

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
4. ANTECEDENTES, DOCUMENTOS DE REFERENCIA Y PLANTEAMIENTO GENERAL.....	4
5. TRABAJOS A REALIZAR POR EL CONTRATISTA	9
6. GARANTÍA	20
7. CERTIFICACIONES	21
8. PLAZO DE EJECUCIÓN DE LOS TRABAJOS	22
9. PRECIOS DE CONTRATO.....	23
10. VALORACIÓN Y ABONO DE LOS TRABAJOS REALIZADOS	24
11. PRESUPUESTO DEL CONTRATO	25

ANEJO: CUADRO DE PRECIOS

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, el 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

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 (Information 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 prácticas 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.

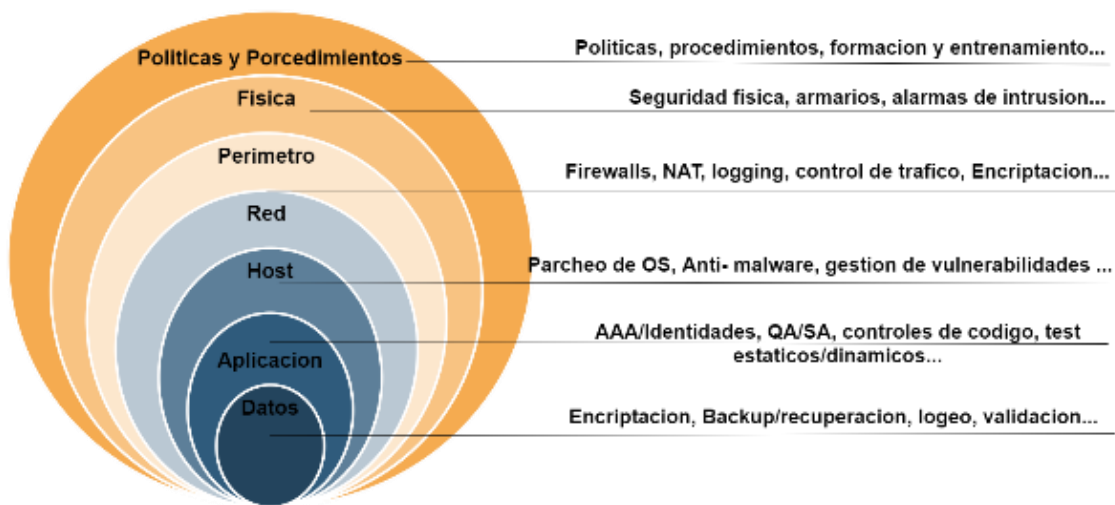


Figura 1: Arquitectura de defensa en profundidad

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 requisitos de los nuevos sistemas implantados.

4.6. DOMINIO Y ACTUALIZACIONES DE SISTEMA OPERATIVO

La red IT de ETS dispone de la plataforma SCCM 2016, que gestiona el inventario del software instalado, el inventario de hardware, despliegue de sistemas operativos 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 específicas para los dispositivos OT y su software específico 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 aplicaciones de la red OT con el dominio 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 incluidos 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
- Actualización de las políticas de seguridad de ETS
- Control de los resultados
- Documentación 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

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. Dominio y actualizaciones automáticas

5.3.1.1. 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.

Unión 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 dominio 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 gestión 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 técnicas dirigidas al mantenedor.

Todos los manuales/instrucciones técnicas están definidos en el punto 5.3.

Suministro de servidor físico

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 Enterprise (Licencia perpetua)
- 5 años de garantía 4 Next Business 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.

5.3.1.2. 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:

Requisitos generales:

- 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)

Requisitos funcionales:

- 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 realizará 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 técnicas dirigidas al mantenedor

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

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 incompatibilidad 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 de los 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 uno 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 operativos.

Procedimiento que describa los puntos deben contener los manuales de instalación y recuperación de backup de cada uno de los sistemas OT, que sirva como procedimiento de continuidad de negocio a partir de una máquina sin

sistema operativo. Dicho procedimiento servirá de plantilla a los mantenedores de los sistemas OT, que ampliarán dicho procedimiento con los detalles del sistema OT que mantienen.

5.4.4. SCCM y Dominio

El adjudicatario de este lote, deberá crear una Instrucción Técnica 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 Instrucción técnica que indique la política de actualizaciones de los equipos de la red OT:

- Política 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 último nivel de actualización que deben tener aquellos sistemas operativos 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.

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.

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 licitadores 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 pliego.

ANEJO: CUADRO DE PRECIOS

Id.	SERVICIO DE DOMINIO	Med.	Precio Unitario	Importe
2.1	Servidor físico + licencia windows server OEM + ILO/iDRAC + instalación física	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	Configuración e implementación del servicio	1		
2.6	Actualización de políticas y procedimientos	1		
	TOTAL			50.000,00 €