PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA ADJUDICACIÓN, POR POR PROCEDIMIENTO ABIERTO SUJETO A REGULACIÓN ARMONIZADA, DEL SERVICIO DE COMUNICACIONES (LOTE1) Y LINEA DE ACCESO A GISS (LOTE2) PARA MUTUA MONTAÑESA, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 7

Índice

1. INTRODUCCIÓN

Mutua Montañesa posee una red de comunicaciones compleja que sustenta su actividad diaria tanto a nivel de datos ethernet y wifi, como de voz fija y móvil. En este sentido en 2015, Mutua Montañesa licitó los servicios de comunicaciones antes descritos según expediente de licitación 2015-002-015 y con una duración principal de 4 años prorrogable por otros 2 años y un precio base de licitación de 1.532.990,26 € y un valor estimado de contrato de 2.529.433,93 € siendo adjudicataria la UTE formada por Telefónica de España y Movistar en oferta integradora de ambos lotes.

Llevado a cabo la implementación y el desarrollo de la parte principal del contrato de manera satisfactoria para las partes, una vez finalizado el plazo principal de 4 años se procedió a hacer efectiva la prórroga de 24 meses por lo que dicho expediente tiene como fecha de fin el 31/10/2021.

En los últimos años se ha observado como la diferenciación que antes se hacía de los distintos entornos de comunicación existentes se ha ido diluyendo en un paradigma de comunicaciones unificadas en los que simplemente se habla a nivel general de comunicaciones englobando las mismas en datos, wifi, voz, móvil, dependiendo de la necesidad, lugar, situación en la que se esté.

Es por esto que actualmente unificamos el servicio en una solución global de comunicaciones corporativas que engloben todos los aspectos antes descritos, bajo una visión de flexibilidad y sobre todo de seguridad, aspecto que desde Mutua Montañesa tenemos muy presente y que por tanto vamos a trasladar al proyecto desde el mismo momento de su inicio con esta licitación.

1.1. OBJETIVOS DEL PROYECTO

El objetivo de la presente licitación es renovar, potenciar y asegurar los sistemas de comunicaciones globales de la organización, dotando a la misma de las herramientas necesarias para acometer el día a día de la organización, así como los retos tecnológicos que en el ámbito de las comunicaciones puedan surgir en los próximos 4 años de manera flexible, potente y segura.

1.2. ALCANCE DEL PROYECTO

El alcance del proyecto consiste en la contratación durante 48 meses en modo servicio gestionado de todos los elementos de comunicaciones tanto HW como SW como de cualquier otra índole que den respuesta a las necesidades de Mutua Montañesa, en los siguientes grandes bloques:

- Comunicaciones de datos
  - Líneas de comunicaciones WAN y routing
  - Switching
  - Wifi
  - Internet
- Comunicaciones de Voz
  - Líneas fijas y móviles con tarifa plana de voz y franquicia de datos.
  - Terminales tanto móviles como de sobremesa
  - SoftPhones
  - Servicios de Centralita Virtual
- Seguridad

El alcance del proyecto incluye la totalidad de las sedes de la organización que se enumeran en la siguiente tabla:

Sede	Población		Dirección	Tipo
HOSPITAL Mutua Montañesa	Santander	39012	Avda. Faro-Pintor Eduardo Sanz, 19	CPD1
Central - Ataulfo Argenta	Santander	39004	Ataulfo Argenta,19	CPD2
Zamudio	Zamudio	48170	TEKNOLOGI ELKARTEGIA, S/N	1
Barcelona	Barcelona	8029	Diagonal 491	1
Salamanca	Salamanca	37002	Ancha s/n	2
Cáceres	Cáceres	10001	Ruta de la Plata 14	2
Torrelavega	Torrelavega	39300	España 8	2
Madrid	Madrid	28014	Prado 16 4º	2
Girona	Girona	17003	Lluis Pericot 13-15	2
Valladolid	Valladolid	47004	Colón s/n	2
Miranda de Ebro	Miranda de Ebro	9200	Comuneros de Castilla 15	2
Castro Urdiales	Castro Urdiales	39700	Leonardo Rucabado 23	2
Olot	Olot	17800	Barcelona 1	2
León	Leon	24002	Renueva 38	2
Palencia	Palencia	34003	Cuba 13	2
Plasencia	Plasencia	10600	Alfonso VIII 13	2
Mérida	Mérida	6800	Reina Sofia,18	2
Vigo	Vigo	36201	Camelias 80 Bajo	2
Oviedo	Oviedo	33001	Alcalde Manuel Garcia Conde,5	3
Ávila	Avila	5001	Benigno Lorenzo Velázquez 1	3
Burgos	Burgos	9004	Cid Campeador 112	3
Murcia (Prestaciones)	Murcia	30007	Navegante Juan Fernández, 19	2
Murcia (Asistencial)	Murcia	30004	Escultor Francisco Salzillo 11	3
Badajoz	Badajoz	6011	Juan Pereda Pila, 20	3

2. LOTE1. SERVICIO GLOBAL DE COMUNICACIONES

A continuación, se exponen los requisitos de obligado cumplimiento.

2.1. REQUERIMIENTOS DE CARÁCTER GENERAL

2.1.1. ***MODALIDAD DE SERVICIO TODO INCLUIDO***

Se considerarán incluidos en la oferta a presentar por los proveedores todos los equipos, suministros y servicios necesarios para el cumplimento de los requerimientos expresados en la presente licitación (obra civil, infraestructuras, ingeniería, permisos, canalizaciones, cableados de interconexión, cableados interiores para el acceso a las redes de comunicaciones, elementos de administración repartidores, equipamiento,....), así como su mantenimiento integral a lo largo de la vigencia de la presente licitación.

Se requiere que todo el material utilizado para la implantación de las soluciones y servicios descritos en este pliego, que esté ubicado en dependencias de Mutua Montañesa, sea NUEVO (enrutadores/FW/SW/AP (red de datos), terminales fijos y móviles, antenas, auriculares, … etc.)

Todos los aspectos incluidos en el presente lote se entienden suministrados en modalidad de servicios, es decir, un pago por uso de una serie de líneas de comunicaciones, infraestructuras, equipos y servicios que el licitante pone a disposición de Mutua Montañesa para cubrir los requerimientos detallados en el presente documento. Así mismo todos los consumos recogidos en esta licitación tanto de voz, como de datos como de cualquier otra índole se entenderán en la modalidad de "tarifa plana" sin que sea posible llevar a cabo ningún tipo de regularización económica por consumos a lo largo de la vida del contrato, salvo los recogidos expresamente en este pliego técnico o en las clausula PCAPD.

2.1.2. ***ADAPTACIONES FUTURAS***

Así mismo se entienden como incluidos los trabajos y actuaciones necesarias, en el ámbito del presente lote, fruto de:

- la apertura o cierre de centros, la agrupación de centros dispersos en nuevos centros, obras de remodelación, …
- eventos no previstos con necesidad de servicios de telecomunicaciones urgentes.
- situaciones de emergencia que pueden requerir necesidades adicionales de servicios.
    - Se considerarán situaciones de emergencia aquellas que afecten al CPD Principal o al CPD secundario, afectando a la calidad o garantía de servicio.
- la evolución de las necesidades en servicios de comunicaciones (ancho de banda, líneas de voz, etc.).
- adecuación de los servicios a la realidad del mercado en cada momento y prever los nuevos requerimientos en servicios de comunicaciones.

2.2. RED DE DATOS

El proveedor deberá proponer una solución global que abarque todos los aspectos relativos a comunicaciones de datos se refiere. Dicha red deberá contener tanto la red WAN de comunicaciones con la red LAN y Wifi en una solución que permita una integración total entre todos los elementos que la componen. Se valorará la capacidad de integración entre todos los elementos que componen la red de datos (WAN/LAN/WIFI), la gestión unificada de la plataforma, así como la flexibilidad a la hora de gestionar el trafico que por ella discurre. La premisa de la seguridad desde el diseño de la solución debe ser objetivo prioritario de la solución propuesta, por lo que se valorará de manera importante las capacidades de seguridad global de la nueva red a implantar.

2.2.1. ***REDES WAN***

El proveedor deberá dotar a Mutua Montañesa de una red de comunicaciones robusta, escalable, segura, con las siguientes características generales para todos los elementos que la componen:

- Encriptación de datos. La red propuesta deberá garantizar la privacidad de los datos que por ella viajan, mediante el empleo de técnicas de encriptación u otros mecanismos análogos que garanticen dicha encriptación. En cualquier caso, deberá ser compatible con lo dispuesto a tal efecto en el Esquema Nacional de Seguridad.
- La velocidad de enlace de una sede deberá ser mantenida a lo largo de toda la red del operador, sin que se produzcan "cuellos de botella" al atravesar los distintos puntos de unión de la red del operador. Así si en una ciudad o área metropolitana confluyen el tráfico de dos sedes, la conexión de esa área metropolitana con la red nacional del operador deberá ser no inferior a la suma aritmética de caudales de las dos sedes.
- QoS. La red permitirá la gestión de caudales y la priorización de los mismos atendiendo al origen y destino de las comunicaciones, así como a las aplicaciones que por ella se cursen. La red deberá ser capaz de identificar los tipos de aplicación que se cursan en la red (al menos de las principales aplicaciones de mercado), permitiendo el encaminamiento de tráficos dentro de la red en función del tipo de tráfico que se curse. Así mismo el proveedor deberá proporcionar a Mutua Montañesa de un sistema de monitorización y gestión de red que permita:
    - Visualizar informes
    - Inventario de equipamiento de red
    - Monitorizar en tiempo real la red
    - Modificar configuraciones de la red básicas.

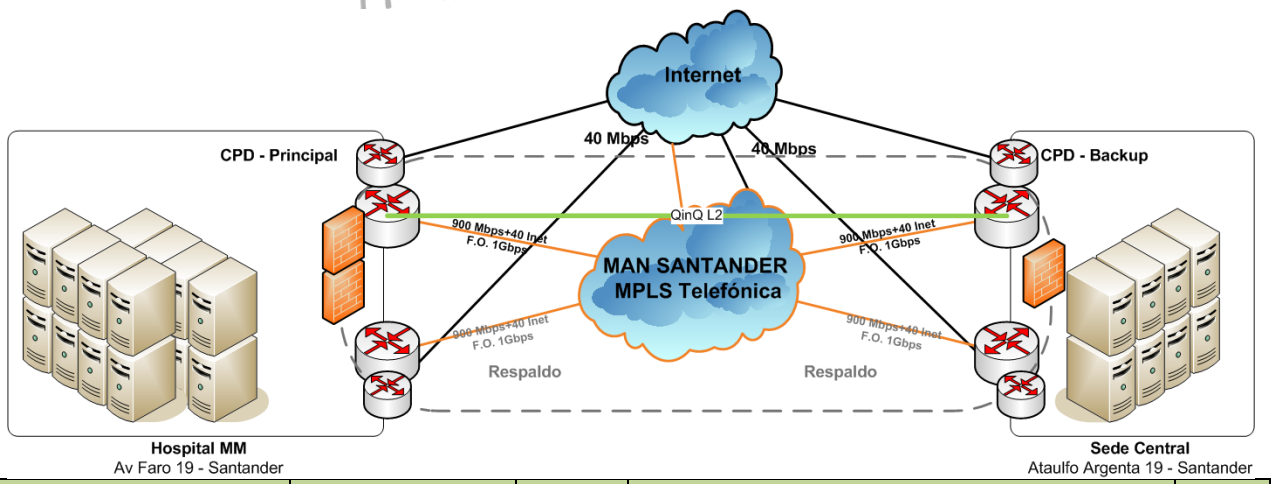
- VozIP. Deberá garantizarse el rendimiento idóneo para dar soporte a la voz de la organización a través de sistemas de telefonía IP, garantizando que aspectos como el Jitter de la red este en valores aceptables para el desarrollo de múltiples conversaciones simultaneas.
- No se admitirá el uso de redes de banda ancha minorista.
- El proveedor deberá tener una red propia de F.O. con cobertura nacional en las direcciones de las sedes indicadas en el presente pliego.
- Soporte IPv4 e IPv6
- Posibilidad de integración en la red privada de tenants que Mutua Montañesa pueda tener operativos en los principales servicios de Cloud Publica existentes (AWS, Azure y Google) mediante extensiones que garantice la homogeneidad de la solución
- Se valorará la orientación de la solución a redes de última generación que permitan la gestión del tráfico, la integración con el cloud y la gestión mediante software de las redes objeto de la licitación a todos los niveles incluida la seguridad.

A continuación, se detalla la situación actual que sea de relevancia y los requerimientos necesarios para los tipos de sedes enumerados anteriormente

2.2.1.1. CPDs Internos

SITUACION ACTUAL

El siguiente esquema recoge la interconexión actual de los 2 CPDs de la organización



Sede	Población		Dirección	Tipo
HOSPITAL Mutua Montañesa	Santander	39012	Avda. Faro-Pintor Eduardo Sanz, 19	CPD1
Central - Ataulfo Argenta	Santander	39004	Ataulfo Argenta,19	CPD2

REQUERIMIENTOS

Se requiere una solución completa a nivel de comunicaciones y red para cada uno de los 2 CPDs internos de la organización con las siguientes características:

- Características Generales
  - Redundancia total de todos los elementos que componen la solución
  - Router y/ó equipamiento similar individual por cada uno de los enlaces, con capacidad para failover automático entre enlaces.
  - Latencia entre routers de los dos CPDs de la organización inferior o igual a 2 ms
  - Líneas PRI/BCK de cada CPD completamente diversificadas tanto en trazado de línea y acometida hasta la propiedad como en Centrales de operador y que discurran por red propia del licitador.
  - Tipos de enlace: F.O. dedicada de acceso exclusivo hasta equipos de Central del operador
  - Capacidad para la entrega de múltiples servicios mediante técnicas de MultiVRF o similares
  - Tunelización Q-in-Q. Se requiere el transporte L2 entre ambos CPDs para las VLAN que Mutua Montañesa determine, lo que permitirá el empleo de una misma subred de CPD en ambas ubicaciones sin necesidad de cambio alguno en los equipos de cliente ni en los equipos de red.

- Acceso Principal:
  - Ancho de Banda: 1 Gbps ampliable a 10 Gbps
  - Caudal:100 % Garantizado
- Acceso Backup:
  - Ancho de Banda: 1 Gbps
  - Caudal:100 % Garantizado

2.2.1.2. Tipo 1

En este tipo de sede se engloban las de mayor tráfico y criticidad para la organización, por el volumen de usuarios o el servicio que se presta en ella.

Sede	Población		Dirección	Tipo
Zamudio (SARENET)	Zamudio	48170	TEKNOLOGI ELKARTEGIA, S/N	1
Barcelona	Barcelona	8029	Diagonal 491	1

Se requiere una solución completa a nivel de comunicaciones y red con las siguientes características:

- Características Generales
  - Redundancia total de todos los elementos que componen la solución
  - Router y/ó equipamiento similar individual por cada uno de los enlaces, con capacidad para failover automático entre enlaces.
  - Latencia entre routers de la sede y los dos CPDs de la organización inferior o igual a 20 ms
  - Se valorará que las líneas PRI/BCK de la sede estén completamente diversificadas tanto en trazado de línea y acometida como en Centrales de operador y que discurran por red propia del licitador.
  - Tipos de enlace: F.O. dedicada de acceso exclusivo hasta equipos de Central del operador
  - Capacidad para la entrega de múltiples servicios mediante técnicas de MultiVRF o similares

- Acceso Principal:
  - Ancho de Banda: 100 Mbps ampliable a 1 Gbps
  - Caudal:100 % Garantizado
- Acceso Backup:
  - Ancho de Banda: 100 Mbps
  - Caudal:100 % Garantizado

2.2.1.3. Tipo2

En este tipo de sede se engloban las sedes con capacidad asistencial y menos de 12 puestos de trabajo.

Sede	Población		Dirección	Tipo
Salamanca	Salamanca	37002	Ancha s/n	2
Cáceres	Caceres	10001	Ruta de la Plata 14	2
Torrelavega	Torrelavega	39300	España 8	2
Madrid	Madrid	28014	Prado 16 4º	2
Girona	Girona	17003	Lluis Pericot 13-15	2
Valladolid	Valladolid	47004	Colón s/n	2
Miranda de Ebro	Miranda de Ebro	9200	Comuneros de Castilla 15	2
Castro Urdiales	Castro Urdiales	39700	Leonardo Rucabado 23	2
Olot	Olot	17800	Barcelona 1	2
León	Leon	24002	Renueva 38	2
Palencia	Palencia	34003	Cuba 13	2
Plasencia	Plasencia	10600	Alfonso VIII 13	2
Mérida	Merida	6800	Reina Sofia,18	2
Vigo	Vigo	36201	Camelias 101	2
Murcia (Prestaciones)	Murcia	30007	Navegante Juan Fernández, 19	2

Se requiere una solución completa a nivel de comunicaciones y red con las siguientes características:

- Características Generales
  - El router de la delegación podrá aglutinar las conexiones Principal y Backup.
  - Latencia entre routers de la sede y los dos CPDs de la organización inferior o igual a 50 ms se valorará un compromiso de latencia inferior a 40 ms

- Equipamiento físico capaz de gestionar ancho de banda superiores sin necesidad de cambio de equipo.
- Tipos de enlace: FTTO (Fiber to the Office) y enlace móvil 4G/5G para el backup En el momento que el proveedor tenga homologado en su red el 5G como sistema de enlace deberá realizar el upgrade sin coste adicional para mutua. Se valorará la mejora de los medios de acceso (F.O. Dedicada)

- Acceso Principal:
  - Ancho de Banda: 100 Mbps simétricos
  - Caudal:100 % Garantizado
- Acceso Backup:
  - Ancho de Banda: Fondo de línea 4G/5G

2.2.1.4. Tipo 3

En este tipo de sede se engloban las sedes administrativas en la mayoría monopuesto.

Sede	Población		Dirección	Tipo
Badajoz	Vigo	36201	Camelias 101	3
Oviedo	Oviedo	33001	Alcalde Manuel Garcia Conde,5	3
Ávila	Ávila	5001	Benigno Lorenzo Velázquez 1	3
Burgos	Burgos	9004	Cid Campeador 112	3
Murcia (Asistencial)	Murcia	30004	Escultor Francisco Salzillo 11	3

Se requiere una solución completa a nivel de comunicaciones y red con las siguientes características:

- Características Generales
  - El router de la delegación podrá aglutinar las conexiones Principal y Backup.
  - Latencia entre routers de la sede y los dos CPDs de la organización inferior o igual a 60 ms se valorará un compromiso de latencia inferior a 50 ms
  - Tipos de enlace: FTTO (Fiber to the Office)
- Acceso Principal:
  - Ancho de Banda: 100 Mbps simétricos
  - Caudal:50 % Garantizado

2.2.1.5. Otras líneas

Requerimientos

Se solicita una línea móvil integrada en la red privada de la organización con router para provisión de sede en modo de emergencia ante incidencias graves o para provisión de un acceso corporativo en eventos, reuniones, fuera de las dependencias de la organización. Dicho enlace deberá ser como cualquier otra sede de la organización y basado en tecnología 4G/5G

También se solicita un mínimo de 2 líneas (una por cada CPD) de acceso de tipo residencial básicas (FTTH o similares) con acceso a internet no integradas en la VPN corporativa para la realización de pruebas y como salida a internet de cortesía. Se valorará que tengan IP fija.

2.2.2. *INTERNET*

Se requiere dotar de conectividad a internet para toda la organización mediante el suministro de un servicio tanto en el CPD principal como en el de respaldo (esta última conexión solo se activará en caso de contingencia grave) con las siguientes características

- Doble Acceso Activo/Pasivo por cada CPD, con 300 Mbps de ancho de banda simétrico 100% garantizado en cada acceso.
- El acceso a internet debe ser garantizado, sin priorizaciones ni ralentizaciones de contenidos ni servicios. El uso de aplicaciones protocolos y tecnologías no pueden estar limitados por la operadora.
- Mínimo 16 Direcciones IP públicas
- Los enlaces de internet deberán ser individualizados de la red interna de la organización entregándose en F.O. Diferentes o garantizando, que no interfiere en los caudales requeridos para las sedes CPDs y que ante una posible ampliación de caudal en los CPDs ya sea de internet o de acceso de red interna no hay saturación en el canal.
- Routers independientes de la red WAN para la gestión del tráfico de internet.
- Sistema de Failover automático entre enlace principal y Backup
- Sistema de Failover entre CPD Principal y Secundario que garantice la entrega de estas IPs Publicas de la organización en el CPD secundario como mínimo mediante procedimiento manual de centro de gestión de red valorándose positivamente la posibilidad de que sea automatizado .
- Servicio de protección contra DoS proporcionado por el operador, previo a la entrega de las IPs en los routers.
- Se valorará la inclusión de sistemas de Local breakout para ciertos traficos de internet (EJ: Videoconferencia/Teams/O365/…) en las sedes hasta tipo 2 inclusive, cumpliendo con las preceptivas medidas de seguridad que sean necesarias para que ese tráfico sea seguro.

2.2.3. ***LAN***

Se requiere dotar de conectividad LAN a todos los equipos de la organización. A continuación, se detallan los requerimientos generales de este servicio.

- Solución corporativa integral. Deberá ser una solución homogénea a nivel de marca valorándose positivamente que dicha solución Lan también se integre con la solución WAN de última generación aportada.
- Posibilidad de acceso a consola de gestión global en cloud sin instalación de equipos de gestión onpremise de la solución LAN valorándose positivamente que esta misma consola incluya también la solución Wifi con la que esta solución LAN debe quedar completamente integrada
- Deberá ser de una marca de reconocido prestigio en networking para datacenter y en consonancia con el resto de equipamiento de red proporcionado que permita la mejor integración posible entre elementos. Se valorará y tomará como referencia el Cuadrante mágico de Gartner 2020 sobre infraestructuras de acceso a red cableadas e inalámbricas

2.2.3.1. CPD Principal Hospital MM

Situación Actual:

Mutua Montañesa posee en propiedad un core de switch para la operación del CPD instalado en Junio de 2015 compuesto por dos equipos HP A5500-48G-4SFPunidos mediante STACK y con Software Version 5.20.99 y con una ocupación de puertos del 70%.

El grueso de servidores de la organización están virtualizados en 4 host de VMWare con 8 tarjetas de red 1000 baseT cada uno.

Así mismo existen dos switchs Cisco Catalyst 3850 – 24 puertos Giga en stack, propiedad del operador actual, para la operación de los equipos de comunicaciones con una ocupación de puertos del 40%. Están unidos al CORE de CPD por 2 puertos Giga en trunk.

Requerimientos:

El proveedor deberá dotar, implantar, mantener y evolucionar un CORE de red adecuadamente dimensionado que permita la retirada de todos los equipos LAN antes descritos y que permita tanto la operación de CPD como de los equipos de comunicaciones del operador. Dicho core o cores de red deberán tener las siguientes características mínimas:

- Totalmente redundante y tolerante a fallos tanto a nivel de suministro eléctrico como de disponibilidad de puertos mediante técnicas de Stack o similar
- Cada core deberá actuar como una única unidad de gestión y conectividad de todos sus puertos.
- Todos sus puertos deberán ser mínimo 1000Mpbs incluyendo un porcentaje de puertos 10G para enlaces WAN u otros usos futuros
- Capacidad bruta total deberá garantizar un 40% de bocas libres 1Gb para posibles ampliaciones o modificaciones.
- Facilite la segmentación de los diferentes servicios de CPD
- Carcteristricas de switch de CORE LAN.

2.2.3.2. Red Hospital Mutua Montañesa

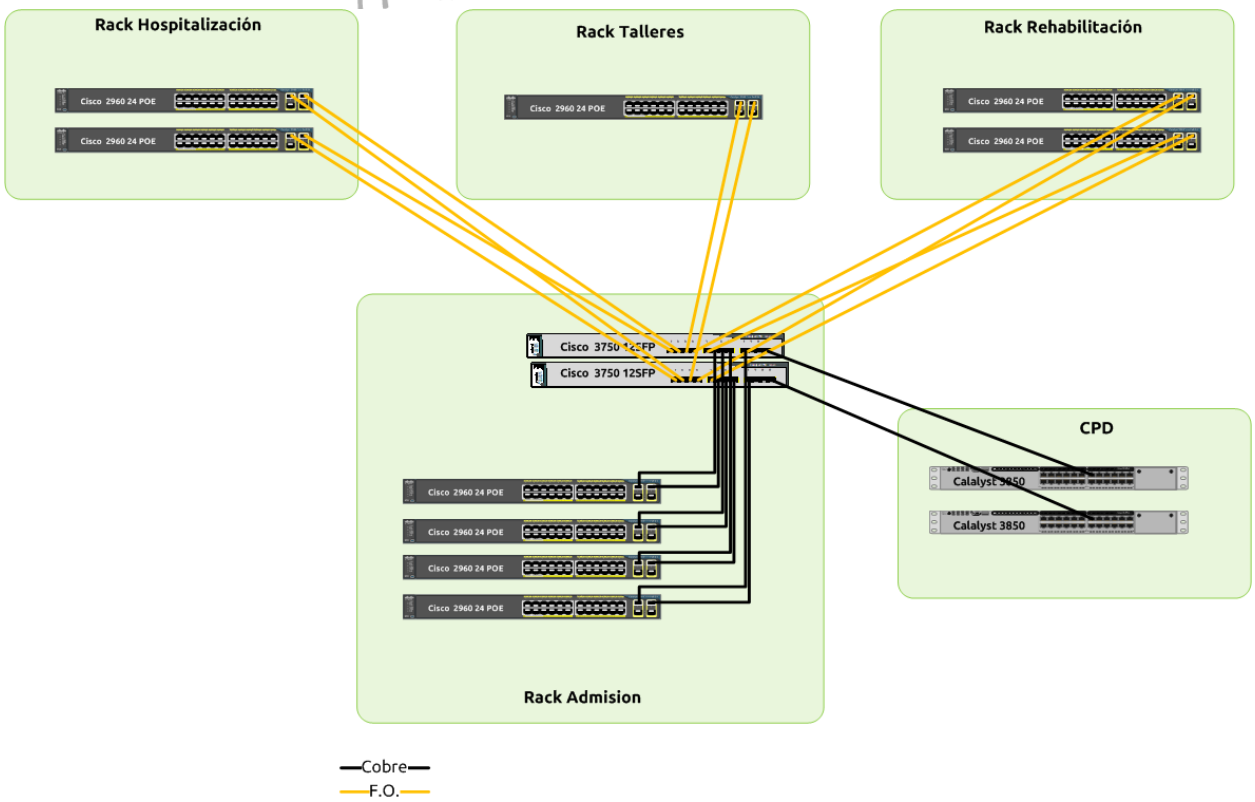
Situación Actual

La red de clientes del Hospital Mutua Montañesa está formada por una estrella de fibra multimodo 62,5/125 cuyo nodo central es el área de admisión del hospital compuesto por un core de red formado por 2 Cisco 3750 12SFP en Stack que se unen al CPD principal de la organización mediante un trunk de 2 puertos 1000TX y 4 switches de acceso CISCO WS-C2960-24PC-L al 90% de ocupación.

Como áreas remotas los siguientes Rack:

- Hospitalización:
  - 2 x CISCO WS-C2960-24PC-L
  - Enlace: 2 x F.O. 1000Base FX por switch
  - Ocupación actual 90%
- Rehabilitación
  - 2 x CISCO WS-C2960-24PC-L
  - Enlace: 2 x F.O. 1000Base FX por switch
  - Ocupación actual 80%
- Talleres
  - 1 x CISCO WS-C2960-24PC-L
  - Enlace: 2 x F.O. 1000Base FX por switch
  - Ocupación actual 0% (área en desuso actualmente)

El siguiente esquema recoge la topología de red del Hospital



Requerimientos

Se requiere dotar al hospital de una red que sustituya al actual garantizando tanto la estabilidad como la capacidad de crecimiento de la misma. Para ello se deberá dotar de una solución análoga a la existente mediante un core de red redundante en equipo y enlaces y tolerante a fallos y un sistema de switches de acceso de cliente con las siguientes capacidades mínimas por ubicación:

- Admisión:
  - Puertos 1000TX PoE: 120(*)
  - N.º de equipos mínimos:4
- Hospitalización:
  - Puertos 1000TX PoE: 72(*)
  - N.º de equipos máximo:2
- Rehabilitación
  - Puertos 1000TX PoE: 72(*)
  - N.º de equipos máximo:2
- Talleres
  - Puertos 1000TX PoE: 48(*)
  - N.º de equipos máximo:1

(*) Puertos de acceso de cliente netos, APs wifi excluidos

2.2.3.3. CPD Backup ATAULFO ARGENTA

Situación Actual:

En este CPD de respaldo posee en propiedad un core de switch obsoleto formado por 2 swtich 24 puertos 1000 Base T en Stack con una utilización actual del 45%.

La red de servidores de backup de la organización está virtualizada en 3 host de VMWare con 6 tarjetas de red 1000 baseT cada uno.

Así mismo existen dos switchs Cisco Catalyst 3750 – 12 puertos Giga SFP en stack, propiedad del operador actual, para la operación de los equipos de comunicaciones Están unidos al CORE de CPD por 2 puertos Giga en trunk.

Requerimientos:

El proveedor podrá reemplazar el core de red por una solución similar a la adoptada en el CPD principal ajustando nº de puertos que en esta ubicación es de menos densidad. A estos equipos de core se les deberá dotar de 2 puertos SFP F.O. para unión con rack 2ª planta (ver apartado siguiente). A modo de resumen se requiere la siguientes características mínimas:

- Totalmente redundante y tolerante a fallos tanto a nivel de suministro eléctrico como de disponibilidad de puertos mediante técnicas de Stack o similar
- Todos sus puertos deberán ser mínimo 1000Mpbs incluyendo un porcentaje de puertos 10G para enlaces WAN u otros usos futuros
- Capacidad bruta total deberá garantizar un 40% de bocas libres 1Gb para posibles ampliaciones o modificaciones.
- Facilite la segmentación de los diferentes servicios de CPD
- Carcteristricas de switch de CORE LAN.

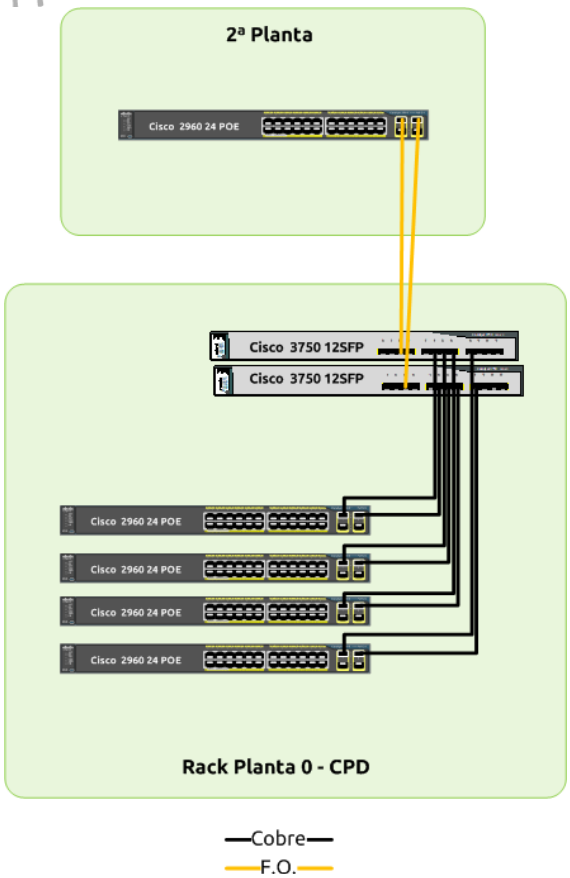
2.2.3.4. Sede Ataulfo Argenta

Situación Actual

La red de clientes de la sede central de Montañesa está formada por una topología centralizada en un rack de comunicaciones compuesto un core de red formado por 2 Cisco 3750 12SFP y los siguientes equipos de acceso de cliente:

- Rack planta 0 - CPD:
  - 4 x CISCO WS-C2960-24PC-L
  - Enlace: 2 x 1000Base TX por switch
  - Ocupación actual 90%
- Rack Planta 2:
  - 1 x CISCO WS-C2960-24PC-L
  - Enlace: 2 x F.O. 1000Base FX
  - Ocupación actual 95%

El siguiente esquema recoge la topología de red de Ataulfo



Requerimientos

Se requiere dotar de una red que sustituya la actual garantizando tanto la estabilidad como la capacidad de crecimiento de la misma. Para ello se deberá dotar de una solución análoga a la existente mediante un core de red redundante enlaces y tolerante a fallos en equipo con capacidad para un enlace de F.O redundate que de acceso al Rack de Planta2 y y un sistema de switches de acceso de cliente con las siguientes capacidades mínimas por ubicación:

- Planta 0 - CPD:
  - Puertos 1000TX PoE: 120
  - N.º de equipos mínimos:5
- Planta 2:
  - Puertos 1000TX PoE: 36
  - Puertos 1000SX 2 para enlace con core Planta 0
  - N.º de equipos máximo:1

2.2.3.5. Sede Barcelona

Situación Actual

La red de clientes de la sede de Barcelona está formada por una topología centralizada en un rack de comunicaciones compuesto un core de red formado por 2 Cisco 3750 12SFP y los siguientes equipos de acceso de cliente:

- Rack planta 0:
  - 3 x CISCO WS-C2960-24PC-L
  - Enlace: 2 x 1000Base TX por switch
  - Ocupación actual 50%

Requerimientos

Se requiere una red que sustituya la actual garantizando tanto la estabilidad como la capacidad de crecimiento de la misma. Para ello y con el fin de simplificar la configuración y reducir el nº de equipos a mantener se requiere de:

- Planta 0:
  - Puertos 1000TX PoE: 72
  - N.º de equipos máximo:3

2.2.3.6. ***Sedes tipo 2***

Requerimientos

Para cada una de las sedes de tipo 2 se requiere de un switch de 24 puertos 10/100/1000 Base TX POE, a excepción de la sede de Valladolid y Torrelavega que requieren de 48 puertos.

2.2.3.7. ***Sedes tipo 3***

Requerimientos

Para cada una de las sedes de tipo 3 se requiere de un switch de 8 puertos 10/100/1000 Base TX POE.

2.2.4. ***WIFI***

Situación actual

Mutua Montañesa posee actualmente una red wifi basada de un controlador Aruba en la que se radian 4 SSID a través de 26 aps instalados en las siguientes delegaciones:

Sede	APs
HOSPITAL Mutua Montañesa	8
Central - Ataulfo Argenta	6
Barcelona	4
Salamanca	1
Cáceres	1
Torrelavega	2
Madrid	1
Girona	1
Valladolid	2
Olot	1

Requerimientos

2.2.4.1. ***Aspectos Generales***

Se requiere la implantación de una nueva red Wifi con más capacidad y servicios que la actual. Dicha red deberá estar completamente integrada con la solución LAN implantada de manera que podamos tener una visión y control global de todos los posibles accesos de cliente a la red de manera unificada.

La gestión y monitorización del wifi será centralizada preferiblemente desde la nube. Se valorará la solución global presentada, prestando especial interés en la robustez del sistema que minimice los puntos únicos de fallo, así como la flexibilidad a la hora de generar nuevas redes o publicar las mismas en función de la delegación incluso seleccionando las zonas o aps en las que exhibirlas.

Así mismo se valorará las medidas de seguridad que se implanten y la capacidad de integración con el resto de los elementos de seguridad existentes en la organización y los incluidos en la presente licitación

El sistema almacenará los logs de todos los accesos y trafico generado durante al menos 1 año.

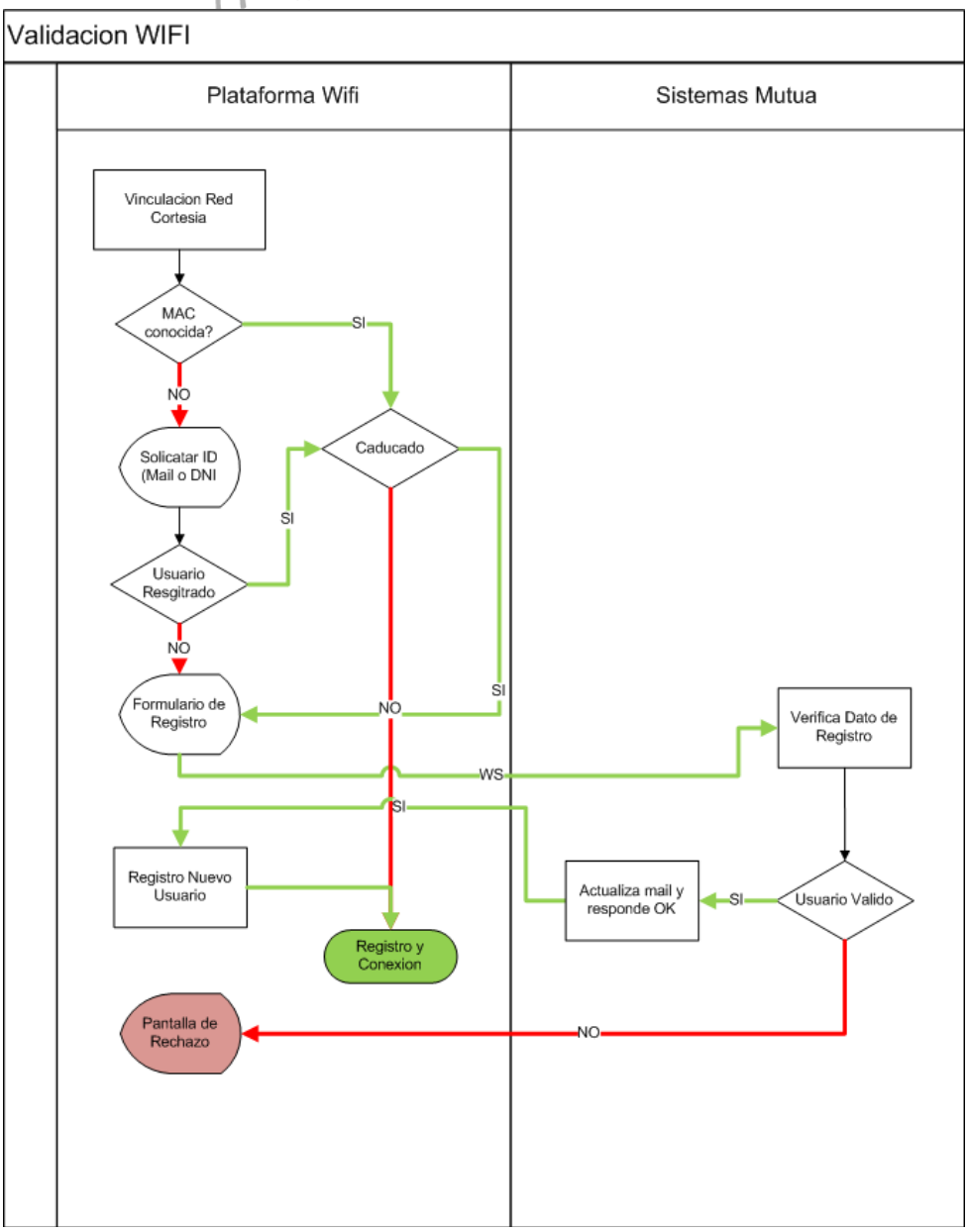
Se radiarán inicialmente un mínimo de 4 redes:

- Empleados: Red de acceso para dispositivos corporativos. Validará las credenciales mediante integración con el Directorio Activo de la organización y se configurará automáticamente mediante GPOs del dominio o método automático similar.
- Proveedores: Permitirá el acceso de proveedores a partes especificas de la red de la organización. Se validará mediante portal cautivo contra una unidad organizativa especifica del DA
- Dispositivos: Permitirá el acceso a la red de dispositivos especiales como TV, Proyectores, Equipos de medida, Deberá poderse individualizar para análisis de IoT en los equipos de seguridad de la organización.
- Cortesía: portal cautivo para dar acceso a internet a pacientes.

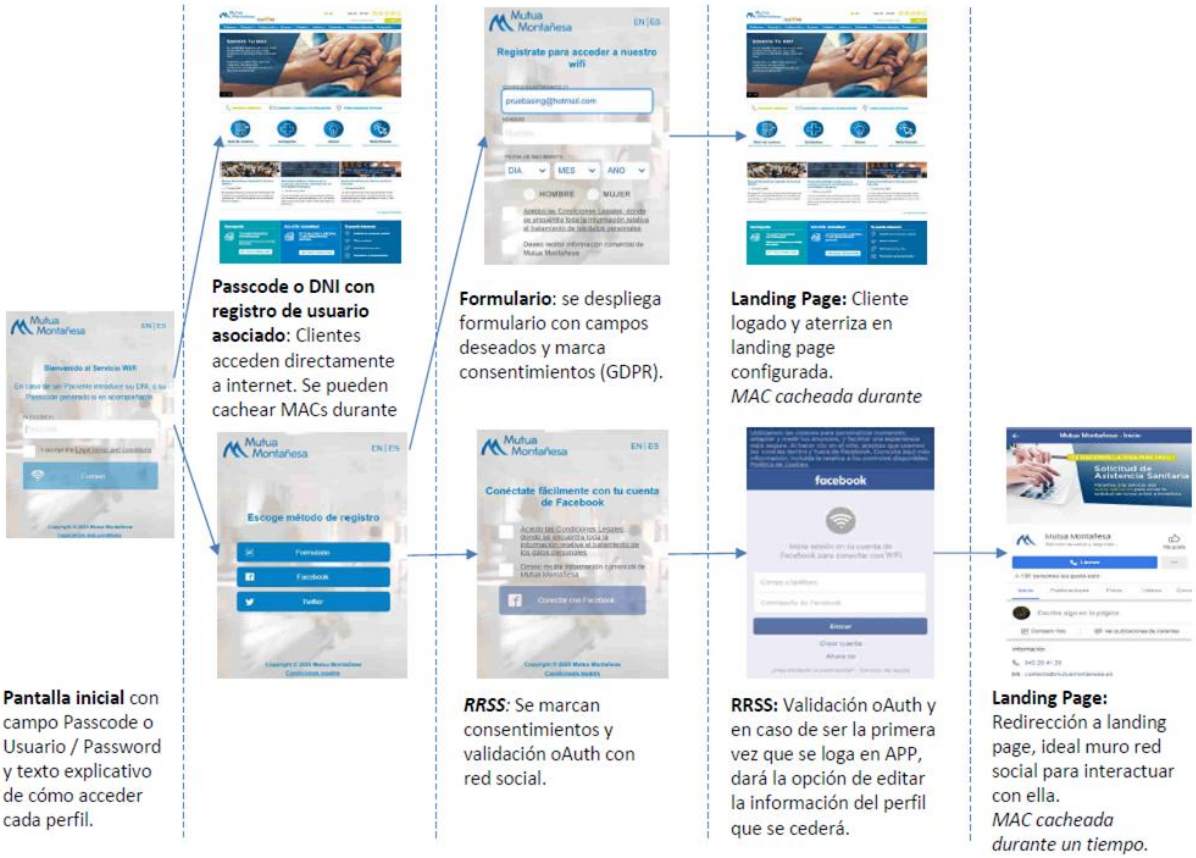
2.2.4.2. Wifi Cortesía

Mutua Montañesa requiere la implantación de un portal cautivo avanzado para dar acceso a internet a los pacientes. El sistema deberá permitir la navegación por internet de los pacientes con un método de validación integrado con los sistemas transaccionales de la organización.

A modo de ejemplo se propone el siguiente sistema para la validación de usuario contra los sistemas transaccionales de la organización (Pacientes/mutualistas) y enrolamiento de usuarios en el sistema.



Así mismo el sistema permitirá seleccionar otros medios de validación como redes sociales, mac,… e interactuar con el usuario mediante la selección de landingpages o campañas de divulgación que Mutua Montañesa establezca. El flujo de acceso en modo grafico sería algo similar a esto.



Se incluirá también la forma de generar "tickets" de acceso temporales desde las aplicaciones transaccionales de la organización o desde un portal especifico de fácil gestión por parte del personal administrativo de los centros de trabajo.

El tráfico cursado por los usuarios de esta wifi de cortesía deberá estar completamente aislado del resto de tráfico corporativo desde su origen hasta la salida a internet que deberá ser diferenciada de la navegación del resto de la organización, pudiéndose establecer limites de ancho de banda por usuario o por red para evitar impacto en el tráfico corporativo.

El proveedor será el responsable de identificación del trafico generado por cada uno de los usuarios en caso de disputa o reclamación judicial sobre el uso de esta red.

El almacenamiento de logs de conexión y accesos se mantendrá, como mínimo durante 12 meses en la red de servicio del operador o sistema Cloud, manteniendo el espíritu del pliego de minimizar la instalación de sistemas de gestión en formato ompremise

El sistema permitirá realizar una analítica de presencia y monitorización que permita a la organización analizar el comportamiento de los usuarios de esta red para adaptar los servicios que se les presta.

2.2.4.3. Cobertura

El proveedor deberá garantizar los siguientes niveles de cobertura wifi por sede:

Sede	APs Actuales	Cobertura Actual (*)	Cobertura Requerida
HOSPITAL Mutua Montañesa	8	40%	100%
Central - Ataulfo Argenta	6	60%	100%
Barcelona	4	50%	100%
Salamanca	1	50%	50%

Sede	APs Actuales	Cobertura Actual (*)	Cobertura Requerida
Cáceres	1	75%	100%
Torrelavega	2	66%	100%
Madrid	1	50%	50%
Girona	1	40%	80%
Valladolid	2	66%	100%
Olot	1	40%	75%
Miranda de Ebro	0	0%	50%
Castro Urdiales	0	0%	50%
Leon	0	0%	50%
Palencia	0	0%	50%
Plasencia	0	0%	50%
Mérida	0	0%	50%
Vigo	0	0%	50%
Murcia	0	0%	50%

(*) estimación no vinculante

El proveedor deberá asumir una variación, incluida en el coste del proyecto, de un 10% en el nº total de APs a suministrar con el fin de poder ampliar la cobertura de alguna de las sedes por necesidades del servicio. Se facilitará previa solicitud por escrito una vez publicado el presente pliego, planos de las delegaciones para el calculo de coberturas, quedando restringidas, por carácter sanitario, las visitas a las sedes para replanteo en fase de oferta, a aquellas en las que existan dudas sobre los planos o estos no sean suficientes para hacer la estimación.

2.3. VOZ

El avance de los sistemas de comunicaciones hacen que cada vez sea más real la integración de sistemas de comunicación que tradicionalmente eran diferenciados (Voz fija, móvil, mensajería,…). En la actualidad hablamos de sistemas de comunicación convergentes en los que se difuminan esas fronteras y en las que se precisa cada vez más flexibilidad de trabajo. En este sentido Mutua Montañesa pretende renovar la solución de telefonía existente por una nueva bajo este paradigma de comunicación, en la que podamos tener puestos fijos, puestos móviles y puestos mixtos, en los que podamos combinar las ventajas de ambos.

2.3.1. *SITUACIÓN ACTUAL*

2.3.1.1. Telefonía Fija

Mutua Montañesa posee un sistema de VozIP como servicio, gestionado por el operador actual, basado en tecnología Cisco HCS con las siguientes características generales:

- 300 terminales IP
  - 283 Cisco 7942
  - 2 Cisco 7940
  - 15 Cisco 7962
- 40 canales concurrentes de acceso a red fija
- 30 canales concurrentes de acceso a red móvil
- Servicio de IM y Presencia que se emplea con Chat interno.

- 21 números de cabecera
- 35 líneas RTB o similar para FAX y servicios auxiliares (Alarmas, Ascensores,..)
- Rango completo 942204100-942204199
- Numero 900 - **900 180 875**
- Supervivencia de Voz en caso de contingencia en las siguientes delegaciones:

Sede	SUPERVIVENCIA
Central	1 Enlace Primario
Hospital Ramón Negrete	1 Enlace Primario
Barcelona	4 Enlace Básico RDSI
Girona	2 Enlace Básico RDSI
Miranda de Ebro	1 Enlace Básico RDSI
Plasencia	2 Enlace Básico RDSI
Burgos	1 Enlace Básico RDSI
Castro-Urdiales	1 Enlace Básico RDSI
Cáceres	2 Enlace Básico RDSI
León	2 Enlace Básico RDSI
Palencia	1 Enlace Básico RDSI
Madrid	2 Enlace Básico RDSI
Mérida	1 Enlace Básico RDSI
Salamanca	2 Enlace Básico RDSI
Torrelavega	2 Enlace Básico RDSI
Olot	2 Enlace Básico RDSI
Valladolid	3 Enlace Básico RDSI

2.3.1.2. Telefonía Móvil

En la actualidad se dispone de 80 líneas móviles estables con franquicia de datos de 10 GB y 10 líneas adicionales que se activan y desactivan en funciona de necesidades de conciliación o situaciones temporales de teletrabajo. Todos los terminales están gestionados mediante un sistema MDM de VMWare Airwatch gestionado por el operador.

2.3.1.3. Volumetría

En el pasado 2020 se registró el siguiente volumen de llamadas:

- Fijas

DESCRIPCION	LLAMADAS	SEGUNDOS
Llamadas a móviles	29	548
Llamadas a Numeraciones 800/900	356	87271
Llamadas a Numeraciones 901	130	21677
Llamadas a Numeraciones 902	1810	238151
Llamadas a Sº de Información y Emergencia	28	5115
Llamadas al servicio Contestador	1	5
Llamadas Internacionales	2	77
Llamadas Interprovinciales	10046	2103230
Llamadas Metropolitanas	105872	16503466
Servicios de información telefónica y tarificación adicional	2	463

- Móviles
  - Voz

TIPO DE TRAFICO	LLAMADAS	SEGUNDOS
A.CONTENIDOS PREMIUM PROMOCIONADOS	1	0
ACCESOS A CONTENIDOS	32	0
DUO CORPORATIVO	585	114729
INTERNACIONAL	4	518
INTERNO BUZON	548	46467
INTERNO CORPORATIVO	68479	18335913
INTERNO CORPORATIVO EN UE	1	454
INTERNO MOVILES	45642	8373767
INTERNO MOVILES EN UE	2	122
LLAMADAS 80X/905 TARIFICACIÓN ADICIONAL	1	20
LLAMADAS A 800/900	177	46823
LLAMADAS A 901	62	14585
LLAMADAS A 902	149	35080
LLAMADAS A INFORMACIÓN Y EMERGENCIAS	27	4985
LLAMADAS A SERV. INFO. 118XX	1	20
LLAMADAS DUO	27271	5771088
LLAMADAS DUO EN UE	43	12105
MENSAJES DICTADOS	23	0
MENSAJES ESPECIALES	32	0
MENSAJES INTERNACIONALES	2	0
MENSAJES MOVISTAR	385	0
MENSAJES OPERADORES NACIONALES	908	0
RESTO DE TRAFICO NACIONAL	28	7103
SERVICIOS EMOCION	5	0
SMS ILIMITADOS	1703	0
TRAF NACIONAL OTROS OPER. MOVILES EN UE	1	128
TRAFICO NAC.OTROS OPER.MOVILES	97524	16675449
TRAFICO NACIONAL A FIJOS	9425	2552334
VIDEOTELEFONIA NACIONAL	9	2084

- Red Inteligente – 900

TIPO DE TRAFICO	LLAMADAS	MEGABYTES
Fijo - Fijo Nacional	298	54743
móvil - Fijo Nacional	1019	214783
Internacional- Fijo Nacional	2	263

- Datos

TIPO DE TRAFICO	LLAMADAS	MEGABYTES
DATOS INTERNET	34065	2871300,7
DATOS INTERNET EN UE	25	4061,92
MENSAJES MULTIMEDIA	35	3,97

2.3.2. ***REQUERIMIENTOS***

Se requiere la implantación de un sistema de telefónica que contemple e integre tanto la telefónica "tradicional" fija de VoIP con la telefonía móvil incluso voz a través de softphone.

2.3.2.1. Funcionalidades Globales

La solución de voz corporativa suministrada deberá comportarse como un único sistema global y unificado de comunicaciones de voz entre todos los puestos de la organización, y como tal contará con las siguientes funcionalidades (como mínimo equiparables a Cisco Call Manager + Cisco Unity) para cualquier tipo de extensión (Fija/móvil/soft):

- La central o sistema de gestión de llamadas estará en la red del proveedor y se proveerá en modo servicio Cloud por lo que Mutua Montañesa no tendrá que preocuparse de elementos físicos referentes al servicio de centralita.
- La solución de voz conectará entre sedes y con la red pública sobre la red corporativa de datos objeto de la presente licitación la cual, deberá aportar los mecanismos de calidad de servicio y reserva de ancho de banda para garantizar la calidad de la voz. Los terminales móviles podrán hacer uso de tecnologías VoLTE para poder cursar llamadas a través de la red wifi-corporativa.
- Funcionalidades básicas de Voz a nivel de extensión:
  - Desvío de llamadas
  - Captura de llamadas
  - Grupos de Salto
  - Grupos de captura
  - Buzon de voz
  - Transferencia de llamadas (Directa y Ciega)
  - Multiconferencia con capacidad de un mínimo de 5 participantes.
  - Aparcamiento de llamadas
  - No Molestar
  - Rellamada
  - Identificación de numero llamante.
  - Selección de numero de presentación
  - Jefe/Secretaria
  - ....
- Directorio Único Corporativo: Integrable con MS Active Directory será consultable a través de los terminales tanto fijos como móviles de la organización a modo de páginas blancas. La consulta se realizará mediante sincronización del Directorio de Mutua Montañesa con el sistema de gestión de directorio que el proveedor proponga como solución. En ningún caso estará permitido la consulta directa de ningún dispositivo al directorio activo, para la obtención de datos de directorio.
- Plan Numérico Corporativo: Basado en 4 cifras para las extensiones internas y los números de marcación rápida (Agenda Global de contactos externos). Para las extensiones móviles se podrá tener extensión a 5 dígitos 6+<ext fija del usuario>
- Tarifa plana de llamadas de voz tanto desde extensiones fijas como móviles. Mutua Montañesa hará un uso razonable y adaptado a sus necesidades de las llamadas de voz, sin que exista posibilidad de regularización económica ni por exceso ni por defecto del volumen de llamadas realizadas. Ver apartado anterior como referencia de la volumetría actual, de manera no vinculante.
- Las llamadas realizadas entre numeraciones de Mutua Montañesa (tanto fijas como móviles) tendrán carácter de llamada interna y por lo tanto sin coste por ningún tipo de concepto (establecimiento, duración,....)
- Posibilidad de establecer restricciones de manera global o individualizada por extensión (bloque de llamadas a números de facturación adicional, llamadas internacionales,....)
- Discriminación automática de número externo. No será necesario marcar ningún numero específico para acceder a líneas externas (Ej. 0 ó 9) sino que se marcará el numero publico directamente y el sistema será capaz de discernir el tipo de llamada y ejecutarla según las rutas establecidas

- Numeración Pública: Las extensiones podrán tener asignada numeración publica, manteniendo las existentes actualmente y ampliándola, sin coste adicional en caso de ser necesario. Los números de acceso a la red pública estarán centralizados en la red del operador, pero se mantendrá la regionalización de los mismos. La publicación de dichos números en listas públicas de numeración (Páginas Blancas, Amarillas,....) deberá ser autorizada de manera expresa por Mutua Montañesa.
- Se mantendrá toda la numeración publica actual en todas las dependencias (incluyendo DDIs), haciéndose uso de la portabilidad en el caso de cambio de operador. Si se diese esta circunstancia, el operador adjudicatario indicará claramente los procesos y tiempos que empleará en dichos cambios
- Numero de presentación: Se podrá elegir mediante configuración el nº de presentación de una extensión, pudiendo ser este un DDI de cabecera, un DDI directamente asignado o un numero móvil tanto individual como de grupo a 9 digitos.
- Locuciones y operadora automática: El sistema permitirá la asignación de locuciones de bienvenida y guiado de la llamada individualizadas para cada una de las sedes de Mutua Montañesa
- Sistema de registro y explotación de las llamadas: Se dotará de un portal de consulta del sistema de registro de llamadas que permita la elaboración de informes y el análisis detallado e individualizado hasta el nivel de una llamada concreta. El sistema permitirá poder trazar una llamada desde su inicio pasando por los diferentes saltos que de en la organización hasta su final. Dicho sistema deberá ser fácil de operar por parte del gestor que mutua designe, permitiendo la elaboración de informes propios bajo demanda.
- Canales de presencia en redes públicas. El operador proveerá de los enlaces suficientes y necesarios para garantizar todas las llamadas de voz que la organización emita/reciba (fijo-fijo, fijo-movil,móvil-movil). Dicha conexión deberá estar virtualizada en la red del operador, garantizando en todo momento la estabilidad de las comunicaciones mediante diversificación geográfica y de accesos.
- El dimensionamiento de canales deberá garantizar una probabilidad de bloqueo máxima del 1%. A efectos de este pliego, se entiende por probabilidad de bloqueo: la probabilidad de que al establecer una nueva llamada (entrante o saliente), ésta no pueda cursarse por falta de canales telefónicos libres.
- Posibilidad de integración con otras centrales para o entornos para uso de funcionalidades avanzadas
- El proveedor deberá colaborar de forma activa para facilitar integraciones entre los sistemas de Mutua montañesa y la central de telefonía como por ejemplo para identificacion de llamadas entrantes que generen un mensaje o POPUP a un usuario o "Click to Call" que permita activar una llamada desde una aplicación corporativa. En este caso el proveedor deberá proveer capacidades de integración tipo API o similar para llevar a cabo estas integraciones.
- Se valorará la existencia de servicio IVR básico que permita dirigir la llamada a un destino mediante locuciones y arboles de decisión.
- Se valorará la existencia de modulo de CallCenter que permita funcionalidades avanzadas propias de este tipo de extensiones.
- IM mensajería. El sistema deberá permitir la integración de un servicio de presencia y mensajería instantánea interna. El cliente de dicho sistema deberá ser compatibles e implementado en la plataforma Citrix XenAPP 7.15 sobre Windows Server 2012 existente en Mutua Montañesa. Dicho servicio será necesario durante los 6 primeros meses del proyecto hasta que MM implante una solución de Ofimatica integrada que englobe la mensajería instantánea

2.3.2.2. Voz Fija

El proveedor deberá dotar de terminales de VoIP de una marca de reconocido prestigio y compatible con la totalidad de los servicios comunes indicados, valorándose positivamente que los terminales sean de marca CISCO si esto supone una mejora acogida formativa por parte de los usuarios, que ya están acostumbrados al funcionamiento y menús de la marca. Los terminales suministrados deberán ser de dos tipos:

- Usuarios: 220 Terminales básicos con las siguientes características mínimas:
  - Pantalla monocromo 3,5”
  - Multilinea
  - 2 puertos Ethernet 10/100BASE-T
  - PoE
  - Teclas de línea, navegación, servicio,volumen,Play/pausa, Transferencia y conferencia, auricular/altavoz/handset
  - Sonido banda ancha en el teléfono y en el puerto para cascos
  - Protocolo SIP y SCCP
  - Altavoz Full Duplex
  - Toma auriculares conector USB para compatibilidad con PC
  - Soporte regulable
  - Acceso al directorio corporativo
  - Acceso a Memoria del terminal
  - Posibilidad de montar en pared. Se suministrarán los accesorios necesarios para aquellas ubicaciones en las que así se requiera

- Recepcionistas/Dirección 10 Terminales con módulo de expansión: Se empleará el mismo terminal que para los usuarios normales o uno con pantalla más grande pero provisto de una unidad de expansión para el control de líneas. que permita la monitorización de al menos 25 extensiones.

Se plantea un escenario en el que los usuarios con terminal móvil corporativo (aprox 80) prescindan de terminal fijo de sobremesa. Para ellos será condición indispensable poder realizar desde el terminal móvil de manera directa mediante menús simples nativos en el interfaz del teléfono (sin empleo de códigos de marcación) de las tareas habituales de gestión de llamadas como pueden ser:

- Captura de llamada
- Pertenencia a grupo de salto de igual manera que un teléfono fijo
- Transferencia de llamadas con y sin consulta
- Búsqueda en directorio corporativo
- Multiconferencia

En el caso de que estas funcionalidades no sean posibles desde el terminal móvil de manera directa, el proveedor dotará sin coste tantos terminales como se requieran (hasta el máximo de líneas móviles incluidas en este proyecto) para cubrir la necesidad de dotación a aquellos usuarios que por su operativa diaria no puedan prescindir de estas funcionalidades.

El 80% de los terminales deberán incluir auriculares, valorándose positivamente que los mismos sean USB compatibles con el uso en PC.

2.3.2.3. Líneas RTB y Fax

Se deberán facilitar líneas de teléfono RTB o similar para los siguientes servicios (Ascensores, Alarmas, Equipos de medición, …):

Sede	Teléfono
Madrid	914299316
Barcelona	934108808
Ataulfo	942204135
HRN	942204157

Dichas líneas están previsto que en el plazo de un año pasen a ser líneas móviles. Dicho cambio deberá estar incluido en la presente licitación (solo a nivel de línea).

Así mismo el proveedor deberá proporcionar las 30 DDI/líneas RTB existentes (se deberá mantener la numeración actual), que permita tanto el envío como la recepción de FAX

Mutua Montañesa hará un uso muy restrictivo del FAX limitando al máximo su uso retirando el servicio paulatinamente de la organización a lo largo de la vida de este proyecto,

reduciendo, mediante desvíos en red de DDIs a las 5 sedes principales (Central, HMM, Territorial Norte, Territorial Este, Territorial CyL y Extremadura).

2.3.2.4. Red Inteligente – Linea 900

Mutua Montañesa posee un numero de red inteligente 900 para atención al mutualista servicio que deberá estar incluido en la presente licitación hasta el 30 de junio de 2023, momento en el que dicho número se dará de baja. El número que se mantendrá es:

- 900180875

Durante los meses previos a la baja se procederá a activar una locución y posterior desvío indicando que el nº de teléfono va a cambiar por un numero de tarificación normal.

2.3.2.5. Voz Móvil

Se requiere de un mínimo de 80 líneas móviles con un 5% de tolerancia sin incremento de coste con las siguientes características:

- Llamadas de voz ilimitadas
- Franquicia de datos mínima de 10 GB mensuales para el 90% de las líneas e "ilimitado" a máxima velocidad para el 10 % restante. Las líneas con franquicia, una vez consumida verán reducida su velocidad, en ningún caso se podrá cortar el servicio o llevar a cabo facturaciones adicionales
- Multisim hasta un máximo de 2 dispositivos adicionales por línea y posibilidad de uso de ESIM en aquellos terminales que lo soporten.
- 5g donde y cuando el operador de cobertura sin coste adicional.
- Capacidad de establecer perfiles de uso para gestionar los servicios y capacidades por grupos de línea, pudiendo establecer restricciones de uso como (llamadas en roaming, datos en roaming, límite de facturación individual de la línea, …)
- Servicios de valor añadido (mensajería de voz, envío y recepción de mensajes cortos o SMS, envío y recepción de mensajes multimedia o MMS, etc.).
- Envió de SMS Masivo que permita la integración de dicho envío con los sistemas corporativos de la organización.
- Bonos de datos internacionales. Aunque de carácter muy residual (en el ultimo año solo se contrataron 2 bonos mundiales de datos de un mes cada uno para una línea) estarán incluidos un numero de bonos de datos mundiales. Dichos bonos se activarán por meses individuales para casos muy excepcionales de necesidades de conexión de trabajadores en el extranjero (fuera de Zona 1)
- Posibilidad de Tarjetas Duales con función dual empresa/Privado la cual mediante un cambio de pin permitirá el acceso a una y otra línea. Dicho servicio, ni los desvíos oportunos para su funcionamiento tendrán un coste ni para Mutua Montañesa ni para el empleado que decida hacer uso de manera particular de esta opción. En su defecto se deberá poder garantizar la funcionalidad mediante dispositivos y tarjetas con doble sim Física/Virtual.
- Se deberá garantizar la portabilidad de los números actuales en caso de ser necesaria por cambio de operador.

Tal y como se ha indicado anteriormente las líneas móviles estarán completamente integradas en la organización como si de cualquier otra línea de comunicaciones se tratase, pudiendo formar parte de grupos de salto mixtos (Fijos y móviles), grupos de captura, realizar transferencia de llamadas, … incluso poder disponer asociada a la línea móvil de un número de teléfono de red fija que pueda ser empleado tanto para recibir como para emitir llamadas desde el terminal móvil, con numero de presentación fija.

Los servicios de comunicaciones móviles deberán estar soportados por estaciones base con tecnología digital de última generación que satisfagan las recomendaciones y normativas internacionales, siendo el adjudicatario responsable del diseño de la arquitectura de red que soportará el servicio.

Así mismo, la Red deberá ser actualizada de forma continua por el proveedor, adaptando el Servicio a las tecnologías vigentes y manteniendo las funcionalidades más avanzadas en el servicio prestado.

El proveedor garantizará una cobertura suficiente de telefonía móvil tanto para voz como para datos (estos últimos en modo mínimo 4G) para todas las delegaciones de Mutua Montañesa . En caso de detección de zonas de sombra en el interior de los locales, correrá por cuenta del proveedor las medidas correctivas necesarias para la garantía de dicha cobertura.

Terminales

Se requiere el suministro de 2 modelos de terminal con los siguientes requerimientos mínimos:

- Terminales Tipo 1. Gama Alta (25% del Parque). Modelo actual a modo de referencia no vinculante iPhone 11 128GB
  - S.O.: IOS o Android
  - Pantalla: >5" y <6,2" resolución mínima 2.340 por 1.080 píxeles
  - Procesador: 64 bits Octacore, A14 o similar...
  - Memoria Interna: 128 GB
  - Dispositivo de seguridad biométrico para acceso al terminal
  - Peso <=169 gr
  - Batería que permita:
    - Tiempo de conversación en 4G hasta 14 Horas
    - Tiempo de Navegación/internet en 4G 10 Horas
  - Conectividad:
    - GSM/EDGE
    - UMTS/HSPA+
    - DC-HSDPA
    - 4G LTE
    - 5G
    - Wi-Fi 802.11a/b/g/n/ac/ax MIMO 2x2
    - Bluetooth 5.0
    - NFC
    - GPS,Galileo y GLONASS
  - Acceso a correo electrónico corporativo Exchange 2007
  - Compatible con VPN-Ipsec Cisco/Fortinet
  - Visor de documentos Word/excel/pdf/imágenes

- Terminales Tipo 2. Gama media(75% del Parque) Modelo actual a modo de referencia no vinculante Samsung Galaxy A50
  - S.O.: IOS o Android
  - Pantalla: 6,5" o superior
  - Procesador: OctaCore 1,8 Mhz op superior
  - Memoria Interna: 128 GB
  - Peso <194gr
  - Dual SIM
  - Batería que permita:
    - Tiempo de conversación en 4G hasta 30 Horas
    - Tiempo de Navegación/internet en 4G hasta 15 Horas
  - Conectividad:
    - GSM/EDGE
    - 3G UMTS/HSPA+
    - 4G LTE
    - 5G
    - Wi-Fi 802.11 b/g/n
    - Bluetooth 5.0
    - NFC
    - GPS,Galileo y GLONASS

- Auriculares 3.5 mm
- Cargador
- Acceso a correo electrónico corporativo Exchange 2007
- Compatible con VPN-Ipsec Cisco/Fortinet
- Visor de documentos Word/excel/pdf/imágenes

Los licitadores deberán incorporar en sus propuestas técnicas al menos dos modelos de terminales para el tipo 1 (uno por cada S.O. Admitido) y al menos tres para el tipo 2, seleccionando Mutua Montañesa el modelo que considere más adecuado para cada tipo. La oferta debe comprender, en su caso, todas las licencias necesarias para cumplir los requisitos técnicos especificados.

Renovación de Terminales

Los terminales deberán proveerse al inicio del contrato y estarán sujetos a una renovación tecnológica de todo el parque a los 30 meses de contrato por terminales de iguales o superiores características a los provistos en el arranque del servicio, preferiblemente por el modelo de sustitución que marque el fabricante como evolución del anterior, siendo en todo caso aprobados por Mutua Montañesa.

Devolución de Terminales

Dada la modalidad de servicio que rige la totalidad de la presente licitación Mutua Montañesa se compromete a la devolución de todos los terminales suministrados por el proveedor, tanto los de provisión inicial como los terminales renovados al cese del contrato. Para ello, Mutua Montañesa, dispondrá de 2 meses desde la entrega de los terminales de reposición o del fin del contrato (según la remesa a devolver) para la devolución de los terminales entregados. Mutua Montañesa no se responsabilizará del estado de los terminales a su entrega. En el caso de perdida o robo de alguno de los terminales, Mutua Montañesa no estará obligado a reponer/resarcir de ninguna manera al proveedor.

Dentro del cumplimiento de las medidas de seguridad exigibles a este proyecto, el proveedor deberá certificar la destrucción de los datos de todos los terminales que se le entreguen, ya sea por avería o por devolución.

Mantenimiento de Terminales Móviles

El operador deberá ofrecer un servicio de garantía y mantenimiento de líneas y terminales durante la vigencia del contrato. El operador deberá dar soporte para que todos los usuarios cuenten con líneas y terminales plenamente operativos, actualizados y capaces de soportar los servicios contratados en todo momento.

La comunicación de las incidencias técnicas y la solicitud de solución deben poder realizarse todos los días laborables en horario de atención al público, por teléfono o correo electrónico. Sin embargo, la comunicación de las incidencias graves y su solicitud de solución, como la suspensión de línea por pérdida o robo del terminal, se deberá poder realizar por vía telefónica 24 horas al día los 365 días del año.

El servicio de mantenimiento deberá primar la disponibilidad en el menor tiempo posible de un terminal operativo para cada usuario El proveedor indicará el procedimiento a seguir, para la sustitución/reparación de equipos con incidencia. El proveedor deberá dotar a la organización de una stock mínimo (2 equipos gama alta,3 equipos gama media) en depósito, de terminales para reposición, los cuales se repondrán en la medida que se vayan reparando, no pudiéndose dar el caso de estar en stock 0 durante mas de 24 horas y tratando siempre de respetar los modelos homologados durante el periodo de contrato.

El proveedor se responsabilizará de que la información almacenada en los terminales que se envíen a reparar sea debidamente borrada para impedir el acceso a sus datos. En caso de que no pueda borrarse el dispositivo móvil por imposibilidad de acceso al mismo el proveedor procederá a la destrucción del terminal para impedir el acceso a la información contenida y por tanto su posterior utilización

Asimismo, en caso de extravío, hurto o robo, el proveedor facilitará un terminal móvil de sustitución tramitándose previamente la correspondiente denuncia, de modo que el stock de terminales se mantenga. las propuestas podrán consignar un porcentaje máximo de terminales a entregar sin coste para atender estas incidencias, que no podrá ser inferior a un 5 por ciento anual, por cada tipo de terminal suministrado.

2.3.2.6. Gestión

El proveedor dotara de un servicio de ventanilla única para todas las gestiones referentes a la telefonía. Así mismo dotara a Mutua Montañesa de un servicio web en el que poder llevar a cabo de manera autónoma el mayor número de gestiones tanto administrativas como técnicas sobre las líneas como, por ejemplo:

- Alta administrativa de línea.
- Cambio de dirección de facturación.
- Cambio de datos bancarios.
- Cambio de número de teléfono.
- Introducción de IMEI en tabla de robados.
- Suspensión/rehabilitación, robo o pérdida.
- Activación/rehabilitación bajas temporales.
- Asignación/anulación número de pedido de terminales.
- Asignación/anulación número de pedido de tarjeta SIM.
- Asignación/anulación número de avería de servicio posventa.
- Provisión de códigos de seguridad (PIN, PUK).
- Mantenimiento de agrupaciones.
- Bajas de línea.
- Correcciones de Bajas/Altas de líneas
- Cambio de Tarjeta SIM

2.3.2.7. Softphone

Para los usuarios en movilidad, inicialmente, siendo posible una futura ampliación a más perfiles, se deberá dotar de un sistema de cliente de voz por software (SoftPhone) compatible con equipos Windows 10 PRO y Windows Server 2012 o superior. Así mismo el software suministrador deberá ser compatible para su uso en la plataforma CITRIX XENAPP existente basada en Windows Server 2012 con Citrix XENAP 7.15 o superior.

El cliente SoftPhone permitirá las funcionalidades básicas de igual manera que el resto de terminales propuestos y se integrará como si fuese un dispositivo mas de gestión de llamadas de tal manera que los usuarios en movilidad puedan atender indistintamente las llamadas desde su terminal fijo/móvil o SoftPhone.

2.4. SEGURIDAD

Mutua Montañesa esta especialmente sensibilizada con la necesidad de reforzar y mantener unos niveles de seguridad elevados propios de una organización seria y moderna como esta. En este sentido, y entre otras actuaciones, Mutua Montañesa está en proceso de certificación del Esquema de Seguridad Nacional en nivel Medio, lo que refuerza y por otra parte también condiciona las necesidades en cuanto a seguridad respecta.

Será requerimiento general del proyecto, observar y garantizar todas las medidas de seguridad necesarias para todas sus fases, desde este pliego hasta la ejecución y cese del servicio, pasando por el diseño e implantación. Para ello el proveedor deberá estar

certificado en el Esquema Nacional de Seguridad valorándose el nivel de certificación obtenido para los mismos.

Uno de los aspectos que más peso tendrá en las valoraciones será la seguridad global de la solución propuesta presentada por el proveedor a todos los niveles (WAN/LAN/WIFI/…) y las capacidades de adaptación a nuevas necesidades y elementos de protección.

2.4.1. ***SEGURIDAD PERIMETRAL***

Situación Actual

Actualmente se dispone de una tecnología de Fortinet para la protección del perímetro de red de la organización. Esta plataforma, en modo servicio, esta compuesta por 2 FW Fortigate 201E en cluster Activo-Pasivo y un equipo adicional idéntico en standby fuera del cluster y ubicado en el CPD de Respaldo. Así mismo, para la gestión y conservación de logs se dispone de un sistema Fortinalyzer y de un sistema de mta de correo fortimail destinado principalmente para la encriptación de correo de manera transparente mediante el servicio IBE de este fabricante Tanto el analizador de log como el mta de correo se encuentran virtualizados mediante VMWare

Requerimientos

Se requiere la implantación/soporte/mantenimiento/operación en modo de gestión compartida de un sistema de seguridad que integre la totalidad de la red de la organización. Se valorará positivamente dentro de la solución global que aporte el proveedor la capacidad de orquestación de todos los elementos de red objeto de esta licitación en lo que a el sistema de seguridad global respecta, con posibilidad de establecer políticas de seguridad a nivel WAN de manera centralizada con capacidad de IPS/IDS/antivirus/control de aplicaciones por sede.

A nivel de CPDs se requiere el empleo de soluciones completamente redundantes que contemple tanto el CPD principal como el CPD de respaldo (este último es de contingencia por lo que no tendrá tráfico salvo en pruebas de continuidad de negocio o incidente critico), A nivel de cpd principal y de backup se requiere de un cluster de equipos Activo pasivo al menos en el CPD principal y una miembro de cluster en stand by o solución alternativa para el CPD de respaldo. En cualquier caso, estos equipos de cabecera deberán cumplir las siguiente funcionalidades mínimas, completamente licenciadas:

- Firewall de aplicación capa 7, capaz de gestionar la seguridad a nivel de usuario y aplicación. la necesidad actual de securización pasa por la identificación de las aplicaciones y la gestión de quien puede o no generar y cursar un tráfico de red para una determinada ubicación, más allá del equipo o red a la que esté conectado.
    - Mínimo de 4000 aplicaciones activas actuales (incluyendo aplicaciones Web 2.0) pudiéndose agregar firmas manuales para otras aplicaciones
    - La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías / subcategorías (control granular dentro de la aplicación)
    - Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.
    - Capacidad para identificar las aplicaciones bajo túneles HTTPS.
- Solución de alta disponibilidad física
- Fuentes de alimentación redundantes en cada equipo
- Enrutamiento L3 de toda la red corporativa con capacidad RIP v2, OSPF, BGP y Multicast para IPv4 e Ipv6. Routing basado en políticas,NAT
- Puetos 100/1000 y 10G para CPD principal con capacidad de agregación LCAP
- Posibilidad de SSL Offloading para trafico HTTPS y balanceo web
- 5 Gbps mínimo de throughput con todas las protecciones habilitadas valorándose positivamente un incremento de rendimiento en los equipos del CPD principal
- Puerto especifico de management
- Puerto Especifico clustering HA
- Capacidad de agrupación de interfaces por zonas para definición de reglas de filtrado

- Solución de Sandboxing en la nube a la que se remitirán todos aquellos ficheros cuyo hash no se encuentre ya registrado en la bbdd del fabricante, obteniendo un veredicto en el menor tiempo posible. El fabricante deberá certificar la ubicación geográfica de sus sistemas de Sandboxing sin que en ningún caso puedan ser remitidos a países que no formen parte de la Unión Europea.
- Thread Prevention
- Filtrado URL por usuario de directorio activo, con posibilidad de filtrar e identificar unívocamente y sin necesidad de solicitud de usuario y contraseña, las acciones de red generadas por un usuario a nivel de navegación, independientemente de si el usuario cursa el tráfico desde su equipo o desde una sesión ICA de terminal contra un servidor con Citrix Virtual Apps.
- Identificación de usuarios
    - Identificar usuarios, integrándose con Microsoft Active Directory y Novel eDirectory
    - Control de usuarios Citrix.
    - Control de usuarios de Microsoft Terminal Server.
    - Soporte de mensajes Radius Accounting para SSO.
    - Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+
- Funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP.
- Reporting avanzado con un periodo de retención mínimo de un año.
    - Top sitios visitados
    - Top usuarios por ancho de banda
    - Informe detallado de actividad de un usuario
    - Amenazas
    - Eventos de seguridad y acciones ejecutadas
- Posibilidad de generar notificaciones por correo ante:
    - Detecciones de severidad alta o critica en cualquiera de sus motores
        - Url Filtering
        - Theat Prevention
        - Sandboxing
- VPN IPSec
- VPN SSL portal y Tunel para clientes móviles (ios y android) y portátiles (windows 10 o superior) sin límite de clientes a nivel de licencia ni costes adicionales.
- MFA para conexiones VPN SSL para un mínimo de 20 clientes.
- IPS/IDS de aplicación
- Deberá permitir la creación de firmas específicas de IPS.
- Autenticación unificada. Active directory y controlador wifi
- Data Loss Prevention basada en patrones predefinidos o creados específicamente por el administrador.
- Balanceo de salidas en Internet de forma dinámica (sd-wan).
- Gestión Web para el mayor número de configuraciones posibles. Sera penalizada aquella oferta que presente un alto nivel de complejidad en su operativa y requiera el uso de consolas de terminal para realizar análisis o troubleshooting de manera común.

Se requiere que el fabricante propuesto, figure en el apartado de líderes del cuadrante mágico de gartner de Network Firewalls 2020

Deberá existir publicadas las guías de empleo seguro para el fabricante del FW dentro del catálogo del Centro Criptológico de Seguridad, CCN-STIC, que el proveedor deberá respetar y seguir durante su implantación.

2.4.2. *LOG REPORTING Y GESTIÓN*

A nivel de log y reporting, se requiere de un sistema cloud que almacene todos los logs de trafico generados con un periodo de retención mínimo de 1 año. Esta herramienta de log y reporting será capaz de aglutinar no solo los logs de los propios equipos de seguridad sino que permitirá el envío de eventos desde otros sistemas como switches mediante syslog o integración nativa con el sistema de log suministrado.

Así mismo se valorará positivamente la capacidad de tener una herramienta de gestión global de la seguridad de todos los elementos que componen la solución.

2.4.3. *TEST INTRUSION*

El proveedor deberá realizar 2 test de intrusión en modalidad caja negra (a los 6 meses y 30 meses de contrato respectivamente) y entregar los resultados de la misma así como un informe de medidas a implantar para la corrección o mejora de los resultados del informe.
Aquellas que dependan de la infraestructura objeto de este contrato deberán ser implantadas de inmediato tras acuerdo con el Dpto de Sistemas de Mutua Montañesa

2.4.4. *GESTION COMPARTIDA Y CENTRO DE RESPUESTA (SOC)*

El sistema de seguridad se contemplará en modalidad de gestión compartida, con el fin de garantizar la máxima flexibilidad a la hora de dar respuesta a las necesidades de la organización Mutua Montañesa deberá tener capacidad de gestión de los equipos suministrados a nivel de seguridad que le permita de manera autónoma establecer reglas/perfiles de filtados/usuarios/Vpns/…

El proveedor deberá dotar de un servicio de soporte L2 y coordinación L3 y respuesta ante incidentes y amenazas de seguridad, con especialistas en los productos implantados y que esté completamente integrado en el equipo de soporte global del proyecto.

2.5. MDM

Para la gestión e inventario de los terminales asociados a las líneas móviles solicitadas (+ un 50 % adicional de dispositivos que puedan hacer uso de la facilidad multisim) se requiere un sistema de gestión de dispositivos móviles (MDM).

Las funcionalidades que debe incorporar el servicio propuesto son las siguientes:

- A nivel de dispositivo:
  - Inventario hardware y software de los terminales móviles.
  - Configuración remota de dispositivos en función de los diferentes perfiles.
  - Bloqueo de funcionalidades del dispositivo (cámara, bluetooth,…).
  - Protección frente al robo del terminal (encriptado de datos, bloqueos, aplicar borrados selectivos o completos, requerir contraseña con determinada complejidad).
  - Gestión de acciones automáticas ante el incumplimiento por parte de un usuario de una política de configuración corporativa.
- A nivel de aplicaciones:
  - Catálogo corporativo de aplicaciones en función de perfil de usuario. Se debe poder controlar permisos para instalar las aplicaciones en los dispositivos (en base al perfil de usuario).
  - Actualizaciones, borrados de aplicaciones.
  - Capacidad de inhabilitar la ejecución de una aplicación.
  - Gestión de acciones automáticas ante el incumplimiento por parte de un usuario de una política corporativa sobre las aplicaciones.
- Capacidad de monitorización y generación de informes
- Gestion de configuraciones
  - Correo

- Requerir autenticación mediante usuario/contraseña para acceder al correo
- Encriptado local del correo
- Capacidades de Data Loss Protection
- Impedir la descarga de archivos adjuntos de un correo
- Establecer el tamaño máximo de los archivos adjunto de un correo
- Habilitar el cifrado de los adjuntos
- Dominios restringidos: listas blancas/negras de dominios para remitir correos

- VPN
  - Posibilidad de distribuir configuraciones de VPN de manera centralizada.

Dicho sistema se facilitará en modo servicio, con posibilidad de ejecutar de manera autónoma, al menos las funcionalidades básicas del sistema (Consulta de inventario, Bloqueo/borrado/reactivacion del Dispositivo, Forzado de políticas, Notificación push,....)

3. LOTE 2. LINEA DE ACCESO A LA GISS

La Gerencia Informática de la Seguridad Social mantiene una serie de conexiones con Entidades externas (entidades colaboradoras y organismos públicos) para el intercambio de datos. Dichas conexiones se realizan a través de una VPN IP de Extranet, apoyada sobre MacroLan, (CCEE).

Para el acceso a la VPN IP la GISS dispone, tanto en el CPD Principal como en el CPD Secundario, de dos encaminadores Cisco ASR 1001-X.

Dado que la comunicación se realiza apoyándose en una MacroLan compartida con distintas Entidades, los requisitos de seguridad exigen que la conexión en esta red separada se realice tunelizada en túneles 1 a 1 que finalizan los ASR 1001-X, en los que un extremo es siempre la GISS y el otro extremo la Entidad externa conectada, impidiendo de esta forma la suplantación o el desvío de tráfico por errores de configuración.

La GISS actúa como promotor de la conexión, siendo la adquisición del equipamiento y las líneas en el extremo de la Entidad externa responsabilidad de la misma. En este sentido Mutua Montañesa como Mutua Colaboradora con la Seguridad Social, tiene la necesidad y obligación de conectar sus sistemas con la Gerencia Informática de la Seguridad Social para el intercambio de datos inherentes a nuestra actividad y naturaleza de entidad colaboradora.

Por lo tanto, se requiere de una conexión directa mediante VPNIP (FFTO o similar)con 10 MB de ancho de bando completamente dotada y configurada a dicha red de la GISS con backup 4g y accesible desde los dos CPDs de Mutua Montañesa en Santander descritos en el Lote 1.

En el caso de ser adjudicatario del Lote 1 se permitirá el uso de los equipos objeto de dicho lote 1 para establecer dicha conexión con un caudal equivalente al indicado en estos requerimientos mediante técnicas de multVRF o similar.

4. DESPLIEGUE, SOPORTE Y ANS

Este punto afecta a ambos lotes de esta licitación.

4.1. PLAN DE DESPLIEGUE

El licitante presentará un plan de despliegue detallado que tenga una visión global de todo el proyecto y un despliegue detallado por cada uno de los servicios demandados en todos los lotes. Dicho plan no podrá exceder de 90 días naturales desde la firma del contrato, para los servicios incluidos en este contrato.

En el caso de que, para la diversificación de líneas el proveedor tuviese que acometer una obra civil, el plazo de ejecución de dicha diversificación será de un máximo de 9 meses desde la firma del contrato, no significando esto la no provisión de la línea objeto de dicha actuación, sino que dicha línea podre discurrir inicialmente sin diversificación hasta la realización de las obras necesarias.

Todas las tareas incluidas en este plan de puesta en marcha, que implique un impacto en el servicio a los usuarios, deberán minimizarse al máximo, ya que existe un servicio hospitalario que trabaja en horario 24x7. Será Mutua Montañesa, la que apruebe y fije la ventana horaria de trabajos para las tareas de migración de la red de comunicaciones, pudiendo esta ser en días festivos y horario nocturno, sin que esto suponga ningún tipo de coste adicional.

El plan de despliegue deberá tener en cuenta la minimización en la duplicidad de servicios con el operador saliente ya que Mutua Montañesa analizará y validará la implantación de servicios pudiendo condicionar el planning para evitar el pago por duplicado al operador saliente y entrante.

Para la implantación del Servicio, el adjudicatario nombrará a una persona debidamente cualificada que actuará como Jefe del Proyecto, con dedicación necesaria (completa o parcial dependiendo del grado de avance del proyecto) para Mutua Montañesa. Su objetivo será garantizar la implantación del proyecto con éxito y en el plazo requerido, realizando además funciones de interlocución y coordinación de trabajos con los responsables de Mutua Montañesa.

Durante la fase de implantación de los servicios el adjudicatario estará obligado a la elaboración y presentación de informes de progreso que, entre otros, contendrán los puntos siguientes:

- Informe de situación y progreso del proyecto de implantación
- Re planificación sobre la inicial , gestión del cambio.
- Incidencias y problemas surgidos
- Principales Hitos conseguidos
- Sugerencia de acciones correctivas o preventivas.
- Revisiones de ítems para el próximo período
- En el caso de cambio de operador se detallará ampliamente todo el proceso y tiempo utilizado por el nuevo operador para el cambio de líneas, la portabilidad del plan de numeración, cambios para el direccionamiento público, … etc.

La periodicidad de los informes será quincenal durante la implantación.

4.1.1. *PLAN DE PRUEBAS*

Una vez formalizado el contrato, y como parte de la documentación necesaria para la etapa de despliegue, el adjudicatario deberá proponer un Plan de pruebas que permita comprobar el correcto funcionamiento de todos los nodos de la red.

El Plan de Pruebas propuesto deberá ser revisado de forma conjunta con Mutua Montañesa y ejecutado por el adjudicatario del lote según los protocolos de prueba que se acuerden. Durante el plan de pruebas el proveedor facilitará, cuando le sea requerido, un listado en formato electrónico (hoja de cálculo) que indique el contenido completo del plan de pruebas y su grado de evolución y cumplimiento según los requerimientos del pliego.

Dicho plan de pruebas deberá perseguir minimizar al máximo los trabajos de prueba y validación de la solución propuesta por parte de personal de Mutua Montañesa, con el fin de que ante un despliegue de estas características y con las restricciones de tiempo existentes, no se conviertan en un cuello de botella para el proveedor. Entre estas actividades que deberá tener en cuenta el proveedor, estarán la generación de manuales, formación de usuarios, adaptación de procedimientos de uso,…

Una vez finalizado el plan de pruebas, Mutua Montañesa dará por concluido el proceso de aprovisionamiento y puesta en marcha del servicio, comenzado la fase de mantenimiento y operación de este.

4.1.2. *FORMACIÓN*

El proveedor deberá indicar en su propuesta un plan de formación diferenciado tanto para los usuarios internos como para los usuarios técnicos de mutua montañesa. Se valorará la calidad y detalle de este plan de formación.

4.1.3. *PORTABILIDAD DE NÚMEROS TELEFÓNICOS*

Como ya se ha indicado, en caso de ser necesario, correrá por cuenta del ofertante las tareas de solicitud y portabilidad de la totalidad de números públicos de los que Mutua Montañesa dispone tanto fijos como móviles, manteniendo su regionalización cuando corresponda y reglas de enrutamiento, tal y como están en la actualidad. Dicho plan de portabilidad deberá ser presentado en la fase de implantación y aprobado por Mutua Montañesa

4.2. SOPORTE

El soporte del proyecto deberá realizarse en la medida de los posible con un modelo de ventanilla única en la que se centralice todas las solicitudes/incdencias del servicio. Dentro de este modelo de ventanilla única deberá existir las siguientes figuras básicas para el soporte en explotación que serán:

- **Asesor Técnico**: Contacto técnico a nivel global. Su misión debe ser la de canalizar las necesidades técnicas que se puedan presentar y gestionar esas necesidades dentro de la empresa que da el servicio. Sera también el responsable de escalar y gestionar aquellas incidencias que por su criticidad o por que cualquier otra índole sea necesario focalizar el esfuerzo. El recurso no deberá tener dedicación exclusiva pero si
- **Ingeniero de soporte**: Interlocutor técnico principal a nivel de configuración y resolución de incidencias de red. Deberá conocer los pormenores de la totalidad de la infraestructura desplegada por el proveedor en Mutua Montañesa. El acceso a dicho recurso se hará de manera directa a través de teléfono móvil o mail. Dicho perfil tendrá potestad para llevar a cabo cambios de configuración inmediatos por requerimientos del servicio o ante situaciones imprevistas.
- **Comercial asignado a la cuenta**: interlocutor comercial con conocimiento de toda la red y productos que Mutua Montañesa tiene contratado. Deberá ejercer también como promotor de nuevas acciones y canalización de lo que el proveedor como socio tecnológico de Mutua Montañesa pueda proponer como respuesta a las necesidades del sector o tendencias del momento.

La asignación de estos perfiles deberá ser estable, una rotación superior a 12 meses de servicio/perfil sin una causa justificada y válida para Mutua Montañes, podrá suponer penalización al proveedor.

4.2.1. *CENTRO TÉCNICO DE SOPORTE*

El adjudicatario pondrá a disposición de Mutua Montañesa un centro de gestión y soporte técnico para la totalidad de los elementos contenidos en la presente licitación. Dicho centro unificará la interlocución técnica entre Mutua Montañesa y el proveedor.

El centro de soporte se encargará entre otras de las siguientes tareas:

- Interfaz con el Cliente.
- Creación, seguimiento y cierre de tickets.
- Informe periódico sobre el estado de una incidencia activa.
- Escalado en la organización
- Monitorización proactiva de la red 24x7x365.
- Modificaciones de equipos y configuraciónes de red.
- Consultas sobre reportes de rendimiento.
- Consultas sobre capacidad.
- Petición de pruebas.
- Peticiones de respaldo, filtrado o seguridad.
- Informes de ANS

La prestación del servicio de atención, gestión y mantenimiento por el adjudicatario deberá:

- cuando Mutua Montañesa así lo requiera, por su criticidad o impacto en la producción de los usuarios, acordar que las intervenciones se realicen fuera del horario laboral y en festivos.
- Notificar con una antelación mínima de 2 días laborables de aquellas actividades que puedan afectar al servicio.
- atender a la solicitud en cualquier momento de informes sobre las labores de gestión y mantenimiento realizadas por el adjudicatario. Dichos informes deberán entregarse en un plazo máximo de cinco días laborables desde su solicitud.
- Adicionalmente, el adjudicatario deberá entregar informes mensuales en los que se detalle el estado de las infraestructuras suministradas y los servicios que presta, así como el nivel de cumplimiento de los Acuerdos de Nivel de Servicio (en adelante ANS o SLA) contraídos con Mutua Montañesa. Dichos informes deberán incluir el detalle necesario para la aplicación inequívoca de los Acuerdos de Nivel de Servicio. A tal efecto, el adjudicatario deberá ajustar el formato y contenido de dichos informes hasta cumplir en cada momento con los requisitos exigidos por parte de Mutua Montañesa a lo largo de la duración del contrato.

4.2.2. ***HORARIO DE SOPORTE***

Con carácter general el servicio de soporte activo discurrirá en horario de 12x5 de 07:30 a 19:30 de Lunes a Viernes salvo Festivos de carácter nacional.

Sin embargo, para incidencias criticas (EJ: Incomunicación total o parcial de sedes CPD) el horario de soporte será en modalidad 24x7 y con unos acuerdos de nivel de servicio que a continuación se describen.

4.3. ANS Y GARANTÍA

4.3.1. ***CARÁCTER GENERAL***

El adjudicatario garantizará durante el periodo de vigencia del contrato los productos y equipamientos derivados de la presente contratación, a contar desde la fecha de puesta en marcha del proyecto. Durante este periodo estará obligado a realizar los cambios necesarios para solventar las deficiencias detectadas si así lo solicita Mutua Montañesa, así como las actualizaciones necesarias sobre todo en materia de seguridad de la información.

4.3.1.1. Disponibilidad de la infraestructura

Se define disponibilidad de la infraestructura como la capacidad que tiene la misma para permitir a un usuario acceder y usar los servicios objeto de este lote, cuando éste lo requiere y con el rendimiento y funcionalidad (de la plataforma) esperado.

La disponibilidad de la infraestructura se medirá por sede y en base a los 3 servicios fundamentales existentes en esta licitación y que son WAN, LAN y VOZ (solo WAN para Lote2):

- La infraestructura, en su totalidad, se considerará disponible cuando permita a los usuarios acceder y usar los servicios de voz, datos lan o wan objeto de esta licitacion, cuando éste lo requiera y con el rendimiento y funcionalidad requerido.

No se considerarán indisponibilidades de la infraestructura todas aquellas paradas planificadas y previamente notificadas y acordadas entre el proveedor y Mutua Montañesa . El adjudicatario deberá:

- Notificar la parada con un mínimo de 1 día de antelación.
- Informar del motivo de la parada
- Informar de la fecha y hora de inicio y de la fecha y hora de finalización de la parada
- Recibir la aceptación de Mutua Montañesa

Se considerará indisponibilidad de la infraestructura todo el tiempo que transcurra desde la fecha y hora planificadas de finalización de la parada hasta la fecha y hora real de vuelta de la disponibilidad de la infraestructura.

Será objetivo del adjudicatario la resolución de las indisponibilidades de la infraestructura en el mínimo tiempo posible. El adjudicatario y Mutua Montañesa, colaborarán en el diagnóstico y la resolución de las indisponibilidades de la infraestructura a fin de minimizar el impacto y el tiempo de restablecimiento del servicio.

Para establecer la disponibilidad objetiva se procederá a realizar la siguiente segmentación de sedes:

- Prioridad Alta
  - **Hospital Mutua Montañesa**
  - **Ataulfo Argenta**
  - **Sedes Tipo 1**
- Prioridad Media
  - **Sedes tipo2**
- Prioridad Estándar
  - **Resto de Sedes**

A pesar de la globalidad del servicio se establecen distintos ratios de disponibilidad dependiendo de la criticidad de la Sede según los siguientes criterios:

- **Disponibilidad >=99,85%, en horario 24x7 para sedes de prioridad alta:**
- **Disponibilidad >=99.70% en horario 24x7 para sedes de prioridad media**
- **Disponibilidad >=99.40% en horario 12x5 para sedes de prioridad estándar**

La fórmula a aplicar para el cálculo de la disponibilidad mensual de la infraestructura será la siguiente:

$$\%\ Disponibilidad\ mensual\ sede = \left(\frac{(1440 * DM) - TI}{1440 * DM}\right) * 100$$

Dónde:

- DM = número de días naturales del mes
- TI = tiempo de indisponibilidad (en minutos). Número de minutos en que la infraestructura no ha estado disponible

La disponibilidad mensual de la infraestructura de un mes determinado se calculará, por sede, durante los primeros 15 días del mes siguiente.

El adjudicatario entregará durante los 15 primeros días del mes, un informe que refleje el % de disponibilidad de la infraestructura correspondiente al mes anterior. Dicho informe deberá incluir una relación de las indisponibilidades acontecidas durante el mes anterior, incluyendo:

- Sede/s afectada/s

- Servicio/s afectado/s
- Fecha y hora de inicio de indisponibilidad de la infraestructura
- Fecha y hora de finalización de indisponibilidad de la infraestructura
- Motivo detallado de la indisponibilidad
- Solución adoptada
- Indisponibilidad SI/NO

Adicionalmente, el informe deberá también relacionar las paradas planificadas, incluyendo:

- Fecha y hora de notificación de la parada
- Previsión de fecha y hora de inicio de la parada
- Previsión de fecha y hora de finalización de la parada
- Fecha y hora de inicio reales de la parada
- Fecha y hora de finalización reales de la parada
- Motivo detallado de la parada

4.3.1.2. Resolución de incidencias

Se define incidencia de la infraestructura como la interrupción parcial no planificada de la capacidad que tiene la misma sobre el conjunto de los servicios requeridos y ofertados por el proveedor.

Ante una incidencia de la infraestructura se determinará su prioridad de resolución en base a los parámetros de impacto y urgencia de la misma, que se asignarán aplicando las siguientes tablas:

A. Impacto de la incidencia de la infraestructura. Se definen los siguientes tramos:
    a. Afecta a menos de 5 usuarios
    b. Afecta a menos de 15 usuarios
    c. Afecta a menos de 50 usuarios
    d. Afecta a 50 o más usuarios
B. Urgencia de la incidencia de la infraestructura. Se definen los siguientes tramos:
    a. Baja
    b. Media
    c. Alta
    d. Crítica

El impacto y la urgencia de cada incidencia de la infraestructura se acordarán entre el adjudicatario y la Mutua contratante.

En base a los parámetros acordados de impacto y a la urgencia de la incidencia de la infraestructura, se aplicará la siguiente matriz de prioridades:

Urgencias / Impactos	Afecta a menos de 5 usuarios	Afecta a menos de 15 usuarios	Afecta a menos de 50 usuarios	Afecta a 50 o mas usuarios
Baja	Baja	Media	Media	Alta
Media	Media	Alta	Alta	Alta
Alta	Alta	Alta	Crítica	Crítica
Crítica	Crítica	Crítica	Crítica	Crítica

Para cada una de las prioridades resultantes de esta matriz se establecen los siguientes tiempos máximos de resolución de las incidencias de la infraestructura, desde la fecha y hora de su comunicación:

A. Prioridad baja: Tiempo de resolución no superior a 36 horas laborables
B. Prioridad media: Tiempo de resolución no superior a 24 horas laborables
C. Prioridad alta: Tiempo de resolución no superior a 12 horas laborables.
D. Prioridad crítica: Tiempo de resolución no superior a 4 horas (24x7).

El horario laborable se establece de lunes a viernes, de 08:00h a 20:00h. excepto festivos de ámbito nacional y las tardes del 24 y 31 de diciembre

Será objetivo del adjudicatario la resolución de incidencias de la infraestructura en el tiempo máximo definido a partir de su comunicación y según la prioridad asignada. El adjudicatario, junto con Mutua Montañesa, colaborarán en el diagnóstico y la resolución de la incidencia de la infraestructura a fin de minimizar el impacto y el tiempo de resolución.

Se fija como objetivo mensual de resolución de incidencias de la infraestructura, la resolución de un mínimo del 90% de las incidencias de la infraestructura dentro de los plazos de tiempo establecidos.

Se valorará positivamente un incremento en el porcentaje de incidencias resueltas dentro de los tiempos indicados. El porcentaje final indicado por el proveedor en su oferta, se tomará como base para el cálculo de penalizaciones descrito en los puntos posteriores.

El porcentaje de resolución mensual de incidencias de la infraestructura dentro de los plazos de tiempo establecidos de un mes determinado se calculará durante los primeros 15 días del mes siguiente, mediante la siguiente fórmula:

$$\%\ Resolucion\ de\ Incidencias\ en\ plazo = \frac{Incidencias\ Resueltas\ en\ Plazo}{Nº\ Total\ de\ Incidencias\ aceptadas} \times 100$$

El adjudicatario entregará durante los 15 primeros días del mes, un informe que refleje el % de resolución de incidencias de la infraestructura dentro de los plazos de tiempo establecidos correspondiente al mes anterior. Dicho informe deberá incluir una relación de las incidencias de infraestructura acontecidas el mes anterior, incluyendo:

- Fecha y hora de comunicación de la incidencia de la infraestructura
- Aceptación de la incidencia por tener que ver con los servicios ofertados
- Explicación detallada de la incidencia
- Impacto aplicado
- Urgencia aplicada
- Prioridad aplicada
- Fecha y hora estimada de resolución de la incidencia
- Fecha y hora real de resolución de la incidencia
- Solución adoptada

4.4. CESE DEL SERVICIO

En el caso de cese del servicio contratado, sea cual fuese la causa del mismo, el proveedor se compromete a facilitar a Mutua Montañesa la información que requiera sobre las

configuraciones particulares del servicio implantado. Quedará excluida de dicha entrega, aquellas configuraciones que sean específicas de la infraestructura del operador (redes de gestión, direccionamientos propios del operador, claves de cifrado,...) el resto de configuraciones deberán entregarse en un plazo máximo de 15 días desde su solicitud por parte de Mutua Montañesa en el formato que esta estime oportuno.

Así mismo se comprometerá a facilitar la transición del servicio Mutua Montañesa y al operador entrante en los procesos de portabilidad y demás actividades administrativas y técnicas necesarias para culminar el proceso de cambio de operador.

El operador deberá, en los 3 meses posteriores al cese del servicio, retirar, previa autorización expresa de Mutua Montañesa, todo el equipamiento de su propiedad de las sedes de Mutua Montañesa. Pasado los 3 meses, el adjudicatario no podrá reclamar a Mutua Montañesa por ningún concepto relativo a la entrega de dicho material. En caso de incumplimiento de la condición de retirada de equipos, Mutua Montañesa podrá reclamar al proveedor los gastos ocasionados para la retirada y adecuación de equipos en desuso de los que el proveedor cesante sea responsable.

Dentro de estos 3 meses posteriores, el proveedor saliente podrá facturar a Mutua Montañesa, por aquellos servicios que, con el fin de garantizar un cambio ordenado y dada la naturaleza del servicio sea necesario mantener en paralelo.

4.5. PRESENTACIÓN DE DOCUMENTACIÓN

El ofertante deberá presentar su documentación, en formato papel y electrónico, estructurada según el índice que marca este documento para el Lote en cuestión. Se deberá indicar sobre el índice del presente documento la hoja en la que se describe el servicio en la oferta del proveedor.

5. CUMPLIMIENTO ENS

El adjudicatario deberá garantizar la seguridad, disponibilidad, confidencialidad e integridad de la información de Mutua Montañesa a la que tenga acceso en el desarrollo del proyecto mediante el cumplimiento de las siguientes normas básicas:

- Cumplir con los estándares y políticas de seguridad de Mutua Montañesa.
- Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y transmitida por su red.
- Informar a Mutua Montañesa acerca de su política de seguridad, así como de la implementación y seguimiento por parte de su organización.
- Informar por escrito a Mutua Montañesa tan pronto como se detecten riesgos reales o potenciales de seguridad en su red o en el equipamiento del cliente.
- Acceso a cualquier equipamiento de red y/o sistemas de información mediante un control de acceso lógico, garantizando la restricción a los usuarios autorizados.
- Garantizar la estricta aplicación de las normas de seguridad por parte de su personal.

El adjudicatario deberá desarrollar en materia de seguridad todas las modificaciones requeridas que cumplan con la normativa en LOPD, RGPD y ENS (Nivel Medio).

Por tanto, el adjudicatario deberá tener en cuenta como mínimo los requisitos de seguridad y Compliance recogidos en la siguiente tabla:

Codigo ENS	Título	BAJA	MEDIA
[op.acc]	Control de acceso		
[op.acc.1]	Identificación	1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación. 2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad. 3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que: a) Se puede saber quién recibe y qué derechos de acceso recibe. b) Se puede saber quién ha hecho algo y qué ha hecho. 4. Las cuentas de usuario se gestionarán de la siguiente forma: a) Cada cuenta estará asociada a un identificador único. b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario. c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.	

Codigo ENS	Título	BAJA	MEDIA
[op.acc.2]	Requisitos de acceso	Los requisitos de acceso se atenderán a lo que a continuación se indica: a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema. c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.	
[op.acc.3]	Segregación de funciones y tareas		El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita. En concreto, se separarán al menos las siguientes funciones: a) Desarrollo de operación. b) Configuración y mantenimiento del sistema de operación. c) Auditoría o supervisión de cualquier otra función

Codigo ENS	Título	BAJA	MEDIA
[op.acc.4]	Proceso de gestión de derechos de acceso	Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios: a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada. b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones. c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.	
[op.exp]	Explotación		

Codigo ENS	Título	BAJA	MEDIA
[op.exp.2]	Configuración de seguridad	Se configurarán los equipos previamente a su entrada en operación, de forma que: a) Se retiren cuentas y contraseñas estándar. b) Se aplicará la regla de "mínima funcionalidad": 1. El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad, 2. No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible. 3. Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue. c) Se aplicará la regla de "seguridad por defecto": 1. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. 2. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes. 3. El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.	

Codigo ENS	Título	BAJA	MEDIA
[op.exp.3]	Gestión de la configuración		Se gestionará de forma continua la configuración de los componentes del sistema de forma que: a) Se mantenga en todo momento la regla de "funcionalidad mínima? ([op.exp.2]). b) Se mantenga en todo momento la regla de "seguridad por defecto? ([op.exp.2]). c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]). d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]). e) El sistema reaccione a incidentes (ver [op.exp.7]).
[op.exp.4]	Mantenimiento	Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. b) Se efectuará un seguimiento continuo de los anuncios de defectos. c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.	

Codigo ENS	Título	BAJA	MEDIA
[op.exp.8]	Registro de la actividad de los usuarios	Se registrarán las actividades de los usuarios en el sistema, de forma que: a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información. b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema. c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados. d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema	
[op.exp.11]	Protección de claves criptográficas	Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final. a) Los medios de generación estarán aislados de los medios de explotación. b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.	a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5]. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Codigo ENS	Título	BAJA	MEDIA
[mp.com.3]	Protección de la autenticidad y de la integridad	a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver [op.acc.5]). b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos: 1. La alteración de la información en transito 2. La inyección de información espuria 3. El secuestro de la sesión por una tercera parte c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.	a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional. c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.
[mp.si]	Protección de los soportes de información		
[mp.si.5]	Borrado y destrucción	La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos. a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.	b) Se destruirán de forma segura los soportes, en los siguientes casos: 1. Cuando la naturaleza del soporte no permita un borrado seguro. 2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,. c) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].
[mp.sw]	Protección de las aplicaciones informáticas		

Codigo ENS	Título	BAJA	MEDIA
[mp.sw.1]	Desarrollo		a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción. b) Se aplicará una metodología de desarrollo reconocida que: 1. Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida. 2. Trate específicamente los datos usados en pruebas. 3. Permita la inspección del código fuente. 4. Incluya normas de programación segura. c) Los siguientes elementos serán parte integral del diseño del sistema: 1. Los mecanismos de identificación y autenticación. 2. Los mecanismos de protección de la información tratada. 3. La generación y tratamiento de pistas de auditoría. d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
[mp.info]	Protección de la información		
[mp.info.1]	Datos de carácter personal	Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.	

Codigo ENS	Título	BAJA	MEDIA
[mp.info.4]	Firma electrónica	Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.	a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados. b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional. c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin: d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación: 1. Certificados. 2. Datos de verificación y validación. e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d). f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.

Codigo ENS	Título	BAJA	MEDIA
[mp.s.2]	Protección de servicios y aplicaciones web	Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias. a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos: 1. Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado. 2. Se prevendrán ataques de manipulación de URL. 3. Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies". 4. Se prevendrán ataques de inyección de código. b) Se prevendrán intentos de escalado de privilegios. c) Se prevendrán ataques de "cross site scripting". d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés". Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.	