ANEXO II: MARCO DE PRESCRIPCIONES TÉCNICAS DE SALUD DIGITAL

Índice:

1. Objetivo

El objetivo del presente documento es especificar los requisitos técnicos en materia de Tecnologías de la Información y las Comunicaciones que deben tenerse en cuenta en la adquisición de cualquier Sistema de Información y/o equipamiento que vaya a hacer uso de los Sistemas TIC del SESCAM.

Servidores

Todos los servidores deben permitir, sin disminución de rendimiento de los sistemas que gestione, la instalación de un software de protección frente a virus, malware, etc. En la actualidad el SESCAM utiliza Symantec Endpoint Protection v.12.1.6. Así mismo, deben permitir, en las mismas condiciones anteriores, la instalación de parches críticos de seguridad y estabilidad para los sistemas operativos Windows y Linux.

Deberá permitir la instalación de un agente del software de backup de Commvault

La solución propuesta deberá ejecutarse al menos en uno de los siguientes sistemas operativos:

- Microsoft Windows 2012r2
- Linux Red Hat Enterprise v.7
- Linux Centos 7

Solución basada en servidores físicos

En el caso que el sistema de información a suministrar requiriese de una plataforma sustentada en servidores físicos, el diseño de la solución deberá basarse en una arquitectura que garantice la continuidad del servicio mediante Cluster de alta disponibilidad (HA – Hight Availability), funcionando con el software **Veritas Cluster HA**.

Se deberá suministrar el número de servidores necesarios que permita el correcto y óptimo funcionamiento de los sistemas que gestionen. Los equipos deberán permitir su instalación en rack, y se suministrarán todos los elementos necesarios para enrackar en armario de 800 x 1000 cm. (ancho x fondo). Se valorará la menor ocupación en U.

Deberá proveerse de todas las tarjetas, cables y dispositivos adicionales necesarios para la conexión de los sistemas hardware a la LAN del SESCAM.

Solución basada en servidores virtuales

Cuando la solución propuesta estuviera basada en una plataforma de servidores virtualizados, está deberá estar basada y certificada para las tecnologías VMWare 6 y/o Hyper-V (ver. 2012). Hacer mención a que deberá suministrar el número de licencias necesarias.

Bases de Datos y almacenamiento

Los licitadores detallarán expresamente el sistema o sistemas gestores de bases de datos utilizados por la solución propuesta. Así mismo, se deberá indicar el espacio de almacenamiento necesario para el primer año de funcionamiento y una estimación de crecimiento anual en condiciones normales de uso.

Sistema Gestor de Base de Datos (SGBD)

La solución deberá poder ejecutarse sobre al menos uno de los siguientes Gestores de Bases de Datos (SGBD):

- Oracle Database Enterprise Edition ver. 11g (11.2.0.3), 12c (12.1.0.2 ó 12.2.0.1)
- Sql Server 2008 R2
- IBM Informix 11.70 FC6
- MySQL Advance 5.6.14
- PostgreSql 9.3.1

La empresa licitadora deberá proporcionar si así fuera necesario y el SESCAM lo estimará oportuno, un acceso externo a dicha BD mediante un cliente ODBC/JDBC para una posible y futura explotación de los datos o integración con algún otro sistema.

Almacenamiento

La solución propuesta deberá contemplar la posibilidad de usar alguna de las siguientes cabinas de almacenamiento:

- NetApp
- EMC VNX5600
- Hitachi VSP
- Hitachi HCP/HDI

Servidores de aplicaciones (Middleware)

En el caso que la solución esté diseñada utilizando aplicaciones web que requieran una capa de servidor de aplicaciones, ésta deberá adecuarse a las siguientes capas:

Capa Front-End

Tecnología	Versión
Apache HTTP Server	2.4.23 mod_jk/1.2.42 mod_wl/12cR1
Internet Information Server (IIS)	8.5.9600.16384 - w2k12R2

Capa Back-End

Tecnología	Servidor/Tipo	Versión	S.O.	Modo	JVM
PHP, PYTHON	LAMP	PHP 5.3.3 + Python 2.6.6 + Perl v5.10.1	RHEL 6.3 - 6.6		OpenJDK 1.6
JAVA	Weblogic	12c – 12.1.3.0.0	RHEL 7.3	Standalone & Clúster	Java HotSpot 1.7 y 1.8
	Apache Tomcat	7 – 7.0.55 (Adapt. Multi-instancia)		Standalone & Clúster	Java HotSpot 1.6 y 1.7
		8 - 8.5.20 (Adapt. Multi-instancia)			Java HotSpot 1.7 y 1.8
.NET	Microsoft Windows	Server 2003 - 2012R2	MS w2k3 - w2k12R2	Standalone	.NET 2.0
JS	NodeJS	NodeJS - 6.11.X, NPM - 3.10.X, PM2 - 2.7.X	RHEL 7.3	Standalone & Clúster	

Telecomunicaciones.

Desde el punto de vista de conectividad y acceso a la red corporativa del SESCAM (en adelante SANITEL), se deberán analizar las siguientes cuestiones antes de la implantación de cualquier infraestructura o servicio TIC en sedes del SESCAM:

- Se deberá proporcionar la arquitectura de red de la solución, servicio o hardware a instalar. Entre otros, tomas de red, interfaces, vlanes, direccionamiento o esquemas de conexionado y cableado.
- Se deberá entregar igualmente información relativa a los requisitos de telecomunicaciones de la solución o hardware implantado: Tipo de conector, medio físico (fibra o cobre), ancho de banda necesario, flujos de tráfico a habilitar, securización a implementar, o cualquier otro requisito importante que pueda hacer variar el correcto funcionamiento del servicio implantado.
- Tal y como se ha indicado en puntos anteriores, y sobre todo en escenarios de elevado consumo de puertos o interfaces de red, se deberá contemplar la posibilidad de incluir, dentro de la arquitectura de la solución a desplegar por la empresa licitadora, equipamiento de red y cableado para su interconexión en la sede correspondiente del SESCAM. Desde la Unidad de Telecomunicaciones no se garantiza la disponibilidad de puertos de acceso disponibles en todas las sedes y circunstancias.
- Igualmente, y de manera especial para servicios no relacionados directamente con actividad asistencial o directamente integrados en plataformas y soluciones TIC del SESCAM, se recomienda la dotación por parte de la empresa licitadora de líneas de comunicaciones independientes. Esto permitirá, por un lado, independizar el tráfico no asistencial del tráfico sanitario, y evitará que el SESCAM se convierta en proveedor y responsable de los enlaces de comunicaciones para el acceso a los servicios implantados. La interconexión o integración con la red SANITEL se podría realizar a través de conexión segura VPN. Este escenario es especialmente recomendable en sedes del SESCAM no Hospitalarias, donde el ancho de banda de red de telecomunicaciones disponible es inferior y limitado.
- En el caso indicado en el punto anterior, se deberá contratar, al menos y bajo el criterio de alta disponibilidad y cumplimiento de SLAs, una línea de comunicaciones para cada sede remota con servicios implantados. La tipología y ancho de banda de los enlaces deberá ser analizada y propuesta por parte de la empresa licitadora.

Para dotar de conectividad a infraestructura y servicios centralizados en sede Hospitalarias o CPDs regionales del SESCAM, se deberá analizar la idoneidad de integrar este equipamiento en la red local de dichas sedes o la opción de disponer igualmente de enlaces de comunicaciones dedicados que permitan, por un lado, la conexión y gestión

del equipamiento desplegado de manera independiente, y por otro, la integración con la red corporativa del SESCAM a través de acceso seguro VPN.

En el SESCAM hay desplegado equipamiento de diferentes fabricantes y modelos, el cual se clasifica según el ámbito tecnológico que abarca cada uno. El equipamiento que se pretenda instalar ha de cumplir como mínimo los requerimientos indicados a continuación.

En términos generales, el equipamiento o solución de telecomunicaciones deberá cumplir con los siguientes requerimientos:

- Monitorización por sflow o netflow, SNMP v2 y v3.
- Automatización SDN vía API, por ejemplo, Ansible.
- Se deberá dotar de todos los elementos activos y pasivos, cables, adaptadores, transceptores, etc., necesarios para la correcta implantación e integración del equipamiento que se adquiera.
- Se deberá especificar la cantidad de almacenamiento necesario para poder albergar los logs que genere la nueva solución a implantar según establezca la normativa en cada caso.
- Las soluciones que se puedan virtualizar deberán cumplir con los requerimientos que se indica en el apartado 2.2 del presente documento.
- Los equipos que se adquieran deberán pertenecer, en la medida de lo posible, al catálogo de productos STIC perteneciente al Organismo de certificación del Centro Criptológico Nacional.
- Los equipos deberán estar dimensionados de tal manera que sean capaces de asumir la carga en cuanto a número total de usuarios, conexiones simultáneas, dispositivos contemplados, sedes, etc., que se especifiquen en cada momento.
- En la medida de lo posible cuando se estime necesario se deberá suministrar un entorno de PRE.
- Se deberá incluir un estudio total de cobertura que refleje el estado de la conectividad WiFi en los centros donde se pretenda implantar dicha tecnología.
- Las soluciones de forma general deberán presentar una arquitectura con redundancia para permitir alta disponibilidad.
- En la adquisición de nuevas soluciones se deberá impartir una formación que permita dotar de las capacidades necesarias para poder gestionar y dar soporte a dicha solución.
- La titularidad de licencias de las soluciones que se adquieran deberán, en la medida de lo posible, pertenecer a personal de SESCAM.

- Se deberá entregar la siguiente documentación al SESCAM:
    - Descripción técnica de la solución:
        - Diseño de Alto Nivel: se especificará la arquitectura de bloques tanto a nivel lógico como físico.
        - Diseño de Bajo Nivel: se describirá la arquitectura e interconexión de todos los componentes de forma lógica y física.
        - Diseño de integración de los componentes, especificando las funcionalidades disponibles con la nueva arquitectura.
        - Inventario de elementos.
        - Gestión y operación de la infraestructura.
    - Los servicios que se adquieran se ajustarán en todo momento, en lo que resulte de aplicación, a lo dispuesto en el Real Decreto 3⁄2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

5.1 Equipamiento de red:

- **Conmutación (Switchs):**
    - Gestionables por IP.
    - Spanning-Tree modos RSTP o PVSTP.
    - Capacidad de full PoE.
    - Soporte para Dot1x e integración con sistemas NAC.
    - AAA por RADIUS o TACACS+.
    - Interfaz de gestión por CLI y WEB segura (https).
    - Soporte para CDP o LLDP.
- **Enrutamiento (Routers):**
    - Enrutamiento estático y dinámico (RIP, EIGRP, OSFP y BGP).
    - Soporte para IPv4 e IPv6.
    - Capacidad de VRF lite o similar (vpn-instance).
    - Soporte para CDP o LLDP.

- **Balanceadores:**
  - Gestión de tráfico a nivel de aplicación (capa 7)
  - Gestión de tráfico SSL.
  - Creación de instancias o virtualización del balanceador.
- **Navegación / Proxy:**
  - Gestión de perfiles de navegación.
  - Creación de listas blancas y negras.
  - Gestión de sitios por bases de datos des reputación.
  - Actualización dinámica de categorizaciones y bajo demanda.
  - Integración con sistemas NAC.
  - Monitorización por sflow o netflow, SNMP v2 y v3
  - Automatización SDN vía API, por ejemplo, Ansible.
- **Controladoras WiFi.**
  - Posibilidad de integrarse en Máquina virtual.
  - Soporte de protocolos 802.11 a/b/g/n y ac.
  - Soporte para Dot1x e integración con sistemas NAC.
  - Monitorización por sflow o netflow, SNMP v2 y v3
  - Automatización SDN vía API.
  - Debe gestionar automática y dinámicamente la frecuencia y potencia a la que deben trabajar los puntos de acceso para optimizar la cobertura existente y rendimiento de los clientes inalámbricos.
  - Debe garantizar un acceso equilibrado entre los clientes.
  - El controlador deberá ser capaz de disminuir los efectos de la interferencia co-canal.
  - El controlador deberá poder grabar el espectro durante un intervalo de tiempo para poder analizar posteriormente la presencia de interferencias
  - Soportarán redundancia con replicación automática de configuraciones entre controladores.

- Los controladores soportaran redundancia N+1ª nivel 3.
- Soporte de los siguientes métodos de autenticación:
    - 802.1x - (EAP, LEAP, PEAP, EAP-TLS,EAP-TTLS, EAP-FAST, EAP-SIM, EAP-OTP,EAP-GTC, EAP-TLV, EAP-AKA,EAP-MD5)
    - MAC.
    - Portal Cautivo.
    - Soporte de autenticación sobre distintos tipos de servidores:
        - Base de datos interna.
        - LDAP/ SSL Secure LDAP.
        - RADIUS.
        - AD.
- Soporte de roles de usuario que permita:
    - Asignación de ancho de banda por rol o por usuario
    - Reglas de Firewall basadas en la identidad del usuario y no en la dirección del origen del usuario
    - Reglas de acceso por horario o por localización dentro de la red (punto de acceso).
    - Mapeo opcional del usuario a una VLAN independiente del SSID al que este asociado
    - Capacidad de realizar las funciones de IDS (Intrusión Detection System) wireless, como detección de Rogue APs o ataques de denegación de servicio (DoS).
    - Capacidad de realizar funciones de IPS (Intrusion Protection System) wireless, con mecanismos de contención de intrusos.
- Limitar el ancho de banda:
    - Por usuario
    - Por grupo de usuarios
    - Por AP
    - Por aplicación
- El controlador deberá soportar mecanismos para reducir de una manera sencilla el tráfico

de broadcast y multicast, limitando el número de usuarios por VLAN y asignando nuevos usuarios a las VLANs menos ocupadas (“vlan-pooling”).

- El controlador debe ser capaz de enrutar entre las VLANs definidas sin necesidad de un router externo.

- **Puntos de acceso Wi-Fi**
  - Los APs deberán poder ser configurados de forma estática o dinámica para funcionar exclusivamente en modo sonda (no participan en la transmisión de datos).
  - Todos los puntos de acceso deben tener la posibilidad de implementar redes mesh wireless para que en el futuro la red wireless se pueda extender desde cualquier AP instalado sin necesidad de nuevo cableado o nuevas conexiones de red ethernet.
  - Todos los puntos de acceso deberán tener la posibilidad de conmutar localmente el tráfico de un SSID hacia la LAN local sin necesidad de enviarlo hacia el controlador.
  - Los puntos de acceso deberán tener la inteligencia suficiente para decidir si en un SSID determinado el tráfico debe ir hacia el controlador a través del túnel o ser conmutado hacia la red local.
  - Los puntos de acceso deberán soportar el estándar 802.11ac así como mantener la compatibilidad con estándares anteriores 802.11 a/b/g/n.
  - Los puntos de acceso deberán incluir filtros para protegerse de las interferencias provocadas por redes 3g/4g.
  - Las radios deberán poder hacer Análisis de Espectro para detectar interferencias no-WiFi y servir clientes de manera simultanea
  - El AP deberá poder detectar y clasificar las fuentes de interferencia externas (Microondas, bluetooth, DECT, etc…).
  - Soporte de los siguientes métodos de cifrado:
    - CCMP/AES (recomendado).
    - TKIP.
    - Secure Sockets Layer (SSL) and TLS:
    - RC4 128-bit and RSA 1024- and 2048-bit
    - L2TP/IPsec (RFC 3193)

- PPTP (RFC 2637)

- **Plataforma de gestión WiFi**
  - Actualización centralizada del firmware de los dispositivos.
  - Auto-Descubrimiento de dispositivos.
  - Auto-Configuración de los puntos de acceso que se vayan incorporando a la red.
  - Comprobación de las políticas de seguridad configuradas en los Puntos de Acceso.
  - Permitirá la creación de grupos de dispositivos en función de distintos criterios definidos por el administrador.
  - Configuración masiva de dispositivos mediante la descarga de plantillas que se cargan simultáneamente a grupos de Puntos de Acceso creados por el administrador.
  - Permitirá la detección de Puntos de Acceso instalados sin autorización (Rogue Access Points).
  - Permitirá su integración con sistemas de gestión mediante SNMP.
  - Monitorizará el espectro radioeléctrico para detectar posibles interferencias, así como situaciones en las cuales la calidad del servicio está sufriendo degradaciones.
  - Permitirá almacenar, al menos, el último fichero de configuración, facilitando la "marcha atrás" en caso de ser necesario.
  - Permitirá la supervisión y control de toda la infraestructura WiFi mediante la recolección de alarmas y eventos de los elementos de la misma y su representación visual.
  - Soportará la funcionalidad de mapa de red en donde se presente el estado de todos los elementos de la red WiFi así como su estado de operación con tiempos de refresco no superiores a 5 minutos.

- **Sistema de control de acceso a Redes (NAC):**
  - El sistema estará disponible en versión "appliance" y en versión "máquina virtual" para facilitar su despliegue.
  - El sistema deberá utilizar protocolos estándar que garanticen su compatibilidad con distintos equipos de acceso (switches, routers, firewalls, controladores WLAN,

terminadores VPN) de distintos fabricantes.

- Compatibilidad con los estándares definidos por TNC (Trusted Network Connect) con especial foco en el estándar 802.1X.
- Soporte de servicios AAA (Authentication, Authorization and Accounting) con los métodos de autenticación más utilizados en la industria.
- Posibilidad de separar los procesos de Autenticación y Autorización – cada proceso deberá poder utilizar bases de datos distintas.
- El sistema tendrá funcionalidades de Autorización del acceso en función de características como pertenencia a un grupo de usuarios, tipo de dispositivo móvil, aplicación utilizada, localización del dispositivo, estado de salud (health check) del dispositivo, etc…
- Compatibilidad con distintas bases de datos:
    - Microsoft Active Directory
    - Kerberos
    - LDAP standard
    - ODBC- compatible con SQL
- El sistema proporcionará una infraestructura PKI interna que permita que permita generar credenciales específicas de para dispositivos móviles que sirvan para autorizar estos dispositivos en la red (certificados digitales). Debe ser compatible con los dispositivos más habituales: iOS (Apple iPad, iPhone),Android, MacOS X, Windows Mobile, Windows 7.
- Las credenciales utilizadas para los dispositivos móviles permitirán controlar el acceso de estos dispositivos a la red y denegarlo en caso de robo o pérdida del dispositivo.
- El sistema proporcionará estadísticas de uso e inventario de los dispositivos móviles.
- El sistema tendrá la capacidad de utilizar las credenciales de autenticación de red (802.1X) para autenticar también las sesiones de las aplicaciones móviles.

- **Seguridad (Firewalls capa 7):**
    - El sistema estará disponible en versión “appliance” y en versión “máquina virtual” para facilitar su despliegue.

- Capacidad de filtrado de tráfico a nivel de aplicación (capa 7).
- Posibilidad de finalizar túneles VPN.
- Capacidades de antivirus, antispam, DNS filter, web filtering, application control, IPS, DLP, SSL/SSH inspección, etc.
- Aplicación de calidad de servicio (QoS).
- Control de tráfico (Traffic Shapping).
- Creación de instancias o virtualización del firewall.
- Tener visibilidad de las aplicaciones que atraviesan el perímetro de la red.
- Poder vincular a los usuarios de la red con las aplicaciones.
- Poder disponer de información de seguridad centralizada en un único dispositivo para poder analizarla, correlacionarla y estudiarla en caso de que acontezca algún incidente de seguridad.
- Disponer de funcionalidades IPS en el cortafuegos.
- Disponer de filtrado de URLs en el cortafuegos.
- Creación de informes programada o manual con criterios de filtrado
- QoS para poder priorizar las aplicaciones más críticas
- Integración con Directorio Activo
- Protección ante ataques de denegación de servicio, incluyendo los de naturaleza distribuida.
- Base de datos de firmas con actualización periódica así como posibilidad de definir firmas personalizadas.
- Soporte para validación de protocolos, así como detección de ataques de todo tipo, incluyendo aquellos combinados con técnicas de evasión.
- Soporte para IPv4 e IPv6.

5.2 Plataformas de voz y telefonía.

Cualquier solución o plataforma de voz a implantar, deberá permitir la integración con las actuales centralitas IP del SESCAM, mediante protocolos o mecanismos estándar:

- SCCP o SIP para señalización de endpoints
- H.323 o MGCP para control de dispositivos
- CTI para control e integración de aplicaciones
- Web Services incluidos en las APIs de comunicación de las plataformas actuales.

En la actualidad, el SESCAM dispone de centralitas IP basadas en tecnologías Cisco (Call Manager) y Alcatel (OXE), un Contact Center IP basado en tecnología Cisco Enterprise, y una solución de Session Border Controller basada en SBCs Oracle Acme Packet.

Todas las plataformas anteriormente descritas están implantadas con mecanismos de alta disponibilidad, y redundadas en los cuatro CPDs corporativos del SESCAM. En la medida de lo posible, y siempre que los servicios a desplegar lo soporten, se valorará positivamente la implantación de soluciones bajo plataformas virtualizadas y con arquitecturas de servicio centralizadas.

Se valorarán positivamente soluciones de escritorio compatibles con cualquier versión de sistema operativo o distribución de software instalada en los PCs.

En la actualidad, todas las plataformas de video, voz y colaboración comparten un único plan de numeración corporativo a 5 cifras (con prefijo * para llamadas a la JCCM), que permite acceder a cualquier servicio desde cualquier origen, independientemente de su naturaleza o tecnología.

Cualquier despliegue masivo de terminales, requerirá de la compra de licenciamiento asociado tanto para Cisco Call Manager (licencias Enhanced, Enhanced Plus o CUWL en función de los servicios a incluir), como para Alcatel OXE.

Cualquier despliegue masivo de agentes o servicios de Contact Center, requerirá un análisis de necesidad y valoración de compra de licenciamiento asociado a Cisco UCCE (Agentes concurrentes, licencias de Call Manager, etc..).

En el anexo I de este documento se detallan las versiones actuales de soluciones implantadas y endpoints disponibles.

5.3 Plataformas de video y colaboración

El SESCAM dispone, en la actualidad, de una solución de videoconferencia basada en plataformas de control y registro de Cisco (VCS-Control y VCS-Expressway).

Los endpoints internos del SESCAM se registran contra el VCS-Control mediante protocolos SIP o H.323, en función del modelo de dispositivo, dando siempre preferencia al registro SIP, siempre que esté soportado. Estos dispositivos se registran bajo el dominio “video.sescam.jccm.es”. El VCS-Expressway permite la entrada o salida de llamadas desde o hacia el exterior del SESCAM (Inet). Actualmente no se permite el registro de terminales ni otros servicios a través de esta plataforma.

Además, el SESCAM dispone de una solución de gestión de salas de videoconferencia basado en una MCU Cisco Codian, que registra las salas mediante protocolo H.323 en el VCS-Control, y proporciona, de manera adicional, acceso a dichas salas a través de conexiones RDSI con la PSTN.

Por último, se dispone de una solución de videocolaboración de escritorio, que proporciona capacidad de conexión a salas de videocolaboración a través de un cliente ligero de PC o móvil (salas con video, chat, pizarra compartida, compartición de archivos y de contenidos, moderación o control remoto), además de una herramienta de IM propia que permite la conexión de clientes de mensajería al servidor.

En la actualidad, todas las plataformas de video, voz y colaboración comparten un único plan de numeración corporativo a 5 cifras (con prefijo * para llamadas a la JCCM), que permite acceder a cualquier servicio desde cualquier origen, independientemente de su naturaleza o tecnología.

Cualquier solución o endpoint a desplegar en el SESCAM deberá ser integrable y compatible con las plataformas actualmente desplegadas. Los endpoints de videoconferencia a implantar, deberán soportar conexiones HDMI para salida de video y varias conexiones (HDMI y VGA al menos) para la entrada de compartición de contenidos. Se valorarán positivamente los mecanismos de conexión inalámbricos.

Se valorarán positivamente soluciones de escritorio compatibles con cualquier versión de sistema operativo o distribución de software instalada en los PCs.

Cualquier despliegue de terminales, requerirá de la compra de licenciamiento asociado a Cisco VCS-Contro o Call Manager (licencias de registro en VCS o CUWL en CUCM, en función de los servicios a incluir).

En el anexo I de este documento se detallan las versiones actuales de soluciones implantadas y endpoints disponibles.

5.4 Accesos Remotos

En caso de los accesos externos, los proveedores deben cumplir lo siguiente dependiendo del tipo de acceso:

Acceso remoto:

- Sistema operativo Windows 7.
- Con software Anyconnect de la version 4.1 o superior.

LAN-TO-LAN:

- IP Publica estática que actué como peer del túnel (no tiene por qué estar dedicada).
- Router/Firewall de cualquier fabricante que pueda configurar las siguientes propuestas (no daremos soporte a cualquier otra si el túnel no levanta)

  - Parámetros ISAKMP

    - Hash: SHA/HMAC-160
    - Encryptions: 3DES-168
    - Diffie-hellman Group: Group2
    - Authentication Mode: Pre-shared secret
    - Key lifetime: 86400 secs

  - Parámetros IPSec

    - IPSEC Encapsulation Túnel Mode
    - IPSEC Protocol Type ESP
    - IPSEC Cipher Algorithm 3DES-168
    - IPSEC Authentication: SHA/HMAC-160
    - IPSEC SA Lifetime: 28800
    - IPSEC Perfect Fordward Secrecy: Off
    - Pre-shared-key
    - El tráfico ha de ser Nateado en origen a un direccionamiento incluido en la red 10.70.x.x (a excepción de direccionamiento solapado)

Aspectos Generales

Las empresas licitadoras detallarán sus requerimientos en cuanto a permisos / credenciales de Sistema Operativo, seguridad, bases de datos, conexiones externas, conexión a Internet, etc., para la ejecución/actualización de la solución propuesta.

La solución permitirá la configuración de usuarios con distintos roles (usuario, usuario administrador, usuario integrador, etc.), y se integrarán con el sistema LDAP corporativo, sistemas de Directorio Activo y sistema de gestión de identidades corporativos del SESCAM.

Todos los trabajos de configuración, parametrización, conexionado y puesta en marcha de la solución deberán ser realizados con medios materiales y personales del adjudicatario.

Todas las licencias de software, Sistemas Operativo, Bases de Datos, clientes, agentes, etc., deberán ser proporcionadas por el adjudicatario, incluyendo soporte y mantenimiento de las mismas durante el período de garantía y/o mantenimiento que establezca el contrato.

Todo el entorno cliente en el que se ejecute la solución deberá adaptarse a las características técnicas del puesto de trabajo corporativo del SESCAM.

Todo el equipamiento hardware suministrado deberá incluir, además de la garantía legal de fabricante, soporte y mantenimiento, que cubran las posibles averías, actualizaciones, etc., necesarias durante el periodo de garantía y/o mantenimiento que establezca el contrato.

Deberá proveerse al SESCAM de todos aquellos manuales de operaciones y de administración, del hardware y del software suministrado.

ANEXO 1. Resumen de requerimientos técnicos

Tecnología / Productos	
Antivirus	Symantec EndPoint Protectión 12
Sistemas Operativos de Servidor	Microsoft Windows 2012r2
	Linux Red hat Enterprise v.7
	Linux Centos 7
Cluster de HA	Veritas Cluster HA
Virtualización / Hypervisor	VMWare 6
	Hyper-V v.2012
Sistema Gestor de Base de Datos (SGBD)	Oracle Database Enterprise Edition ver.11g (11.2.0.3), 12c (12.1.0.2 ó 12.2.0.1)
	SQL Server 2008 R2
	IBM Informix 11.70 FC6
	MySQL Advance 5.6.14
	Postgre SQL 9.3.1

Almacenamiento	NetApp
	EMC VNX5600
	Hitachi VSP
	Hitachi HCP/HDI

Tecnología	Versión
Apache HTTP Server	2.4.23 mod_jk/1.2.42 mod_wl/12cR1
Internet Information Server (IIS)	8.5.9600.16384 - w2k12R2

Tecnología	Servidor/Tipo	Versión	S.O.	Modo	JVM
PHP, PYTHON	LAMP	PHP 5.3.3 + Python 2.6.6 + Perl v5.10.1	RHEL 6.3 - 6.6		OpenJDK 1.6
JAVA	Weblogic	12c – 12.1.3.0.0	RHEL 7.3	Standalone & Clúster	Java HotSpot 1.7 y 1.8
	Apache Tomcat	7 – 7.0.55 (Adapt. Multi-instancia)		Standalone & Clúster	Java HotSpot 1.6 y 1.7
		8 - 8.5.20 (Adapt. Multi-instancia)			Java HotSpot 1.7 y 1.8
.NET	Microsoft Windows	Server 2003 - 2012R2	MS w2k3 - w2k12R2	Standalone	.NET 2.0
JS	NodeJS	NodeJS - 6.11.X, NPM - 3.10.X, PM2 - 2.7.X	RHEL 7.3	Standalone & Clúster	

Toledo, a fecha de firma electrónica

EL DIRECTOR GENERAL DE ASISTENCIA SANITARIA

Fdo.: Ibrahim Rafael Hernández Millán

Castilla-La Mancha
Avda. Río Guadiana - 45071 TOLEDO