

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA RENOVACIÓN TECNOLÓGICA DE LOS ACTUALES EQUIPOS DE LA RED ATENDIENDO PRINCIPALMENTE A NECESIDADES Y CRITERIOS DE DISEÑO JUNTO A LA ADECUACIÓN DE LA CONECTIVIDAD DE FIBRA DE LAS DISTINTAS UBICACIONES, ASÍ COMO UN SOFTWARE DE GESTIÓN DE LA RED Y DE SEGURIDAD Y CONTROL PARA SERVICIOS DE TXINGUDI-TXINGUDIKO ZERBITZUAK, S.A.

Código de Expediente: 2022SUM002

1. OBJETO DEL CONTRATO

El objeto de la presente licitación es la renovación tecnológica de los actuales equipos de la red de Servicios de Txingudi atendiendo principalmente a necesidades y criterios de diseño (topología de la red). Esta renovación implica adecuación de la conectividad de fibra de las distintas ubicaciones, así como un software de gestión de la red y de seguridad y control de Servicios de Txingudi – Txingudiko Zerbitzuak, S.A. (en adelante Txinzer).

Todo ello de conformidad con lo previsto en el presente Pliego y en el Pliego de Cláusulas Económico- Administrativas.

2. SITUACIÓN ACTUAL

La red actual de Txinzer consta de equipos ya llegados a su fin de vida y en los mismos se ofrecen los siguientes servicios:

- . Servicios de comunicación de datos básico entre las distintas sedes de la Organización, así como acceso al CPD
- . Servicios de vídeo
- . Servicios de ToIP
- . Interconexión con solución wifi

Debido a que los modelos de switches de diferentes sedes de Txingudiko Zerbitzuak están ya descatalogados, y ya no soportan evolución ni actualizaciones, se estima necesario realizar la migración de la electrónica de red de los nodos de comunicaciones ubicados en entorno oficinas. Para ello se plantea el cambio del equipamiento de electrónica de red de las siguientes ubicaciones:

- . Perujaran nodo planta primera (servidores)
- . Perujaran nodo planta 0
- . Perujaran FCC
- . OAP
- . EDAR armario principal

. ETAP armario principal

El diagrama de red actual se muestra en el anexo 1.

Perujaran Nodo Planta 0 (baja)

Actualmente el rack de planta baja de Perujaran hace de concentrador de los enlaces de fibra monomodo que llegan de las sedes remotas Oficina de Atención al Público (OAP), EDAR y ETAP, además de los armarios de comunicaciones FCC y Talleres FCC que se encuentran en la sede de Perujaran, y están unidos por fibra monomodo. En este pliego, se plantea cambio de la velocidad de conexión y equipamiento de FCC, pero no así de Talleres FCC. No obstante, hará falta puerto de conexión para Talleres FCC a 1Gbps en la nueva electrónica.

Las velocidades de todas estas sedes son de 1Gbps a excepción de OAP que es a 10Gbps. En el nodo de Planta Baja de Perujaran se cuenta con un switch Hp ProCurve 5412 zl y además de las conexiones de fibra cuenta con 168 puertos 1Gbps con PoE. Este nodo se conecta al nodo de planta primera de Perujaran por medio de dos enlaces de 10Gbps cada uno.

Perujaran nodo principal (planta 1ª)

En este nodo se cuenta con un Hp ProCurve 5406R con la unión a 20Gbps con la planta baja del mismo edificio. Del mismo modo, en dicho nodo se conectan los diferentes servidores de Txinzer, teniendo 48 puertos 1Gbps

Perujaran FCC

Cuenta con un switch HP ProCurve 2530-48G con puertos PoE, unido a 1Gbps con el rack de planta 0 de Perujaran.

OAP

Se cuenta en la actualidad con un Aruba 2930M-48G-PoE+ con una unión a 10Gbps con el nodo de planta 0 de Perujaran, y una unión a 1Gbps con una rama de Txinzer que no aplica en esta licitación.

EDAR

Cuenta con dos switches HP Procurve 3500-24G unidos entre sí y una unión a 1Gbps con el nodo de planta primera de Perujaran.

Además de eso, cuenta con dos puertos de 1Gbps de fibra para unión a dos nodos secundarios de la sede (PLC1 y PLC2) que no aplican en este pliego, pero a los que hay que seguir manteniendo conectividad a 1Gbps LX.

ETAP

Se cuenta con un HP Procurve 5406zl con 72 puertos más un switch Aruba 2530 8G PoE+. Cuenta con una unión a 1 Gbps con el nodo de planta 0 de Perujaran.

Además de eso, cuenta con dos puertos de 1Gbps de fibra para unión a dos nodos secundarios de la sede (Elordi y Reactivos) que no aplican en este pliego, pero a los que hay que seguir manteniendo conectividad a 1Gbps LX.

Gestión y Monitorización

En la actualidad no se cuenta con plataforma específica de gestión para el networking. El entorno inalámbrico cuenta con 51 suscripciones a Aruba Central para APs y 3 para dispositivos UXI (User Experience Insight).

Para monitorización se utiliza una plataforma Pandora FMS Enterprise

Control de acceso

En la actualidad se aplica en el entorno inalámbrico por medio de Clearpass, es idea ampliarlo al entorno cableado. Se tienen actualmente 200 licencias NL AC (2 paquetes de 100 JZ400AAE) y un servidor virtual Cx000V VM (JZ399AAE).

3. ALCANCE DEL PROYECTO

Txinzer necesita abordar un proyecto para adecuar la electrónica de red de sus distintas sedes (Perujarán (3) , Oficina de Atención al Público, EDAR y ETAP) que le permita implementar en su red estabilidad, resiliencia y seguridad, así como estar preparada para nuevas necesidades futuras como puedan ser la hiperconvergencia, VDI, etc.

Las principales necesidades a cubrir son:

- Mejorar la infraestructura de fibra óptica que comunica los nodos de planta 0 y planta primera de Perujaran
- actualización de la red tecnológicamente de acuerdo a las nuevas tendencias y estándares de mercado
- homogeneizar la red a nivel de tipología de equipos y fabricantes, mejorando la actual administración y gestión de la red
- Estructurar y articular la red lógica en redes virtuales (VLANs) que podrán ser enrutadas entre sí en cualquier switch de nivel 3

- Ampliación de los anchos de banda de los enlaces troncales de fibra óptica, actualizando los enlaces posibles mínimo a tecnología 10 Gigabit Ethernet
- Solución de alta disponibilidad y rendimiento automático en aquellas uniones múltiples entre equipos, sean swiches, servidores...
- Incorporar un Sistema de Gestión de Red que centralice la capacidad de monitorizar, gestionar configuraciones, gestionar firmware y generar estadísticas de todos los equipos de la nueva electrónica de red. Así mismo, este sistema deberá integrarse con el sistema de monitorización del entorno wifi
- Incorporar control de acceso al medio en el entorno cableado

El nuevo equipamiento deberá estar basado en estándares y recomendaciones internacionales.

El proyecto deberá recoger un detalle profundo de la propuesta incluyendo: características del equipamiento, arquitectura de la solución (topología), software, licencias, plan de migración e implantación, y funcionamiento en el sistema de control de acceso con el que cuenta la Propiedad.

4. REQUISITOS DE LA SOLUCIÓN

La propuesta deberá presentar una solución que optimice el tránsito de la información en la red, no solo debido a las velocidades de comunicación de los enlaces, sino teniendo también en cuenta las redundancias, altas disponibilidades y topología propuesta.

Pensando en las funcionalidades de la solución, la integración de las redes cableadas e inalámbricas y la evolución de las mismas en cuanto a funcionalidades a futuro, una condición a cumplir por el fabricante del equipamiento y los diferentes softwares será que todos los componentes a suministrar deberán ser de marca líder y reconocida en el mercado, cuyos fabricantes certifiquen la continuidad de la gama o familia de los mismos, durante los períodos de entrega que se establezcan, sin que se produzcan cambios que puedan afectar a la arquitectura de red de Txinzer. Se entenderá a modo de referencia marca líder las que se encuentran en el “Magic Cuadrante de Gartner” en el apartado de líderes en las 3 últimas ediciones en cuanto a acceso cableado e inalámbrico.

Además de ello, el software de conmutación deberá proporcionar automatización, analítica distribuida, seguridad y alta disponibilidad en las redes de campus y de centro de datos. Segmentación basada en políticas y/o directivas y a las capacidades de Inteligencia Artificial

Además, el equipamiento incluido en la solución debe cumplir con los siguientes requisitos:

- Presencia en el catálogo de CPSTIC CCN
- Todas las funcionalidades deben estar disponibles e incluidas desde el primer día.

- Ninguna funcionalidad debe estar limitada o restringida en base a licencia o en base a limitación de prestaciones.
- El equipo no debe requerir ninguna clave de activación o licencia para funcionar.
- El reemplazo de un equipo por otro de sustitución en caso de avería debe poder hacerse sin requerir ningún procedimiento administrativo de traspaso de licencia o similar.

Para cumplir con los requisitos necesarios, el proyecto y valoración deberán incluir la renovación de todos los elementos que se consideren necesarios como armarios, fibras, paneles de parcheo...), así como todos los servicios derivados de ello, además de lo exigido en este documento. El proyecto presentado será un proyecto llave en mano.

FIBRA ÓPTICA

El proyecto debe incluir una nueva comunicación de 48 hilos de fibra óptica monomodo entre los racks de planta 0 y planta primera de Perujaran en un único panel en cada extremo.

ELECTRÓNICA DE RED

La nueva electrónica de red propuesta deberá cumplir con:

- Mayor capacidad de proceso y throughput que los equipos actuales.
- Todos los equipos deben ser non blocking.
- Aumentar la velocidad de los enlaces de backbone, mínimo a 10 Gbps entre armarios, en la mayoría como se detalla más adelante con uniones múltiples de este tipo entre diferentes nodos.
- Puertos de servidor mínimos:
 - 33 puertos 1000BaseT
 - 12 puertos a 10Gbps en cobre
- Cubrir el número de puertos necesarios 10/100/1000 Mbps en los switches de acceso, se detallan más adelante
- El ciclo de vida futura de la electrónica deberá ser al menos de 5 años.
- Soporte de fabricante a 3 años en NBD y actualizaciones de firmware incluidas por el mismo periodo
- Todos los componentes (módulos, transceivers, etc.) deben ser oficiales del fabricante, no serán válidos los compatibles
- Motor de análisis de red para detección de los problemas por parte del switch para su solución y análisis a alta velocidad

MONITORIZACIÓN Y GESTIÓN

La oferta deberá contemplar la solución de monitorización del equipamiento propuesto. Deberá permitir monitorizar, gestionar y resolver incidencias desde el mismo en caso de pérdidas de conectividad, caída de un equipo con alertas...

- La herramienta de gestión y orquestación permitirá:
 - Antes de aplicar una nueva configuración en los equipos, se comprobará, en una copia paralela de la configuración actual de los equipos, la validez de la nueva configuración.
 - Antes de aplicar una nueva configuración en los equipos se comprobará, en tiempo real, que los cambios introducidos cumplen con las normas de conformidad corporativas. Esto se realizará en base al modelo de equipo, capa de la red, versión de software, o cualquier otro atributo o etiqueta asignado a los equipos
 - Una vez aplicada una nueva configuración, la herramienta chequeará el estado de diferentes protocolos y funcionalidades, en base al modelo de equipo, capa de la red, versión de software, o cualquier otro atributo o etiqueta asignado a los equipos, antes y después de aplicar la nueva configuración, permitiendo hacer un “rollback” de los cambios en tiempo real.
 - Se permitirá la notificación de las alarmas o eventos producidos en tiempo real:
 - Caídas de equipos, interfaces...
 - Cambios en la configuración de los equipos, incluyendo desviaciones con respecto a las reglas de conformidad de las mismas
 - Configuraciones no guardadas...

Del mismo modo deberá visibilizar el tráfico, identificar problemas de red y generar informes y dar datos en tiempo real del uso de aplicaciones en la red.

Txinzer cuenta en la actualidad con la herramienta de gestión Aruba Central para gestionar todo su entorno inalámbrico que consta de 51 dispositivos AP, y 3 equipos User Experience Insight (R3R67A).

En la Propuesta deberá incluir las licencias a 3 años del nuevo equipamiento, además de los 51 APs actuales comentados, así como para los 3 dispositivos UXI .

Dentro del alcance del proyecto debe estar incluida toda la parametrización de la solución.

CONTROL DE ACCESO A LA RED

En la actualidad, Txinzer utiliza Aruba Clearpass (virtual appliance) como solución de los procesos de autenticación, autorización y accounting (AAA) para realizar el control de acceso de usuarios y dispositivos a la red corporativa mediante la tecnología Wireless.

En la solución ofertada se requiere extender la solución de control acceso implementada mediante Aruba Clearpass a la red cableada. Se quiere implementar una configuración dinámica de los puertos de acceso de la red en función del perfil del usuario o dispositivo conectado. El licitador en su oferta deberá detallar los procedimientos para implementar esta solución. Procedimientos que se desplegarán en la fase de instalación.

Se deberán contemplar en el proyecto 200 licencias adicionales a las que tiene ya Txinzer.

Si la empresa licitadora decidiera ofertar en este proyecto un sistema NAC diferente a Clearpass, ésta, además de ser equivalente en funcionalidades a la actual, deberá contar con licencia para además de las 200 licencias solicitadas, las 200 con las que actualmente cuenta Txinzer.

Dicha propuesta deberá cubrir por 3 años de garantía y actualizaciones de fabricante las 200 licencias nuevas que se solicitan en este pliego, además de contratar mismo soporte para las 200 (2*JZ400AAE) que actualmente tiene Txingudi, y el servidor Aruba ClearPass Cx000V VM SVC [1* JZ399AAE] en modalidad 24*7, o en su defecto la nueva propuesta.

5. NECESIDADES

Tal y como se ha explicado previamente, se busca sustitución total de la electrónica existente en los nodos que alcanza este proyecto, dándose de este modo un salto evolutivo cuantitativo y cualitativo.

Con esta sustitución, además de la mejora de velocidades y funcionalidades debida a la evolución de la tecnología, se busca mejorar el rendimiento en el acceso.

El detalle de lo que se pide es el siguiente:

Fibra Óptica:

Hace falta lanzar 80 metros de fibra óptica monomodo en dos mangueras de 24 puertos entre los dos nodos principales de Perujaran. Dicha fibra tendrá que ir canalizada en conducto corrugado.

En ambos armarios de comunicaciones hace falta una bandeja de hasta 96 fibras en LC con formato de cassetes. En cada una de estas dos bandejas, habrá que instalar 2 cassetes de 24 fibras ópticas.

La solución deberá basarse en bandejas de este tipo por su densidad de puertos, así como en cassetes pensando en una mejor conservación de la fibra óptica, con organizador incluido.

Deberán estar incluidos todos los materiales necesarios, su instalación, así como fusión de todas las fibras y su certificación que se deberá entregar con la documentación del proyecto.

Han de incluirse latiguillos.

A continuación, se detallan los puertos y velocidades mínimas necesarias por nodo.

Perujaran nodo planta 1ª

3 conmutadores centrales (se detallan características más adelante)

Apilado cerrado entre ellos a 50Gbps

Switch virtual

12 puertos 10Gbps RJ45

33 puertos 1000BaseT

Fuente de alimentación redundante

Unión 20Gbps con Planta 0 de Perujaran

Perujaran Nodo Planta 0 (baja)

192 puertos en conmutadores de acceso (se detallan características más adelante)
1000BaseT y con PoE+

Apilado en switch virtual con enlaces de 10Gbps entre todos los switches con stack cerrado

Unión 20Gbps a nodo planta 1

Perujaran FCC

48 puertos en conmutadores de acceso (se detallan características más adelante)
1000BaseT y con PoE+

Unión 10Gbps a backbone

OAP

96 puertos en conmutadores de acceso (se detallan características más adelante)
1000BaseT y con PoE+

Apilado en switch virtual con enlaces dobles de 10Gbps entre todos los switches con stack cerrado

Unión 20Gbps a backbone y una unión a 1Gbps LX con el bombeo de Gal.

EDAR

96 puertos en conmutadores de acceso (se detallan características más adelante)
1000BaseT y con PoE+

Apilado en switch virtual con enlaces dobles de 10Gbps entre todos los switches con stack cerrado

Unión 20Gbps a backbone más uniones a 1Gbps LX con PLC1 y PLC2.

ETAP

96 puertos en conmutadores de acceso (se detallan características más adelante)
1000BaseT y con PoE+

Apilado en switch virtual con enlaces dobles de 10Gbps entre todos los switches con stack cerrado

Unión 20Gbps a backbone y dos uniones a 1Gbps con Elordi y Reactivos

Gestión y Monitorización

Plataforma de gestión que cumpla con los requisitos que se especifican en el documento, que gestione toda la electrónica del proyecto así como los APs de Txinzer de manera unificada, y con licenciamiento y soporte incluido de fabricante a 3 años para toda la solución. Deben estar incluidas las actualizaciones.

Control de acceso

Plataforma de control de acceso a la red tanto para entorno cableado como inalámbrico, que cumpla con los requisitos señalados en este PPT, y que cuente con 400 licencias de usuario, y servidor en formato virtual alojado en la infraestructura de Txinzer. Todas las licencias activas por 3 años y con soporte de fabricante por el mismo periodo, que también incluya actualizaciones.

6. CARACTERÍSTICAS TÉCNICAS MÍNIMAS A CUMPLIR POR LA SOLUCIÓN

Conmutadores centrales (Perujaran Nodo Planta 1ª)

Las características mínimas serán:

- Formato de 1UA
- Puertos SFP+/SFP56
- Puertos 25 GbE ópticos
- Todos los puertos deben ser non blocking
- 880Gbps de capacidad mínima interna de conmutación
- Apilado virtual de switches
- IEEE 802.1D, 802.1s, 802.1w
- IEEE 802.1Q
- Priorización hasta de capa 4
- Calidad de servicio: IEEE 802.1p
- Mapeo de IEEE 802.1p basada en IP address, tipo de servicio IP (ToS), protocolo nivel 3
- VxLAN

- IEEE 802.3ad
- ACLs
- VRRP o similar
- Routing: Rutas estáticas, OSPF
- Soporte IPv6.
- DHCP Server y DHCP Relay
- Protocolo netflow o sflow
- Soporte Multicast: IGMP, PIM
- Soporte 802.1AB, LLDP-MED.
- Filtrados y listas de control de acceso según información de niveles 2 y 3.
- Fuente de alimentación redundante
- SNMP v1 v2 v3, RMON.
- Acceso seguro a la gestión mediante cli, web o MIB a través de ssh, ssl o SNMPv3.

Conmutadores acceso (Resto de nodos)

Las características mínimas serán:

- Formato de 1UA
- Puertos SFP+
- Puertos 10 GbE
- Todos los puertos deben ser non blocking
- 176Gbps de capacidad interna de conmutación mínima
- Apilado virtual de switches
- Densidad de 48 puertos
- Eficiencia energética 802.3az
- Totalidad de puertos de cobre con PoE+
- 802.3af, 802.3at
- IEEE 802.1D, 802.1s, 802.1w
- IEEE 802.1Q
- Priorización hasta de capa 3
- Calidad de servicio: IEEE 802.1p
- Mapeo de IEEE 802.1p basada en IP address, tipo de servicio IP (ToS), protocolo nivel 3
- VxLAN
- IEEE 802.3ad
- ACLs
- VRRP o similar
- Routing: Rutas estáticas, OSPF
- Soporte IPv6.
- DHCP Server y DHCP Relay
- Protocolo netflow o sflow
- Soporte Multicast: IGMP, PIM
- Soporte 802.1AB, LLDP-MED.
- Filtrados y listas de control de acceso según información de niveles 2 y 3.
- SNMP v1 v2 v3, RMON.
- Acceso seguro a la gestión mediante cli, web o MIB a través de ssh, ssl o SNMPv3.

Plataforma de Gestión

Debido a la complejidad y la gran cantidad de equipos que conforman la red de Txingudiko Zerbitzuak un punto clave es la monitorización de la red ya que permite identificar y reaccionar ante eventos. Responde a la necesidad de “saber qué es lo que pasa para poder reaccionar de manera adecuada”.

La solución ofertada deberá ser gestionable de manera centralizada (monitorización y configuración vía interfaz web) desde una única plataforma de gestión. Como se ha dicho en la actualidad Txinzer cuenta con Aruba Central para el entorno Wireless. Es básico que a la finalización del proyecto tanto el entorno Wireless como el cableado se gestionen desde una única plataforma, Aruba Central o la nueva suministrada en esta solución.

Ante problemas de dispositivos de Red (Cableados o Inalámbricos) la plataforma de gestión:

- . Identifica
- . Configura
- . Supervisa
- . Actualiza
- . Soluciona

Dicha plataforma tendrá que cumplir como mínimo con las siguientes características:

- Actualización centralizada del firmware de los dispositivos. Esta tarea podrá realizarse automáticamente de forma programada o mediante actuaciones puntuales.
- Auto-Descubrimiento de dispositivos.
- Gestión de dispositivos, utilizando siempre protocolos de gestión estándar como SNMP, ssh, telnet, etc.
- Comprobación de las políticas de seguridad configuradas en los dispositivos, detectando violaciones o deficiencias en la configuración, 802.1x ...
- Configuración masiva de dispositivos mediante la descarga de plantillas que se cargan simultáneamente a grupos de equipos creados por el administrador.
- Permitir la configuración y administración completa de todos los elementos de la red
- Permitirá la notificación y seguimiento de fallos a través de notificaciones en distintos formatos (Syslog, e-mail y SNMP Traps).
- Permitirá almacenar, al menos, el último fichero de configuración, facilitando la “marcha atrás” en caso de ser necesario.
- Permitirá la supervisión y control de toda la infraestructura mediante la recolección de alarmas y eventos de los elementos de la misma y su representación visual, así como su exportación a otras plataformas mediante protocolos SNMP o syslog.
- Permitirá elaborar informes personalizados sobre la actividad de la red con periodicidad configurable y entregables en varios formatos (pdf, html, csv, etc...)

- Permitirá monitorización proactiva de incidencias basada en umbrales para la generación de eventos y alarmas en base a variables críticas.
- Soportará la funcionalidad de mapa de red en donde se presente el estado de todos los elementos de la red, así como su estado de operación con tiempos de refresco no superiores a 5 minutos. Esto debe incluir la representación, al menos, de los siguientes elementos:
 - Estado operativo de los elementos
 - Representación del estado de cobertura de la red en el caso de los dispositivos wifi
- El sistema debe proporcionar estudios de cobertura en tiempo real en el entorno inalámbrico. Debe mostrar los mapas de calor con la distribución de frecuencias y potencias en tiempo real, a partir de la información que capturan todos los Puntos de Acceso.
- Permitirá monitorizar los conmutadores a los que están conectados los Puntos de Acceso, facilitando información sobre disponibilidad y utilización de los puertos, CPU, y memoria.
- Detecta equipamiento con versiones de software no actualizadas y distribuye las actualizaciones a todos los equipamientos que lo necesiten

Control de acceso

Como ya se ha señalado previamente, Txinzer cuenta con Clearpass de Aruba. Si el ofertante decide cambiar la solución actual, la nueva deberá cumplir con las siguientes funcionalidades:

Arquitectura:

- La solución podrá basarse en appliance físico o virtual
- Deberá existir un único nodo de configuración del sistema y deberá sincronizar la configuración al resto de equipos.
- El sistema deberá incorporar mecanismo de encriptado de datos internos mediante Linux Unified Key Setup (LUKS) mediante AES-256.

Compatibilidades:

- El Sistema deberá realizar descubrimiento y perfilado de dispositivos sin necesidad de sondas o equipos adicionales en las distintas sedes
- La solución debe contar con firmas de profiling incorporadas. En cualquier caso, se podrán realizar actualizaciones de las mismas en función de los dispositivos que se conecten.
- El sistema detectará automáticamente posibles conflictos en el perfilado y marcará los Endpoints si detecta incongruencias.
- El sistema deberá utilizar protocolos estándar que garanticen su compatibilidad con distintos equipos de acceso (switches, routers, firewalls, controladores WLAN, terminadores VPN) de distintos fabricantes.
- El sistema debe poderse integrar en más de un dominio corporativo para realizar consultas en el Directorio Activo.
- Se deberán soportar integraciones con sistemas de entidades externas:
 - Microsoft Active Directory

- RADIUS
- Directorios LDAP
- MySQL, Microsoft SQL, PostGRES y Oracle 11g ODBC-compliant SQL server
- Servidores de Token
- Kerberos
- Microsoft Azure Active Directory
- Google G Suite
- Built-in SQL Store, static host-list
- Soporte de autenticaciones mediante 802.1X, autenticación MAC y con portal cautivo.
- Soporte de autenticación basado con SNMP con switches que no soporten protocolos RADIUS.
- Se deberán poder realizar simulaciones de políticas de seguridad antes de su implantación.
- Soporte de servicios AAA (Authentication, Authorization and Accounting) con los métodos de autenticación más utilizados en la industria
- Posibilidad de separar los procesos de Autenticación y Autorización – cada proceso deberá poder utilizar bases de datos distintas.
- El sistema tendrá funcionalidades de Autorización del acceso en función de características como pertenencia a un grupo de usuarios, tipo de dispositivo móvil, aplicación utilizada, localización del dispositivo, estado de salud (health check) del dispositivo, etc...
- El sistema soportará la gestión automática de claves de acceso

Acceso de invitados con portales cautivos de acceso:

- Se podrá realizar el registro de dispositivos mediante portales cautivos, orientado a invitados, soluciones BYOD y gestión de dispositivos.
- El sistema incluirá la posibilidad de generar diferentes portales cautivos para la autenticación de invitados compatible con las soluciones más habituales de los distintos fabricantes de la industria.
- El portal cautivo incluirá funcionalidades avanzadas de auto-registro, mediante las cuales el invitado podrá generar su propia cuenta de invitado sin comprometer la seguridad de la red.
- El portal proporcionará diversos métodos para la entrega de credenciales de invitado: email, SMS, impresión de tickets.
- El portal proporcionará métodos avanzados de aprobación de la visita por parte de la persona que recibe al invitado que permitan autorizar la visita de manera flexible y sin intervención de personal de IT.
- El tiempo de expiración de las cuentas de invitados deberá ser configurable.
- Los portales cautivos permitirán personalizar la imagen de forma completa, con posibilidad de adaptación del código HTML completo y de las hojas de estilo CSS.
- Los formularios de acceso de invitados podrán personalizarse en todos sus campos con al menos las siguientes capacidades mínimas:
 - Inclusión en el portal de menús desplegable que permitan registrar información relativa al invitado (motivo de la visita, duración de la

misma, persona a la que visita, y cualquier opción adicional. El contenido de estos campos será personalizable.

- Generación de portales HTML de distinto tamaño en función del tamaño y resolución de las pantallas de los dispositivos móviles. El portal deberá redimensionarse automáticamente en función del dispositivo que lo visualiza.
- Posibilidad de incluir todo de tipo de contenido multimedia en el portal: imágenes, audio, video, etc... que varíe de forma dinámica según patrones establecidos. Este contenido podrá referenciarse a enlaces externos o podrá ser incluido en el propio Sistema. No existirá limitación de imágenes o contenidos que se podrán incluir.
- El portal proporcionará informes de actividad relativa al tráfico de invitados: número de visitas, contenido multimedia mostrado, número de SMS enviados con credenciales, etc...
- El portal permitirá integrarse con soluciones de doble factor de autenticación.
- Se podrán realizar integraciones con sistemas de terceros mediante OAuth para permitir a los usuarios invitados validarse con sus credenciales en las redes sociales más utilizadas en España, según el último estudio publicado por el observatorio nacional de las telecomunicaciones y la SI (ONTSI).
- Los portales de acceso permitirán integración con redes sociales como Facebook, Facebook WiFi, Google Plus, Twitter, Instagram, LinkedIn,

Health-Check (actualmente no se utiliza, pero deberá ser capaz de):

- La solución NAC deberá incorporar mecanismos para realizar el control de salud de los dispositivos que se conecten a la red.
- Se soportará health-check mediante funcionalidad “agentless” donde no se requiera la instalación de un agente para entornos Windows.
- La solución deberá proporcionar un workflow sencillo para que los usuarios puedan provisionarse cualquiera de los dos agentes. La provisión se realizará mediante portales cautivos configurables.
- El agente comprobará el estado y actualización de anti-virus, anti-spyware, firewalls, etc...y proporcionará instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas.
- La información de estado proporcionada por el agente deberá de poder ser consultada en tiempo real.

Integraciones:

- Se podrá configurar integraciones con terceros mediante consultas http/https para el intercambio de información.
- El sistema deberá poder exportar a sistemas de terceros información contextual de los usuarios autenticados: username, dispositivo usado, estado del posture, punto de conexión, etc.
- El sistema soportará la recepción de eventos vía Syslog para ejecutar acciones sobre la infraestructura de acceso, desconectando usuarios o cambiándoles de VLANs.

- Se deberá soportar la integración con sistemas MDM para recibir información sobre los dispositivos enrolados en dichas plataformas. Se deberá poder comprobar esta información para crear una política de acceso personalizada.

Otros:

- La solución NAC debe contar con las siguientes certificaciones de Seguridad:
 - FIPS 140-2
 - Extended Package for Authentication Servers Version 1.
 - Collaborative Protection Profile for Network Devices Version 1.0
- El sistema debe contar con un sistema de reporting integrado para generar informes programados y bajo demanda sobre la red, usuarios, dispositivos y autenticaciones.
 - Los informes podrán ser personalizados en cuanto a la fecha y al contenido de los mismos.
 - Se deberán poder hacer informes bajo demanda de autenticaciones satisfactorias y fallidas en periodos de tiempo limitados.
 - Se admitirán filtros en los informes para establecer resultados en función de cualquier atributo RADIUS: NAS, fuente de autenticación, status, etc.
 - Se deberán poder generar dos tipos de informes:
 - Informe PDF de alto nivel con información básica y agregada mediante gráficas.
 - Informe con los datos en bruto en formato CSV con los campos personalizables.
 - Los informes podrán generar notificaciones a direcciones de correo electrónico o mediante SMS.

7. CONDICIONES DE GARANTÍA Y SOPORTE DE MANTENIMIENTO

Los equipos hardware y su firmware tendrán contratado un soporte de fabricante de 3 años que incluya las actualizaciones de firmware y sustitución del equipamiento NBD (Next Business Day).

Los elementos software y licencias suministradas, tendrán contratado un soporte de fabricante por un periodo de 3 años con las actualizaciones incluidas. Además, tal y como se ha señalado, a los elementos software que actualmente tiene Txinzer también deberá añadirseles dicho soporte de 3 años, o de variar la solución propuesta de la actual de Txinzer, ésta deberá incluir las licencias necesarias para sustituir las soluciones actuales por 3 años.

La empresa adjudicataria deberá acreditarse como distribuidor autorizado por el fabricante.

La empresa adjudicataria debe garantizar que el equipo suministrado:

- Viene del canal autorizado por el fabricante.
- Está amparado por el soporte y garantía del fabricante de acuerdo con las políticas del mismo.

- Contará con los contratos de garantía y soporte oficiales de fabricante para este proyecto
- Está acompañado de las licencias de software y firmware válidas.
- Cumple con las normas europeas y nacionales sobre mercado.

La empresa adjudicataria proporcionará a Txinzer, o si ésta lo estima oportuno a la empresa que actualmente mantiene la infraestructura de LAN, todos los accesos necesarios a los contratos de garantía y soporte suscritos con fabricante.

8. SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN, PLAN DE MIGRACIÓN Y PUESTA EN MARCHA DEL NUEVO EQUIPAMIENTO

. Actuaciones previas

Antes de acometer el proyecto será necesaria una fase de revisión del diseño, planificación conjunta entre los técnicos de Txinzer y de la empresa adjudicataria, así como de las políticas a implementar en el acceso a la red. En esta fase se incluirá la revisión de los elementos y configuraciones implantados actualmente en Txinzer que intervengan en la solución a implantar objeto de este contrato y que constituyan una mejora de funcionamiento.

. Suministro del equipamiento

La empresa adjudicataria suministrará todo el equipamiento detallado en su solución: hardware, software y licencias asociadas, accesorios para la instalación.

Todo el equipamiento se suministrará en régimen de propiedad de Txinzer y deberá integrarse en la red de Txinzer con sus protocolos, funcionalidades etc.

Los soportes de los equipos y licencias contratados en este proyecto vendrán del fabricante a nombre Txinzer y será oficial del fabricante

. Instalación y configuración del equipamiento hardware y software suministrado

El adjudicatario realizará la instalación física de los elementos hardware de la solución ofertada.

Configuración de los componentes de acuerdo a la solución ofertada y teniendo en cuenta la revisión en el diseño si fuese necesario.

Las tareas de instalación y configuración deberán ser realizadas por el personal de la empresa adjudicataria contando con el apoyo del personal técnico de Txinzer.

Además de la configuración de los equipos, se configurará la plataforma de monitorización con las parametrizaciones acordadas con el personal de Txinzer, del mismo modo que las nuevas políticas de acceso a la red que se definan.

Los trabajos se realizarán con un calendario de actuaciones acordado con Txinzer, y de forma que alteren lo menos posible el funcionamiento de Txinzer. Cuando sean necesarios, los cortes de servicio se realizarán fuera del horario laboral de los usuarios y de manera acordada y prefijada. Deberá preverse una posible marcha atrás ante incidencias.

Una vez realizada la instalación, el personal técnico de Txinzer será el responsable de la gestión de la solución implantada.

. Pruebas

Especificación de un plan de pruebas que validen el correcto funcionamiento y configuración de la solución. El plan de pruebas verificará el correcto funcionamiento de cada uno de los elementos de la solución propuesta y de la solución global en su conjunto.

Al finalizar la instalación se entregará un documento en el que se especifiquen las pruebas realizadas para validar el correcto funcionamiento de la solución propuesta, con detalle de los resultados obtenidos en ellas.

Plan de Migración

En la propuesta, deberá detallarse un plan de migración en el que se especifique el orden de actuación sobre los diferentes nodos con la metodología, procedimientos de trabajo, tareas a ejecutar, y sus plazos de ejecución y recursos necesarios.

En la misma deberán detallarse los posibles cortes de servicio y duración por las actuaciones de migración. Así mismo, se incluirá un calendario orientativo de suministro si las circunstancias del mercado lo permiten, instalaciones, configuraciones y puesta en servicio. Dichas fechas se acordarán a posteriori con el personal de Txinzer.

Del mismo modo, se indicarán los requerimientos de infraestructura y condiciones necesarias para una correcta ejecución de los trabajos.

. Inventario

Los equipos que se suministren e instalen llevarán una etiqueta para su identificación.

El adjudicatario proporcionará un inventario detallado e individualizado de todos los equipos entregados y/o instalados en el plazo máximo de dos semanas una vez finalizada la instalación.

Asimismo, además de entregar al final en formato digital, el adjudicatario deberá mantener actualizada y accesible para Txinzer durante la duración del proyecto la siguiente documentación:

- Elementos instalados (marca, modelo, ...) y esquema de conexionado.
- Parcheo de puertos en los switches en todos los nodos (cobre y fibra)
- Configuración de cada uno de los elementos.
- Ficheros de configuración.
- Mapa Topológico
- Recorrido de la instalación de la fibra óptica en archivo digital
- Certificaciones de todas las fibras instaladas

No se dará por recepcionada la instalación mientras no se reciba la documentación completa y detallada de la solución propuesta y los manuales técnicos de todos los bienes suministrados.

. Formación

Plan de formación para los técnicos propios y/o pertenecientes a la actual empresa adjudicataria del contrato de mantenimiento TIC de Txinzer, justificando su contenido y planificación para obtener el mejor aprovechamiento y la máxima autonomía de los técnicos.

Asimismo, entregará guías y manuales de funcionamiento de todo el sistema.

9. CONTENIDO DE LA PROPUESTA

Independientemente de que el licitador pueda aportar cuanta información complementaria considere de interés, las propuestas técnicas deberán obligatoriamente constar al menos de la siguiente información:

- Descripción detallada de la solución propuesta.
- Características técnicas de los servicios ofertados.
- Características técnicas de los equipos ofertados detallados por Nodo.
- Características técnicas del software ofertado y licencias.
- Topología Propuesta
- Plan de pruebas.
- Proceso de implantación y migración
- Horarios y ventanas de actuación
- Plan de formación temario, lugar de impartición.
- Equipo humano que instalará y configurará el equipamiento ofertado.
- Integración con el Sistema de Control de acceso actual

ANEXO I. ESQUEMA ARQUITECTURA DE RED

