquier punto de conexión entre redes exista un firewall inspeccionando el tráfico entre las mismas.

Adicionalmente, para garantizar la redundancia y resiliencia de las comunicaciones, los firewalls, piezas centrales de seguridad de la infraestructura, deberán estar en alta disponibilidad formando clústeres en cada una de las ubicaciones.

4.7 SEGURIDAD EN DATOS. ANTIVIRUS

Los sistemas de protección EndPoints ayudan a reducir el impacto de las amenazas informáticas evitando por ejemplo la conexión no autorizada de cualquier dispositivo remoto o unidad de almacenamiento externo que pueda usarse para ingresar o extraer información de él.

Todos los dispositivos susceptibles a ataques deberían tener una solución de punto final (endpoint) para su protección, gestionada de forma centralizada lo que le permitiría realizar acciones sobre ellos y verificar el estado de salud de toda la infraestructura.

El adjudicactario deberá integrar las nuevas licencias en la actual solución de la red IT. Las nuevas licencias incluirán la posibilidad de distribuir una versión para sistemas operativos obsoletos o fuera de soporte, así como una versión de antivirus con un impacto mínimo en la red OT.

El suministro de las licencias de plataformas endpoint y de software antivirus/antimalware/antispyware es parte del objeto del contratato.

Será necesario además crear un documento que incluya la instalación manual del antivirus en el equipo/servidor OT. Dicha instalación la realizará el mantenedor de cada sistemas OT al igual que cuando se actualizan las aplicaciones de los equipos/servidores.

4.8 DOMINIO Y ACTUALIZACIONES DE SISTEMA OPERATIVO

La red IT de ETS dispone de la palataforma SCCM 2016, que gestiona el inventario del software instalado, el inventario de hardware, despliegue de sistemas opertivos de puesto cliente, la distribución e instalación de dicho software, la gestión de parches de sistema operativo y algunas de las aplicaciones en todos los dispositivos pertenecientes al dominio.

Se quiere extender la funcionalidad del SCCM a la red OT, estableciendo directivas especificas para los dispositivos OT y su software especifico asociado. Se quiere además implementar una gestión autónoma para la red OT dentro del SCCM.

En los últimos años se han integrado algunas de las aplicaciónes de la red OT con el domino Windows de la red IT. A través de dos controladores de dominio físicamente

cercanos a los puestos de mando de Amara y Atxuri, se consigue dar servicio a aquellas aplicaciones de la red OT integradas con el directorio activo.

Como parte de los trabajos inlcuidos en el presente pliego, se quiere instalar un nuevo servidor físico que realice funciones de controlador de domino en la red OT, para aumentar la disponibilidad del servicio ante problemas entre la red IT-OT.

Solo se incluirán en el SCCM aquellos dispositivos con sistema operativo con soporte.

5 TRABAJOS A REALIZAR POR EL CONTRATISTA

Todos los trabajos se realizarán tomando las medidas necesarias para garantizar que los procesos que se ejecutan no repercuten en pérdidas de información ni afecta a la operación del sistema ferroviario.

Durante todo el proceso de instalación, configuración y pruebas, el adjudicatario transferirá el conocimiento necesario a los técnicos de ETS para que éstos sean autónomos en la gestión del nuevo sistema.

La formación comenzará con una sesión inicial, previa a la configuración del sistema.

La instalación y configuración de los aplicativos identificados se realizará conjuntamente con las personas que ETS determine, formados en la realización de las tareas tipo y de mantenimiento.

Todo el proceso se realizará en las instalaciones de ETS.

Los trabajos a realizar por el contratista se dividen en las siguientes fases:

- Trabajos Previos
- Análisis de situación actual
- Ejecución de medidas de ciberseguridad en la red de explotación
- Actualizacion de las políticas de seguridad de ETS
- Control de los resultados
- Documentacion y formación
- Soporte

5.1 TRABAJOS PREVIOS

En un primer momento, el Contratista concretará con el Responsable del Proyecto los siguientes aspectos:

- Criterios y pautas de trabajo. Frecuencia de las reuniones de seguimiento, etc.
- Revisión del alcance del contrato y documentación a entregar durante la ejecución y a la finalización del mismo
- Interlocutores por ambas partes para la ejecución de los trabajos recogidos en el alcance del contrato
- Programa de trabajos. Revisión de la planificación del proyecto y fechas de entrega
- Previsión de certificaciones

5.2 ANÁLISIS DE LA SITUACIÓN ACTUAL

El contratista de forma previa al inicio de los trabajos recopilará la documentación de referencia disponible en ETS en relación con el estado actual de la red de explotación, incluyendo:

- Dispositivos de la red y su configuración
- Servidores y equipos integrados en la red de explotación incluyendo su sistema operativo, base de datos, software instalado, etc.

Asimismo, mantendrá las reuniones que sean necesarias con ETS para comprobar el correcto entendimiento de la documentación de referencia y para conocer las últimas actuaciones que ETS haya podido materializar en ella y que pudieran afectar al desarrollo de este servicio.

5.3 MEDIDAS DE CIBERSEGURIDAD EN LA RED OT

El contratista deberá materializar las acciones de mejora identificadas en el documento de auditoría y otras que pudieran haber sido identificadas en la fase previa. De forma previa a su ejecución, el contratista deberá tomar las medidas necesarias para garantizar que los procesos que ejecuta no repercuten en pérdidas de información existente ni afecta a la operación del sistema ferroviario.

5.3.1 LOTE 1: FIREWALL +IDS/IPS

Actualmente el acceso desde el exterior a los recursos de la red de explotación de ETS se realiza mediante VPN utilizando el servicio OpenVPN, siendo objeto de esta licitación la implantación de una nueva solución que mejore la actual.

Se ha previsto implantar una solución basada en Firewalls que deberá garantizar, como mínimo, las siguientes funciones:

- Descubrimiento y control del comportamiento de cada dispositivo conectado a la red
- Detección de un dispositivo infectado en la red
- Establecimiento de políticas de acceso homogéneas para la red.
- Control de proveedores que trabajan en la red
- Control de redes de operación

Una vez conectado a la VPN de la red IT, el Firewall OT será el responsable de permitir el acceso a una máquina de salto específica para dicho uso y este acceso se gestionará en función del usuario que haya accedido. La máquina de salto deberá estar debidamente bastionada y los usuarios que accedan a ella deberán tener los mínimos privilegios posibles, debiendo aplicar mecanismos de filtrado de tráfico para evitar que éste pueda acceder de una a otra sin ninguna restricción.

El contratista deberá suministrar dos clústeres lógicos de dos appliances físicos (Firewalls +IDS/IPS), uno instalado en el Puesto de Mando de Atxuri y otro instalado en el Puesto de Mando de Amara. Estos clústeres deberán estar configurados en alta disponibilidad (HA) y deberán estar integrados con el servicio de directorio activo que también es objeto de esta implantación.

En cada ubicación, Atxuri y Amara, se instalaran una pareja de Firewall que tendrán funciones de un único Firewall lógico.

Caracteristicas tecnicas de los Firewall

El firewall NGFW a suministrar deberá disponer de las siguientes prestaciones:

Seguridad:

- Deberá disponer de funcionalidades de detección y prevención de intrusiones (IDS / IPS) utilizando inteligencia artificial y machine learning.
- Posibilidad de aplicar diferentes perfiles de seguridad (IPS, App Control, Antivirus, Malware, Botnet, Sandbox, Antispan, Web & Video Filtering) al tráfico de diferentes aplicaciones incluso cuando estas aplicaciones se sirven desde el mismo servidor (misma dirección IP, mismo puerto TCP)
- Deberá identificar las aplicaciones dentro de la red para su inspección y aplicación de políticas.
- Deberá detectar e identificar dispositivos de IoT manteniendo estos protegidos a través de firmas de protocolos ics/ sacada constantemente actualizadas.
- Deberá disponer de la posibilidad de actuar como termiandores de conexiones VPN e inlcuir la liecncia para ello.
- Deberá proporcionar protección contra todo tipo de malware.
- Deberá bloquear proactivamente nuevos potenciales ataques a la red
- Deberá disponer de visibilidad total de usuarios, dispositivos y aplicaciones en toda la superficie de ataque y deberá aplicar políticas seguridad de forma constante e independientemente de la ubicación del activo a proteger
- Deberá prevenir la pérdida de datos e identificar toda actividad del usuario
- Deberá disponer de funciones de filtrado en múltiples capas OSI
- Deberá soportar los protocolos criptográficos en su última versión disponible para garantizar las comunicaciones seguras de la red (SSL/TLS).

Rendimiento:

- Deberá proporcionar baja latencia y un rendimiento optimizado en su función de protección de la red; tiempo de latencia con reglas integradas, firewall + antivirus + ips/ids + url filtering no superior a 1 milisegundo.
- Deberá ofrecer como mínimo los siguientes parámetros de rendimiento:
    - NGFW Throughput: 1.6 Gbps

IPS throughput: 2,6 Gbps
Firewall throughput: 20 Gbps
IPSec VPN Throughput: 11,5 Gbps
SSL-VPN Throughput: 1 Gbps

- Latencia: 4,97 us
- Sesiones concurrentes (TCP):1,5 Millones
- Almacenamiento SSD: 480 GB

Red:

- Deberá ofrecer capacidades de red avanzadas que puedan integrar seguridad avanzada de capa 7 y dominios virtuales (VDOM).
  Capacidad para identificar aplicaciones activas actuales (como por ejemplo, RDP, ssh, anydesk, sharepoint, modbus, profinet/profibus,…)
- Los firewalls deberán tener las interfaces necesarias para garantizar el throughput requerido por la red, incluyendo slots:
  - 16 puertos GE RJ45: 2 puestos para HA, 2 puertos para gestión y el resto reutilizables como interfaces FW.
  - 10 GE SFP+ (min 2), además de
  - Se valorará la inerfaces SFP y SFP+ adcionales.
- Se incluirán al menos 2 transceptores SFP GE SX y 1 transceptor SFP+ 10GE SR por equipo.
- El nuevo equipamiento deberá soportar routing dinámico (OSPF, BGP), DHCP relay, protocolos multicast, así como calidad de servicio QoS.
- Deberá ofrecer la posibilidad de enrutador vía OSPF, posibilidad de enrutador por políticas y capa 7, enrutador a través de rutas estáticas y control de tráfico asimétrico.
- Deberá ser capaz de monitorizar y controlar la navegación web sin penalizar el tiempo de respuesta ni la satisfacción del usuario.
- Monitorización de tráfico pudiendo filtrar este por IP Origen, IP Destino, Usuario, Aplicación, Puerto Origen, Puerto Destino, Acción, Regla, etc.

Protocolos: IPSEC site to site, IPS, SSL-VPN, IPv6, TLS 1.3

Disponibilidad:

- La pareja de firewalls deberá soportar la configuración en modo HA (Alta disponibilidad en activo-activo y activo-pasivo), presentando un única dirección IP en cada segmento de red y repartiendo la carga entre ambas máquinas que componen el clúster. En caso de caída de uno de los nodos, el nodo operativo deberá asumir todas las funciones y carga del clúster.

Backup:

- El nuevo sistema deberá presentar funcionalidades de recuperación de sistema mediante copias de seguridad.

Gestión:

- Deberá incluir una consola de gestión que se pueda utilizar de forma sencilla para proporcionar automatización total y visibilidad de la red. El software de administración y gestión de los nodos de firewall se podrá realizar a través de la interfaz gráfica e interfaz de comandos. Tendrá una gestión de usuarios con diferentes niveles de acceso para varios administradores.
- Deberá proporcionar alertas de disponibilidad de la plataforma y alertas de seguridad

Informes:

- Se requiere pode realizar informes ~~"out of the box" y personalizados~~ sin necesidad de desarrollos adicionales. Es imprescindible la capacidad de obtener informes de actividad por usuario (integración con el directorio activo de Windows): aplicaciones utilizadas, web sites visitados por usuario, anchos de banda usados por aplicación, posibles infecciones de máquinas… Exportación a pdf del informe.
- Todos los registros de tráfico (LOGs) generados por el sistema deben incorporar el atributo "aplicación".
- Si se requiere una licencia adicional para cumplir los requisitos de informes comentados, debe estar incluido en el precio ofertado.

Antivirus en el trafico filtrado:

- Proporción de análisis de ficheros para la identificación de virus. Sandbox activado que permita al Firewall enviar muestras sospechosas para que se ejecuten en un entorno controlado. El análisis debe alimentar automáticamente el sistema de firmas de virus, spyware y URL filtering.
- Análisis de contenidos para identificar comunicaciones con los centros de control de Botnets (spyware, phonehome. adware …)
- Análisis de contenidos para identificación de vulnerabilidades tanto de cliente a servidor como de servidor a cliente

Certificaciones:

- Deberá disponer de certificaciones independientes que garanticen el rendimiento y eficacia de sus mecanismos de seguridad.

Reglas, filtrado y control de tráfico:

- El sistema de reglas del Firewall debe poder usar los criterios "usuario", "grupo" y/o "plataforma" para discriminar las políticas de seguridad. Poder, por ejemplo, aplicar protección de Antivirus en red sólo al tráfico generado

por usuarios de un determinado grupo o al generado por un determinado usuario o al generado por un determinado tipo de terminales independientemente del usuario que lo opera.

- Posibilidad de mapear dinámicamente usuarios con direcciones IP usando como información los eventos de seguridad generados por sistemas de confianza como Domain Controllers o Exchange Servers.
- Posibilidad de obtener dinámicamente agrupaciones de usuarios usando directorios LDAP
- Accesorios adicionales. Se incluirán los transceivers SFP+, propios del fabricante, necesarios para cubrir los puertos a 10Gb de downlink de cada uno de los cuatro NGFW que componen los dos clusters. Distancia máxima a cubrir de 300M en fibra multimodo.

Trabajos de configuración

La empresa adjudicataria conectará los equipos perimetrales al cuadro eléctrico y a los dispositivos de la red de explotación correspondientes, incluyendo todos los elementos y trabajos necesarios para que los equipos queden totalmente operativos (latiguillos de red, latiguillos de fibra, etiquetas, fijaciones, etc.).

La empresa adjudicataria se encargará de la instalación de los FW en el rack el etiquetado y colocación de cableado según las necesidades de ETS.

Los trabajos de migración deben incidir mínimamente en el servicio prestado a los usuarios. Algunas tareas se realizarán en el horario definido por ETS, teniendo en cuenta la continuidad del servicio ferriviario y sus sistemas asociados.

El adjudicatario comprobará la compatibilidad de firmware instalados en la electrónica de red conectada a los nuevos firewalls, y se actualizará si fuese necesario.

Antes de la puesta en marcha en producción el adjudicatario realizará junto a los técnicos de ETS la identificación de cada uno de los servicios y aplicaciones, relizando un checklist o banco de pruebas para la implantación. Se realizarán pruebas de funcionamiento y alta disponibilidad de todo el equipamiento firewall.

El adjudicatario configurará en las dependencias de ETS la interfaz de gestión de cada dispositivo asignándole la dirección IP que establezca ETS. Tal y como se ha indicado, la implantación se realizará en alta disponibilidad (HA). Adicionalmente el adjudicatario deberá activar todas las licencias incluidas en su oferta.

El adjudicatario deberá realizar la configuración de los equipos perimetrales y realizar todas las pruebas necesarias para garantizar que la solución implantada funciona de forma correcta:

- Objetos
- Servicios

- Perfiles
- Reglas
- Túneles VPN
- Integración con el servicio de directorio activo
- Importación de certificados
- Etc.

En caso de que ETS detectara algún problema en el funcionamiento de la red, se deberá prever una vuelta atrás a la situación de partida.

Formacion de la nueva configuracion

Durante todo el proceso de instalación, configuración, migración y pruebas, el adjudicatario transferirá el conocimiento necesario a los técnicos de ETS para que estos sean autónomos en la gestión de la nueva plataforma.

La formación comenzará con una sesión inicial, previa a la configuración del sistema. La instalación y configuración se realizará conjuntamente con los miembros del departamento de Sistemas de Información de ETS, formando en la realización de las tareas tipo. Finalmente se instruirá al personal del departamento de Sistemas de ETS para la realización de tareas de mantenimiento.

Todo el proceso se realizará en las instalaciones de ETS.

Documentacion requerida para la nueva configuración:

El diagrama de topología física de la red de ETS, deberá incluir como minimo toda la documentacion generada durante el proceso de configuración, que será:

- Toda la electrónica de los cuartos técnicos que estan interconectados con los Firewalls suministrados.
- Los nuevos firewalls y aquellos que se mantienen
- Identificacion de los puertos e interfaces de conexión
- Diagrama de topología lógica de red IPv4 de ETS
- Se incluyen los elementos lógicos de la red
- Se incluyen los direccionamientos
- Pantallazos y explicaciones detalladas de toda la configuración implementada en los firewalls durante el proyecto.

Se incluirá asimismo, toda aquella información adicional no contenida en data sheets o manuales del equipamiento que sea necesaria para el correcto funcionamiento de la instalación.

El adjudicatario entregará la correspondiente documentación con el diseño y configuración del sistema. Se entregarán los procedimientos necesarios de las tareas habituales a realizar por el administrador de sistemas en ETS, por ejemplo:

- Creación de rutas
- Creación de reglas
- Identificación del tráfico de una aplicación no estándar
- "Best Practices" de configuración firewall

Las empresas licitadoras deberán contar con la correspondiente certificación del fabricante a nivel de empresa. Deberá aportarse la documentación que acredite dicha certificación.

Finalmente el adjudicatario realizará una medición del rendimiento.

Soporte del fabricante

Las licencias que sean suministradas en el presente contrato, inlcuirán un soporte de fabricante para 5 años.

Soporte del Adjudicatario:

Durante el periodo de 5 años del soporte del fabricante, el adjudicatario prestara un soporte especial adicional. Dicho soporte resolverá las dudas de configuiuraciuón a los técnicos de ETS, prestará servicios de coordinación con el soporte del fabricante, resolución de incidencias que afectan al sevicio, etc…

Se valorará la descripción detallada de dicho soporte en las ofertas, los acuerdos de nivel de servicio (SLAs), el horario de atención al cliente y sus canales y gestión de incidencias propuesto.

5.3.2 LOTE 2: DOMINIO Y ACTUALIZACIONES AUTOMATICAS

5.3.2.1 DOMINIO

Los equipos OT a integrar en el dominio serán aquellos que dispongan de un sistema operativo windows que sea compatible con un dominio de nivel funcional windows server 2016.

Trabajos previos

El adjudicatario deberá realizar un análisis e inventariado previo de los equipos suministrado por ETS y sistemas desplegados en la red de OT con el objetivo de obtener:

- Inventariado de equipos, identificando sus características y criticidades por el servicio ofrecido.
- Definición de una estructura de Unidades Organizativas exclusivas para sistemas de OT en el dominio actual de ETS basada en criticidad de sistemas, disponibilidades, posibilidad de actualización y consideraciones semejantes.

Es imprescindible la correcta definición desde la fase de diseño para poder apoyarse sobre estas estructuras en futuras operaciones propias de dominio.

- Inventario de redes pertenecientes a OT.
- Especificar la red en la que se direccionará el nuevo controlador de dominio.
- Solicitar y verificar la apertura de puertos de comunicaciones necesarios entre redes OT e IT para asegurar las funcionalidades de dominio.
- Identificar sitio físico donde residirá el nuevo servidor teniendo en cuenta equidistancias con sistemas OT, seguridad de acceso a cuartos técnicos, etc.

Union al dominio y promoción del controlador de dominio

Toda y cada una de las fases para la unión al dominio y promoción del nuevo servidor se realizarán de forma conjunta con los mantenedores del domino de ETS recogiendo toda la información necesaria y capturas para la generación de una completa documentación. A continuación se enumeran las tareas identificadas por ETS, quedando abiertos a sugerencias por parte del adjudicatario a añadir nuevos pasos.

- Instalación y activación de Windows Server 2019 Estándar.
- Instalación de antivirus.
- Ejecución de script para acotar puertos de comunicación entre DCs (proporcionado por ETS).
- Validación de comunicaciones con Maestro de operaciones de dominio y resto de controladores.
- Definición del nombre del Servidor y unión al dominio de ETS.
- Creación de nuevas Subnets en Sitios y Servicios de Directorio Activo del dominio de ETS
- Creación de nuevo Site en Sitios y Servicios de Directorio Activo del dominio de ETS y asociar las subnets previamente creadas.
- Promoción del servidor al dominio de ETS
- Creación de Unidades Organizativas previamente diseñadas.
- Creación de Grupos de Seguridad para añadir usuarios que operan en OT
- Delegar permisos sobre estas unidades organizativas y grupos de seguridad para asegurar autonomía de gestion a los técnicos OT.
- Diseño y creación de GPOs para aplicar seguridad a equipos OT. Se crearán políticas exclusivas para las unidades organizativas de equipos y grupos OT independientes del resto de los equipos de la red IT.

Instrucciones tecnicas dirigidas al mantenedor.

Todos los manuales/instrucciones tecnicas estan definidos en el punto 5.3.

Suministro de servidor fisico

El adjudicatario suministrará el servidor físico donde se instalará el nuevo controlador de dominio. Las características hardware mínimas del servidor son:

- Procesador: 1 CPU/ 10 cores / 2,4 GHz
- Memoria RAM: 32 GB DDR4 RDIMM
- 2 x Disco duro SAS de 600 GB a 12 Gb/s y 10 000 rpm en RAID 1
- Doble Fuente de Alimentación
- DVD+/-RW SATA Internal
- 2 puertos Gb Ethernet
- IDRAC/ILO de tipo Enteprice (Licencia perpetua)
- 5 años de garantía 4 Next Bussiness Day

Suministro de licencias

Se requiere que el Sistema Operativo quede licenciado correctamente según licenciamiento por Cores de Microsoft. Además el servidor tiene que ser gestionado fuera de línea a través de una ILO/IDRAC Enterprise o similar. El adjudicatario suministrará:

- 1x Windows Server 2019 Standard, 16 núcleos, instalación de fábrica, sin medios, sin CAL
- 1x IDRAC/ILO Enterprise o similar perpetua.

5.3.2.2 SCC (GESTIÓN DE ACTUALIZACIONES E INVENTARIOS)

El escenario final a lograr es la integración de los equipos Windows de OT en la infraestructura SCCM de ETS en su versión Current Branch. Se busca cumplir los siguientes aspectos:

- Homogenizar las tareas de administración y mantenimiento en el parque de endpoints OT.
- Reducción de vulnerabilidades de seguridad conocidas mediante la administración de actualizaciones.
- Realizar la configuración adecuada para maximizar el rendimiento.

Suministro de licencias para SCCM

Se requiere suministro de licencias OPEN (administración pública) para:

- Licenciar Servidores físico y virtuales gestionados por SCCM
    - 2 x System Center Datacenter 16 Core License Government, Soft. Assu.
    - 9 x System Center Standard 16 Core License Government, Soft. Assu.
- •Licenciar 70 endpoints para ser gestionados por SCCM. Licenciamiento por dispositivo (OSE):

- 70 x System Center Configuration Manager CML (Client Management), Soft. Assu.

Trabajos previos

Antes de la integración de equipos en SCCM el adjudicatario deberá:

- Especificar los requerimientos mínimos del servidor SCCM virtual en uso teniendo en cuenta el número de nuevos equipos que se van a gestionar desde la plataforma SCCM.
- Especificar los requerimientos de comunicaciones (direccionamientos, protocolos y puertos) que requiere el servidor para gestionar los agentes de todas las subredes en las que se encuentran los equipos OT a gestionar. La solución se integrará con la infraestructura existente, resolución de nombres, LDAP, etc.
- Tener definidas las Unidades Organizativas en el dominio de ETS de las que SCCM se alimentará.

Configuraciones en SCCM

La parte de configuración de SCCM se realizará de forma conjunta con el departamento de Sistemas de ETS recogiendo toda la información necesaria y capturas para la generación de la documentación correspondiente.

La empresa adjudicataria realizará las tareas necesarias en SCCM para que se cumplan los siguientes requisitos sobre los equipos OT integrados:

<u>Requisitos generales:</u>

- Inventario Hardware
- Inventario Software
- Distribución de Software
- Device Compliance (Cumplimiento de dispositivos)
- Distribución de actualizaciones
- Centro de software
- Remote control y herramientas de administración remota
- Reporting (Consultas e informes)

<u>Requisitos funcionales:</u>

- Integración con directorio activo para generación de colecciones basadas en Unidades Organizativas. El adjudicatario creará la estructura de colecciones necesaria para despliegues de actualizaciones y software. Estas dependerán de la criticidad, disponibilidad y ventanas de mantenimiento de los sistemas OT previamente inventariadas y definidas. La gestión y visualización de estas colecciones estará basada en roles.

- Disponibilidad centro de software. Se deberá monitorizar las actualizaciones disponibles y previamente instaladas.
- El proceso de transferencia de elementos deberá impedir que se produzcan redistribuciones de software previamente distribuido.
- Programación horaria para instalación y actualización de software. Se tiene que asegurar el cumplimiento de las ventanas de mantenimiento.
- Despliegue de software y actualizaciones automáticas basado en dispositivo. Podrán ser requeridos, disponibles o no actualizables. La definición y configuración de los tipos de actualizaciones a descargar/desplegar será a cargo del adjudicatario.
- Administración y generación de informes basada en roles.
- El personal mantenedor de los sistemas será capaz de administrar remotamente los equipos cliente con interacción/permiso por parte del usuario y trazabilidad de las acciones realizadas.

Requisitos de Seguridad

- Administración de SCCM basada en roles. La solución deberá asegurar que los distintos roles administrativos no se interfieren en sus operaciones. Los técnicos de la red OT podrán consultar y actuar todos los equipos de la red OT de manera autónoma. La configuración actual de los equipos IT debe interferir en la configuración de los equipos OT.
- Se deberá tener capacidad de registro de las acciones realizadas en los servidores, a nivel de configuración y despliegues.
- Se realizara un modelo de configuración a nivel de seguridad para los servidores Windows de modo que puedan presentar resistencia a ataques desde la propia red interna (bastionado).
- La herramienta de control remoto debe pedir autorización, debe dejar un log de acciones y debe dejar una clara indicación visual de que se está accediendo.
- Se mantendrá la política actual existente en ETS, en la que los usuarios no tendrán derecho de administrador local del equipo.
- Cumplimiento de normativas legales.

Despliegue de los agentes

El adjudicatario definirá, configurará y desplegará los agentes de todos los equipos soportados por SCCM current Branch.

Instrucciones tecnicas dirigidas al mantenedor

El adjudicatario creará procedimientos indicados en el punto 5.3 del pliego.

5.3.3 LOTE 3: ANTIVIRUS

El contratista deberá suministrar las siguientes licencias para los próximos 2 años:

- 291 licencias Kaspersky EndPoint Security for Business – Advanced.
  - 43 unidades de Kaspersky Endpoint Security for Linux
  - 212 unidades de Endpoint Security for Windows
  - 36 unidades Kaspersky Security 11 for Windows Server
- 178 unidades de Kaspersky Embedded Systems Security

Además, se deberá contratar la extensión del licenciamiento actual de 330 Kaspersky Endpoint Security for Business Advanced European Edition hasta la fecha de fin de las nuevas licencias suminitradas.

Las características de las licencias actuales son las siguientes (finalizan el 11 de julio de 2022):

- Kaspersky Endpoint Security for Business - Advanced European Edition. 250-499 Node 2 year Governmental Renewal License (número: 93AAF8F1B83A4F9FA3BF4528CCF9C8AD) Restricción: 330
- Kaspersky Endpoint Security for Business - Advanced European Edition. 250-499 Node 3 year Governmental Renewal License: Kaspersky Security for WS and FS (número: 1FF8-000451-4B5309CE) Restricción: 330
- Kaspersky Endpoint Security for Business - Advanced European Edition. 250-499 Node 2 year Governmental Renewal License: Security Center (número: 1FF8-0003F9-4B5309CD) Restricción: 330

Integracion con la actual consola Kaspersky

El adjudicatario deberá integrar 20 equipos de la red OT seleccionados durante el proyecto en el sistema de protección Kaspersky security center actual de ETS, teniendo en cuenta:

- Añadirá los nuevos equipos a un repositorio independiente de la consola Kaspersky Security Center actualmente instalada.
- Tendrá en cuenta que el direccionamiento de las redes de los nuevos equipos a integrar son diferentes al del servidor de antivirus y deberán habilitarse las comunicaciones estrictamente necesarias en los equipos de comunicación intermedios para filtrar el tráfico asociado al antivirus.

Para ello el adjudicatario creará con la colaboración con los actuales mantendedores de ETS de la consola Kaspersky un servidor de administración secundario (servidor de administración virtual, en nomenclatura de Kaspersky), que presentará como un nodo distinto de KSC dentro de la misma consola MMC. Este servidor administrará

únicamente los equipos contemplados de la red OT, y futuros equipos de la red OT que se integren en el futuro.

Autonomía en labores administración

La configuración de la consola Kaspersky permitirá dotar de total autonomía a los técnicos de la red OT en los equipos de su propia red: consulta y monitorización de equipos infectados o sin protección adecuada, actualización del producto, distribución de firmas, revisión de informes, acceso a la cuarentena...

Para ello creará un nuevo perfil de acceso a la administración de la consola específico para la gestión de equipos de la red OT.

Creación de tareas dentro del servidor de administración secundario.

El adjudicatario deberá crear como mínimo las siguientes tareas dentro del servidor de administración secundario:

- Actualización de firmas para Endpoint: Actualizar
- Actualización de firmas para Linux
- Actualización de firmas para Servers: Database Update
- Actualización de firmas para Embedded
- Análisis antivirus para Endpoint
- Análisis antivirus para Embedded
- On-Demand file integrity scan para Linux
- On-Demand Scan para Servers

Protección	N equipos	Sistema operativo
Kaspersky Endpoint Security for Linux	5	Distr. Linux
Kaspersky endpoint security 11	5	Windows 7 Professional Windows 10
Kaspersky Embedded Systems Security	5	Windows XP Windows 7 Embedded Standard SP1
Kaspersky Security 11 for Windows Server	5	Windows Server 2003 Windows Server 2008 Wndows Server 2012 Windows Server 2016

Instalación de protección y agente e integración en la consola

El adjudicatario instalará la protección adecuada en función el sistema operativo a un conjunto de 20 equipos propuestos por ETS. Estos equipos deberán ser:

Se instalará el paquete de protección junto con el agente a este listado de equipos. El adjudicatario realizará y probará el procedimiento de instalación/desinstalación que viene descrito en el punto 5.3.

Se trata de un aspecto clave en el proyecto, ya que dicho procediminto lo ejecutarán en el futuro cada uno de los mantenedores de los sistemas OT, según las instrucciones que le facilite el adjudicatario.

Se comprobará la correcta integración con la consola de administración del equipo protegido: se comprobará que la consola lo visualiza en el árbol de dispositivos administrados y refleja el estado de protección y propiedades tales como registro de aplicaciones, tareas, registro de hardware, vulnerabilidades de software y actualizaciones disponibles.

Se designará durante el proyecto un equipo como punto de distribución: un equipo con Agente de red instalado que se utiliza para la distribución de actualizaciones, la instalación remota de aplicaciones y la recuperación de información relativa a dispositivos en red. Se creará a través del equipo elegido el punto de distribución del servidor de administración. Dicha configuración aprovechará al máximo el ancho de

banda existente entre las redes IT/OT. Se ejecutarán satisfactoriamente las tareas creadas en el paso previo a los equipos protegidos.

- Se comprobará en estos equipos que el icono de Kaspersky de la barra de tareas abre una consola local.
- se comprobará que muestra el estado de actualización de las bases de datos.
- Se comprobará que pide credenciales para pausar la protección
- Se comprobará que pide credenciales para desactivar la directiva.
- Se introducirán las credenciales deshabilitar la directiva y realizar una actualización manual.
- Se introducirán las credenciales para pausar la protección manual.
- Se procederá a realizar un escaneo manual.

Instalación de consola administración local servidores

El adjudicatario deberá instalar en local en los Sistemas operativos Windows Server la consola local de administración.

Al acceder al icono de Kaspersky de la barra de tareas, se comprobará que se abre el panel de control de Kaspersky, y que muestra el estado de las bases de datos.

Se procederá a realizar un escaneo manual.

Documentación para el mantenedor

El adjudicatario deberá proporcionar al mantenedor de los equipos OT la autonomía y las instrucciones necesarias para poder instalar a los equipos tanto la protección adecuada como el agente para poder conectar con la consola Kaspersky Security Center.

Procedimiento instalación/desinstalación:

Partiendo de una carpeta compartida que suministrarán los técnicos de ETS, en la que se almacenará la última versión del paquete de protección y agente a instalar, el adjudicatario deberá procedimentar de manera clara y gráfica los pasos a seguir para una correcta instalación del producto. Esta información tiene como objetivo entregarse al mantenedor de los equipos, para la instalación en equipos no protegidos.

Procedimiento actualización:

Partiendo de una carpeta compartida que suministrará el departamento de sistemas, en la que se almacenará la última versión del paquete de protección y agente a instalar, el adjudicatario deberá procedimentar de manera clara y gráfica los pasos a seguir para una correcta actualización del producto. Esta información tiene como objetivo entregarse al mantenedor de los equipos, para la actualización del producto.

Documento de requisitos:

El adjudicatario deberá documentar los requisitos necesarios y recomendados para instalar los 4 tipos de protección (Endpoint, Embedded, Linux y Server):

- Sistemas operativos soportados
- Espacio mínimo en disco
- RAM
- Procesador mínimo
- Requisitos software

5.4 ACTUALIZACIÓN DE LAS POLÍTICAS SEGURIDAD ETS

El contratista deberá actualizar las políticas de seguridad de ETS incorporando las medidas de ciberseguridad que identifique como necesarias para su aplicación en la red de explotación de ETS, que podrán incluir:

- Actualización de sistema operativo sin soporte
- Actualización de versiones de software y firmware
- Actualización de parches de seguridad
- Actualización de protocolos, como es el caso del protocolo de recuperación ante desastres

Si el contratista observara alguna incomaptaiblidad entre los procedimientos de las políticas de seguridad de ETS y la nueva implementación objeto de este pliego, deberá realizar las propuestas de actualización generando las nuevas versiones de los procedimientos que así lo requieran.

Se revisarán todas las instrucciones técnicas, manuales y documentos generados según se recogen en el alcance d elos trabajos de cada uno de los lotes.

El contratista deberá realizar al menos las siguientes instrucciones técnicas y manuales:

5.4.1 BASTIONADO DE EQUIPOS

Procedimiento que describa por cada uno de los sistemas operativos instalados en la red OT, recomendaciones de configuración, directivas locales o limitaciones de ejecución para reducir el riesgo de ciberseguridad.

El destinatario de dicho documento será cada un de los mantenedores de los sistemas OT.

5.4.2 SEGURIDAD EN APLICACIONES

Nueva instrucción que recomiende a nivel de aplicación la utilización de protocolos seguros (o versiones revisadas) por parte de todos los subsistemas que se integran

en la red de OT. Su aplicación corresponde al desarrollador/mantenedor de cada subsistema.

5.4.3 BACKUP LOCAL Y CONTINUIDAD DE NEGOCIO

Procedimiento que incluya la política de backup general que se debe aplicar a un equipo para configurar un backup manual local programado con los ficheros/BD que incluyan la configuración y datos de los sistemas. Dicho documento recomendará las pautas para configurar el script/backup local en cada uno de los sistemas operatvos.

Procedimiento que describa los puntos deben contener los manuales de instalación y recuperación de backup de cada un de los sistemas OT, que sirva como procediminto de continuidad de negocio a partir de una maquina sin sistema operativo. Dicho procedimiento servirá de plantilla a los mantenedores de los sistemas OT, que ampliaran dicho procedimiento con los detalles del sistea OT que mantienen.

5.4.4 ANTIVIRUS

Partiendo de una carpeta compartida que suministrarán los técnicos de ETS, en la que se almacenará la última versión del paquete de protección y agente a instalar, el adjudicatario deberá procedimentar de manera clara y gráfica los pasos a seguir para una correcta instalación del producto. Esta información tiene como objetivo entregarse al mantenedor de los equipos, para la instalación o actualización del producto, según estén los equipos protegidos o se requiera suactualizacion, respectivamente.

5.4.5 SCCM Y DOMINIO

El adjudicatario de este lote, deberá crear una Instrucción Tecnica que contenga toda la documentación detallada para que el mantenedor o responsable del sistema integrado en la red OT pueda unir los equipos al dominio OT.

También se creará una nueva Instrcción técnica que indiqeu la política de actualizaciones de los equipos de la red OT:

- Politica de actualizaciones según criticidad del sistema y sistema operativo del dispositivo.
- El modo que se deben realizar las actualizaciones manuales a través de la herramienta de distribución "Centro de Software" para aquellos S.O. soportados del entorno Microsoft
- como incorporar un nuevo equipo en SCCM explicando de forma detallada los pasos a realizar para el despliegue de un nuevo equipo en la red OT unión en Dominio y su integración en SCCM
- Cual es el ultimo nivel de actualización que deben deben tener aquellos sistemas opertaivos no soportados del entorno microsoft.

- El modo de actualización y la configuración proxy que deben tener los sistemas operativos Linux.

Se requerirá al adjudicatario de este lote, una guía detallada del proceso de actualización del sistema y su comprobación. Se diferenciará entre actualizaciones disponibles y requeridas, indicando para estas últimas las ventanas de mantenimiento previamente establecidas.

5.5 CONTROL DE RESULTADOS

Tras la actualización de las medidas de seguridad, el contratista deberá verificar su resultado. Para ello, deberá aplicar todos los procedimientos que considere necesarios y que permitan comparar la situación final con la situación de partida identificada en el informe de auditoría. En caso de que en esta fase, se detecten nuevas vulnerabilidades no identificadas previamente, el contratista lo deberá notificar a ETS y proponer las medidas que considere necesarias.

Esta fase implicará al contratista realizar pruebas conocidas como pentesting mediante las que se logra exponer vulnerabilidades a través de ataques "provocados" a la red:

- Pruebas de pentesting de la infraestructura interna. Estas pruebas se deberán realizar mediante un equipo conectado a la red de explotación que simularán un ataque interno o externo. El contratista deberá emplear metodologías habituales para este tipo de pruebas como es OSSTM (Open-Source Security Testing Methodology).
- Pruebas de pentesting de la infraestructura externa que consistirán en tests de intrusión conforme a metodología como OWASP (Open Web Application Security Project)

Adicionalmente deberá utilizar sondas activas de control que permitan identificar en tiempo real posibles intrusiones en la red. Podrán ser software o hardware y permitirán detectar tráfico anómalo de la red, detectar posibles indicios de ataques, etc.

El contratista deberá culminar esta fase con la redacción de un informe que refleje la situación final de la red de explotación de ETS.

5.6 DOCUMENTACIÓN Y FORMACIÓN

El contratista deberá a entregar a ETS toda la documentación resultado de la implantación realizada, incluyendo:

- Actualización de la topología física y lógica de la red de ETS
- Datasheets de los equipos implantados
- Documentación de diseño y configuración del sistema

- Documentación funcional de los aplicativos implantados
- Procedimientos para las tareas habituales por el administrador de la red de explotación de ETS:
    - Creación de rutas
    - Creación de reglas
    - Identificación de tráfico de una aplicación "no estándar"
    - Mejores prácticas para la configuración de los equipos
    - Procedimiento para restablecer una configuración mal aplicada
    - Procedimiento para renovación de certificados y licencias

Toda información adicional que sea necesaria para el correcto funcionamiento de la instalación.

Adicionalmente, durante todo el proceso de instalación, configuración, y pruebas, el adjudicatario transferirá el conocimiento necesario a los técnicos de ETS para que estos sean autónomos en la gestión del nuevo sistema.

La formación comenzará con una sesión inicial, previa a la configuración del sistema.

La instalación y configuración de los aplicativos identificados se realizará conjuntamente con las personas que ETS determine, formando en la realización de las tareas tipo y de mantenimiento.

Todo el proceso se realizará en las instalaciones de ETS.

5.7 SOPORTE DEL ADJUDICATARIO

El contratista deberá llevar a cabo el soporte asociado a la implantación de las medidas de seguridad indicadas, en lo referente a los lotes 1 y 2 de la presente licitación, como pueden ser:

- Monitorización de los sistemas y elementos que componen la red de explotación, atendiendo a eventos y alarmas generados en la red:
    - Estado de las máquinas
    - Estado de la CPU
    - Estado de la memoria
    - Error de paquetes
    - Sesiones
    - Etc.
- Realización periódica de verificaciones de ciberseguridad
- Propuesta de implantación de medidas para las vulnerabilidades adicionales que se hayan identificado
- Operación remota de la plataforma en 10x5 o en horario nocturno si la actuación pudiera afectar a la disponibilidad del servicio ferroviario:

    - Se realizarán todas las tareas de gestión necesarias para el mantenimiento de la nueva plataforma ya definida:
      -Modificación de reglas
      -Modificación de perfiles de acceso
      -Aplicación de la solución ante incidencias
      -Actualización y parches
    - La operación será realizada de forma peticionada por ETS o consensuado entre ambas partes cuando el adjudicatario lo proponga de forma proactiva. Todas las tareas que pudieran suponer un riesgo para la disponibilidad del servicio ferroviario, tendrán que ser realizadas en horario nocturno.
- Actualizaciones de los diferentes sistemas incluidos en este servicio:
    - Estas intervenciones se podrán realizar en horario laboral (8x5) o en una franja horaria en la que no haya servicio ferroviario en caso de poderse ver éste afectado, minimizando al máximo los cortes del servicio. Se procederá de la siguiente forma:
      -Se acordará con ETS la fecha para la actualización y se le explicará las implicaciones que tiene.
      -Ejecución de la actualización sobre la solución y verificación del correcto funcionamiento del servicio.
      -Notificación a ETS de la finalización del proceso de actualización
- Aplicación de medidas extraordinarias contra amenazas
- Informes de servicio trimestrales en los que se reflejará el estado de la red y las recomendaciones de mejora

Todas estas actuaciones se deberán llevar a cabo de forma coordinada con ETS y con su previa autorización y se podrán prolongar por un plazo de 3 años desde la fecha de finalización de la implantación de las medidas indicadas en este pliego.

Este servicio se prestará bajo un modelo de provisión de servicios en el que la gestión y la realización de actividades será responsabilidad del adjudicatario y la prestación del servicio está basado en SLOs (Service Level Objective), de forma que, en el transcurso de su horario de atención, el objetivo de equipo de soporte del adjudicatario será responder ante una incidencia o consulta, en un tiempo máximo establecido:

Alerta	**Riesgo de Impacto**	**Tiempo máximo de respuesta**
Alta	Caída del servicio	<= 1 hora
Media	Servicio en riesgo	<= 4 horas

Baja	Bajo rendimiento	<= 16 horas
Consulta	Asistencia General	<= 24 horas

Cualquier actuación realizada por el contratista supondrá la actualización por su parte de la documentación correspondiente.

6 GARANTÍA

Todo el equipamiento propuesto se deberá ofrecer con una garantía de dos (2) años y con un tiempo mínimo de cinco (5) años en el que los fabricantes deberán disponer de piezas de repuesto para garantizar su reparación.

7 CERTIFICACIONES

Las personas incluidas en el equipo de trabajo de la propuesta deberán contar con las certificaciones del fabricante de los productos propuestos en su oferta o, en su defecto, la empresa licitante deberá aportar carta de compromiso de la contratación de los servicios profesionales del fabricante correspondiente.

Adicionalmente las empresas dispondrán de las siguientes certificaciones:

- ISO27001 y ISO20000-1

Asimismo, se requiere que al menos uno de los recursos que participen en la ejecución de los trabajos cuente con la siguiente certificación:

- CISSP: Certified Information Systems Security Professional o equivalente

Esta certificación se solicita al realizar actuaciones de Seguridad sobre la red OT que está compuesta por equipos sensibles que directamente intervienen en la explotación.

8 PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo máximo para la realización de los trabajos objeto del presente pliego es el indicado en el apartado 6 de la carátula.

9 PRECIOS DE CONTRATO

Los concursantes fijarán los precios unitarios designados en el anexo conforme al modelo de presupuesto desglosado en el Anejo III.2 del PCAP [VER ANEJO 12 DE ESTE PLIEGO], que serán de aplicación para su abono en las correspondientes certificaciones, no sufriendo variación por concepto alguno.

Estos precios serán de contrata, de modo que en ellos estén incluidos todos los beneficios, cargas sociales, gastos, impuestos, excepto IVA, etc.

Con la oferta se entregará además la proposición económica según modelo del Anejo III.1 del PCAP.

10 VALORACIÓN Y ABONO DE LOS TRABAJOS REALIZADOS

La valoración y abono de los trabajos realizados por el Contratista se efectuará por certificaciones mensuales en función del avance de los trabajos de cada uno de los apartados desglosados.

Antes del día 20 de cada mes el adjudicatario indicará al Responsable del Contrato una medición del avance previsto en cada tarea al terminar el mes en curso. Una vez aceptada dicha medición, antes del último día del mes, el adjudicatario enviará la hoja de mediciones firmada para su validación, y emitirá la correspondiente factura digital por el importe acordado.

11 PRESUPUESTO DEL CONTRATO

El Presupuesto máximo de licitación, IVA NO incluido, es el indicado en el apartado 3 de la Carátula del concurso

12 ANEJO: CUADRO DE PRECIOS

Id.	LOTE 1: PROTECCION DE RED OT	Med.	Precio Unitario	Importe
1.1	Equipamiento Perimetral Suministro, instalación, configuración, integración, pruebas y puesta en marcha de firewall + IDS/IPS en perímetro, según especificaciones técnicas. Incluso test para garantizar la operación en el entorno de alta disponibilidad.	2		
1.2	Actualizacion de políticas y procedimientos	1		
1.3	Control de resultados	1		
1.4	Soporte anual	5		
			TOTAL LOTE 1	**75.000,00 €**

Id.	LOTE 2: SERVICIO DE DOMINIO	Med.	Precio Unitario	Importe
2.1	servidor físico + licencia windows server OEM + ILO/iDRAC + instalación fisica	1		
2.2	SCCM Licencias CML (Client Management Licence) Government. Software Assurance 2 year	70		
2.3	SCCM: Licencias ML Server Standard Government (16cores) Software Assurance 2 year	9		
2.4	SCCM:Licencias ML Server Datacenter Government (16cores) Software Assurance 2 year	2		
2.5	Configuracion e implementacion del servicio	1		
2.6	Actualizacion de políticas y procedimientos	1		
			TOTAL LOTE 2	**30.000,00 €**

Id.	LOTE 3: SOFTWARE ANTIVIRUS	Med.	Precio Unitario	Importe
3.1	Antivirus: Extensión 330 Licencias KAS ADV hasta fin de caducidad licencias adicionales	1		
3.2	Antivirus: 291 Licencias adicionales KAS ADV 2 Años	291		
3.3	Antivirus: Kaspersky **Embedded** Systems Security 2 Year	178		
3.4	Actualizacion de políticas y procedimientos	1		
			TOTAL LOTE 3	**35.000,00 €**