METRO DE SANTIAGO

ESPECIFICACIONES TÉCNICAS
SOLUCIÓN SEGURIDAD

SUBGERENCIA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

2017

INDICE

1. ANTECEDENTES

La Empresa de Transporte de Pasajeros METRO se encuentra en proceso de expansión debido a la construcción de las Líneas 6 y 3. Esta ampliación de la red de transporte agregará para la Línea 6 una cantidad de 10 estaciones con una longitud total de 15.3 kilómetros, a su vez para la Línea 3 se agregarán una cantidad de 18 estaciones con una longitud total de 18 kilómetros, lo que en términos globales permitirán a Metro tener una red de 140 kilómetros y 136 estaciones.

Dado lo anterior, Metro S.A ha decidido potenciar la seguridad TI en los aspectos que serán abordada en la presente especificación técnica, razón por la cual se realizará un proceso de licitación pública, para adjudicar y adquirir las soluciones de acuerdo a las necesidades operacionales de METRO S.A.

2. SITUACIÓN ACTUAL

Actualmente la Subgerencia TIC es responsable de la seguridad TI para los distintos servicios corporativos y de negocio. En este aspecto y de acuerdo a los nuevos requerimientos de seguridad operacional relacionados con la puesta en marcha de las líneas 6 y 3, se ha tomado la determinación de incorporar tecnologías ad hoc a fin de dar una adecuada cobertura a los requerimientos de seguridad.

La figura N°1 muestra la arquitectura de Red de Metro con las distintas zonas de seguridad que posee actualmente (figura de carácter referencial).

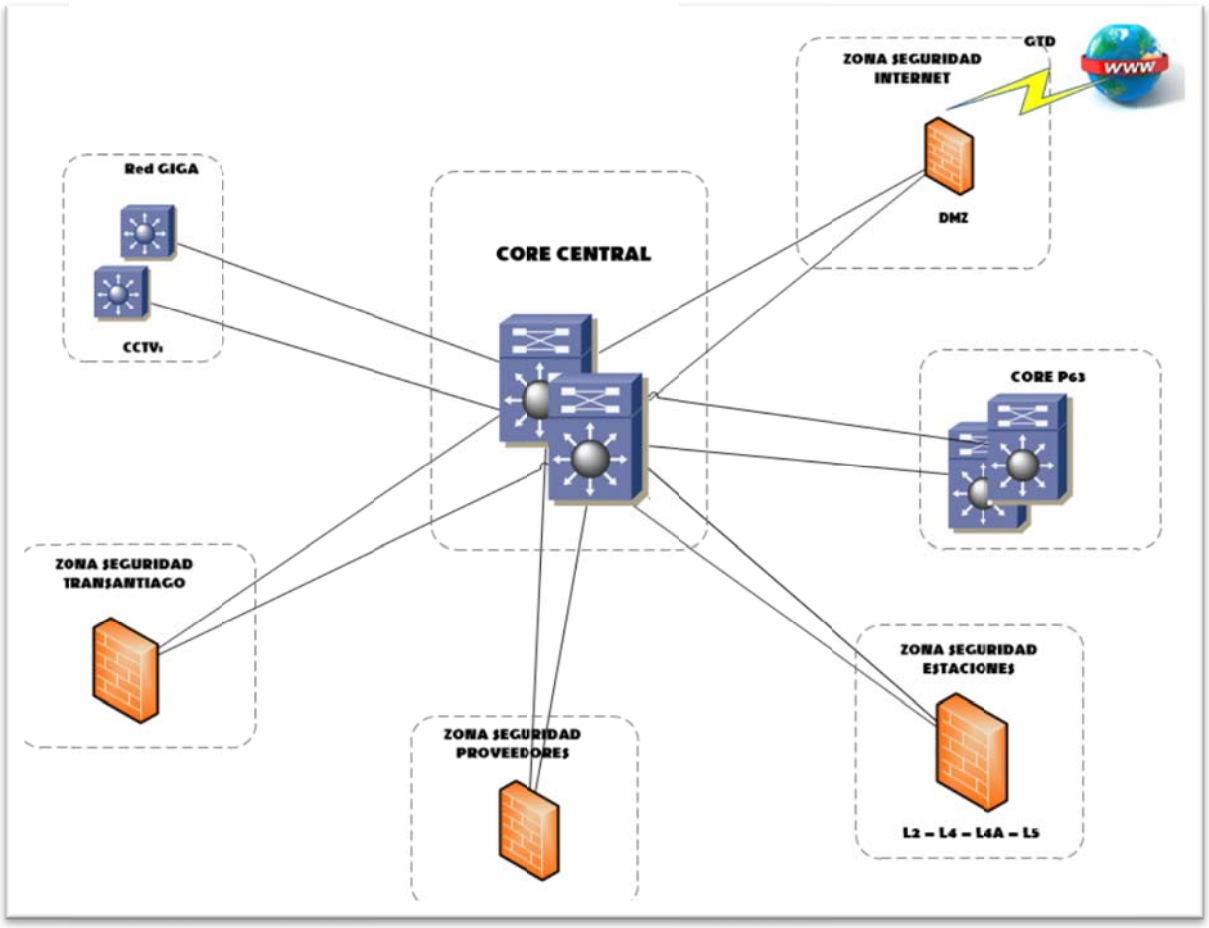

Figura N° 1: Arquitectura de Red Corporativa y Zona de Seguridad

La arquitectura de red está conformada por equipos de CORE para las distintas redes y las 4 zonas de seguridad para los servicios de Metro, servicios de estaciones, servicios de proveedores, servicios con Transantiago, servicios de acceso hacia Internet y las redes exteriores de Metro.

3. OBJETIVOS

3.1. OBJETIVOS GLOBALES

El objetivo global de este proyecto corresponde a los siguientes puntos:

a) Suministrar el equipamiento necesario para de incorporar tecnologías ad hoc a fin de dar una adecuada cobertura a los requerimientos de seguridad.
b) Desplegar las configuraciones necesarias para el correcto funcionamiento de la solución de seguridad.
c) Integrar las herramientas de seguridad y realizar la puesta en servicio funcional de cada una de ellas y la solución en su conjunto.
d) Entregar un acceso seguro para los usuarios y contratistas mantenedores de los sistemas del P63 desde el exterior, acceso que debe ser continuo y garantizado para la operación y mantenimiento de los sistemas.

3.2. OBJETIVOS ESPECÍFICOS

Dotar a Metro S.A de una solución de seguridad compuesta por los siguientes subsistemas:

3.2.1. Subsistema de Seguridad Perimetral (NGFW)

Se define Next Generation Firewall (NGFW), al sistema de seguridad de red basado en hardware o software, que es capaz de detectar y bloquear ataques sofisticados mediante la aplicación de políticas de seguridad, a nivel de aplicación, de puertos y/o protocolos.

Esta licitación considera como primer subsistema la adquisición, actualización, implementación y puesta en servicio de una Zona de Seguridad Perimetral (NGFW) con equipamiento y herramientas de control para el acceso remoto seguro a las redes Metro.

3.2.2. Subsistema de Gestión de Identidades y Control de Acceso a la Red

Se define Gestión de Identidades y Control de Acceso a la Red, como una herramienta de administración de red que permite la creación y aplicación de políticas de seguridad y acceso para dispositivos terminales, conectados a los switches, routers y firewalls corporativos. Su

principal propósito es simplificar la gestión de identidades a través de diversos dispositivos y aplicaciones. Dentro de sus funciones principales la herramienta debe contar con:

a) Fácil incorporación y administración de usuarios temporales.
b) Disponibilidad de gestión sencilla con autoservicio para el uso de dispositivos BYOD.
c) Gestión y unificación de políticas de acceso a la red, proporcionando accesos seguros a los usuarios finales, para conexiones fijas, inalámbricas y VPN.
d) Visibilidad mejorada y precisión en la identificación de dispositivos.
e) Segmentación de software basada en roles con integración con la infraestructura existente.

La Solución de Seguridad considera un segundo subsistema la adquisición, implementación y puesta en servicio de una herramienta de software para la Gestión de Identidades y Control de acceso a la Red, con capacidad de gestionar políticas de seguridad de forma automatizada, entregando acceso seguro contextual a los recursos de la red y que se integre de forma nativa con el Subsistema de Seguridad Perimetral (NGFW) y el equipamiento de Core y acceso de la red P63.

3.2.3. Subsistema de Administración de Dispositivos Móviles (MDM)

Se define como Administración de Dispositivos Móviles (MDM) a la herramienta que se ocupa de desplegar, asegurar, monitorear, integrar y administrar dispositivos móviles, como smartphones, tablets y notebooks. El objetivo del MDM es optimizar la funcionalidad y la seguridad de los dispositivos móviles y de la red corporativa.

La Solución de Seguridad considera como tercer subsistema, a la adquisición, implementación y puesta en servicio de una herramienta de software MDM (Mobile Device Management) de Administración de dispositivos móviles multi-vendor, para administrar todos los dispositivos desde una sola consola central, registrando los dispositivos corporativos, configurando, y securizando cada uno de los dispositivos administrados por esta herramienta.

3.2.4. Subsistema de Correlación de Eventos (SIEM)

Se define como Subsistema de Correlación de Eventos a una herramienta de administración de la seguridad que entrega una visión holística de los dispositivos corporativos que se encuentran monitoreados, permitiendo realizar una búsqueda en tiempo real de patrones de los flujos de información y comportamiento de la data en una red.

La Solución de Seguridad considera la adquisición, implementación y puesta en servicio de una herramienta de correlación de eventos SIEM (security information and event management) que permita procesar una gran cantidad de registros de eventos de distintos equipos de la red, analizando en tiempo real de las alertas de seguridad generadas por el hardware y software de los equipos y dispositivos conectados a la red.

3.2.5. Infraestructura de Máquina Virtual (VM)

Se define como Infraestructura de Máquina Virtual a una implementación de software en un hardware de grandes capacidades y dualidad de componentes de un ambiente de computación en el que se pueden instalar y convivir distintos ambientes de procesamiento y sistemas operativos.

La Solución de Seguridad considera como la adquisición, implementación y puesta en servicio de una infraestructura de hardware que mediante una conformación de servidores permita la instalación de todo el software solicitado en los puntos 4.2, 4.3 y 4.4 necesarios para el funcionamiento integral de la solución junto con su licenciamiento por un período de 3 años.

3.2.6. Integración de Herramientas de Seguridad

Se define como Integración de Herramientas de Seguridad a las configuraciones necesarias para que las herramientas que componen la Solución de Seguridad operen en conjunto, generando los traspasos de información necesarios por cada Subsistema, de forma tal de que cada uno de los sistemas realice la función diseñada, complementándose con el resto de las herramientas.

La Solución de Seguridad considera la ejecución de las actividades para integrar las herramientas de seguridad (4.1, 4.2, 4.3 y 4.4), dar funcionamiento global a la Solución de Seguridad, para lo cual el OFERENTE debe realizar las configuraciones necesarias en los equipos Next Generation Firewall, Gestión de Identidades y Control de acceso a la Red, MDM, Herramienta de Correlación de eventos,para su correcto funcionamiento e integración entre estos equipos.

3.3. DESCRIPCIÓN GENERAL DEL PROYECTO

Este documento abarca las actividades que el OFERENTE deberá ejecutar para el suministro, instalación, configuración, pruebas, puesta en servicio e Integración de la Solución de Seguridad. Dentro de las actividades que el OFERENTE debe ejecutar se considera el levantamiento de toda la información, reglas y políticas configuradas en el equipamiento actual, la revisión de las configuraciones para la exportación, la homologación al nuevo equipamiento (en caso de requerirse), el despliegue de las nuevas configuraciones y las pruebas funcionales de los servicios tanto corporativos como de negocios.

La solución de seguridad deberá permitir la Gestión de Identidades y Control de acceso a la Red desde los accesos remotos, que permita controlar, al menos 250 endpoints. Para lo anterior, se requiere un sistema automático de seguridad que permita controlar dichos dispositivos, perfilarlos, validarlos, y crear reglas de acuerdo a la identidad de la persona que se está conectando a la red, en conjunto con el tipo de dispositivo. La solución requerida debe implementar un sistema de autenticación, autorización y auditoría (AAA) y correlación de eventos de la red, que permita controlar el acceso a ella de dispositivos que cumplan con las políticas corporativas.

4. ESPECIFICACIONES TÉCNICAS

A continuación se describen las actividades generales que el OFERENTE deberá ejecutar en el ámbito del Proyecto dar cumplimiento a los requerimientos de los Subsistemas de la Solución de Seguridad.

4.1. SUBSISTEMA DE SEGURIDAD PERIMETRAL

Para el Subsistema de Seguridad Perimetral el OFERENTE deberá considerar los siguientes requerimientos:

REQ1. El OFERENTE deberá suministrar e instalar el equipamiento Next Generation Firewall (NGFW) en modalidad de HA (High Availability), el lugar de instalación es en el SITE de Metro ubicado en Alameda 1414, Piso 3 edificio Corporativo. La solución de NGFW permitirá el desarrollo de un proceso de administración y protección de seguridad de la infraestructura tecnológica, lograr la eficiencia máxima en el control, segmentación y la detección/prevención de ataques, a través de funcionalidades de detección de anomalías en protocolos de red, minimizando los falsos positivos y falsos negativos en la identificación de ataques, con una administración centralizada contra amenazas conocidas o desconocidas y ataques híbridos.

REQ2. El fabricante del NGFW debe contar con un grupo de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.

REQ3. El NGFW deberá tener la capacidad de integrarse con soluciones de NAC (Network Access Control) y soportar la funcionalidad de “RADIUS Change of Authorization (CoA)” para proveer mecanismos de cambio de atributos en una sesión AAA ya autenticada.

REQ4. El NGFW debe incorporar la funcionalidad para la habilitación de un módulo IPS (Intrusion Prevention System), a fin de garantizar que la funcionalidad a futuro cumple con los estándares solicitados por Metro S.A. Para ello se solicita que el OFERENTE garantice a través de documentación que el módulo IPS tenga un alto reconocimiento de mercado, con al menos 5 años consecutivos en el cuadrante líder de Gartner mágico de Gartner.

REQ5. El equipamiento solicitado debe contar con las siguientes características:

Features	Next Generation Firewall
Stateful inspection firewall throughput	10 Gbps
Concurrent firewall connections	2.000.000
Firewall connections per second	125.000
Option for Security Contexts	Up to 250 **(License required)**
Authentication	Active Directory agent, LDAP, Kerberos, NTLM
3DES/AES IPsec VPN throughput	3 Gbps
Interfaces	16-port 10/100/1000, 4-port 10 Gigabit Ethernet (SFP+) | **10 GbE license required**
Management Ports	2-port 10/100/1000
Virtual interfaces (VLANs)	1024
High Availability	Active/active and Active/standby
Scalability	VPN clustering and load balancing
Redundant Power	Yes
Memory	24 GB

Tabla 1: Características de equipamiento de Seguridad Perimetral.

REQ6. El motor de inspección IPS de la solución NGFW debe contar con el reconocimiento del último reporte realizado en el 2013 de NSS Labs, líder en pruebas de productos de seguridad, en donde se demuestre que la solución completó satisfactoriamente las pruebas contando con al menos 97% de efectividad, para lo cual deberá presentar la documentación respectiva.

REQ7. El dispositivo deberá ser capaz de hacer recomendación de afinación (tunning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.

REQ8. El fabricante deberá proveer el código de sus firmas para demostrar la detección en base a vulnerabilidades y no en comparación de patrones. Este código podrá ser visible en cualquier momento desde la consola de administración para todas las firmas existentes en el IPS.

REQ9. El dispositivo deberá identificar vulnerabilidades de los hosts de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades.

REQ10. El dispositivo debe proporcionar una completa visión del comportamiento de la red para detectar nuevas amenazas, incluyendo la capacidad de establecer líneas de base de tráfico a través de técnicas de flujos.

REQ11. El dispositivo deberá incluir un sistema de integración con directorio activo, que provea las siguientes características:

i. Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.
ii. Deberá permitir tener la información de contacto de los usuarios que están siendo atacados.
iii. Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.
iv. Deberá tener la funcionalidad de generar un mapa de eventos de seguridad generados/recibidos por usuario.
v. Deberá tener la funcionalidad de generar un mapa de tráfico generado/recibido por usuario.
vi. Deberá tener la funcionalidad de mantener un mapa de los usuarios, IP actual, tipo de aplicación usada, y un historial de las IPs que ese usuario ha usado en el tiempo.

REQ12. El dispositivo debe tener la capacidad de detectar tráfico anómalo o vulnerabilidades en al menos las siguientes aplicaciones Instant Messenger y P2P: AOL Instant Messenger; MSN Messenger; Yahoo! Messenger; ICQ; Gnutella; Kazaa; BitTorrent, entre otros.

REQ13. El dispositivo debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.

REQ14. El dispositivo debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, enviar correo electrónico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.

REQ15. El dispositivo deberá ser capaz de entregar propuestas de recomendaciones de afinación (tunning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.

REQ16. El dispositivo deberá proveer la detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero, como una funcionalidad dentro del mismo IPS y sin necesidad del uso de aplicaciones adicionales como sistema de detección de anomalías o scanners.

REQ17. El dispositivo deberá tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.

REQ18. El dispositivo deberá permitir un análisis dinámico y en tiempo real en para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros: Redes existentes; Host activos; Nuevos Host o servers en la red; Nuevas MAC address en la red; Máquinas virtuales nuevas o existentes; Sistema operativo de cada uno de los host identificados; Servicios activos de cada uno de los host identificados; Aplicaciones activas de cada uno de los host identificados; Vulnerabilidades de cada uno de los host identificados.

REQ19. El dispositivo deberá ser capaz de proporcionar mayor visibilidad sobre cómo se consume el ancho de banda, ya sea por dirección o puerto, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red. (sin necesidad de hardware o software separado).

REQ20. El dispositivo debe soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source IP, Destination IP, Source port; Destination port; Rule overhead, Metadata, entre otros.

REQ21. El dispositivo deberá permitir una integración automática para realizar un cambio de configuración o enviar información a módulos de terceros como: Scanners de vulnerabilidades; SEM/SIEM systems; Firewall; Routers; Switches.

REQ22. El dispositivo deberá tener una funcionalidad de “packet level” para realizar actividades de análisis forense.

REQ23. El contratista deberá realizar las actividades de levantamiento Zona de Seguridad, entre ellas:

a) Levantar información asociada a las configuraciones, reglas y políticas de seguridad implementadas en la Zona de Seguridad de Internet Corporativo.
b) Revisión, análisis y homologación de las configuraciones del equipamiento actual con el equipamiento a instalar.

REQ24. De la misma forma el OFERENTE deberá suministrar el software necesario para el hardware que se instalará. Las versiones de software deberán estar validadas por el fabricante y deben corresponder a las últimas versiones vigentes al momento de la Licitación. No se aceptarán versiones en modalidad de desarrollo, beta u otra tipificación distinta a la versión validada por el fabricante.

REQ25. Configuración y Puesta en Servicio, el OFERENTE será responsable de la ejecución de las siguientes actividades:

a) Levantamiento de las configuraciones de la Zona de Seguridad perimetral de Internet.
b) Ejecutar las actividades necesarias que permitan el traspaso de las configuraciones y habilitación de la totalidad de los servicios de la zona de seguridad anterior al nuevo equipamiento.
c) Ejecutar las actividades necesarias que permitan tener conectividad entre red corporativa TIC e Internet junto a completa funcionalidad de los servicios publicados y/o consultados por Metro S.A. en Internet.
d) Ejecutar las actividades necesarias que permitan tener conectividad entre red corporativa TIC y la red multiservicio del Proyecto 6 y 3.
e) Ejecutar todas las actividades necesarias para el correcto funcionamiento de la totalidad de los servicios actualmente en operación y los nuevos servicios asociados al P63, tanto internos como de acceso remoto, o con proveedores externos.
f) Generar y aplicar las configuraciones básicas y avanzadas para todo el equipamiento solicitado en este proyecto.
g) El OFERENTE será responsable de la continuidad operacional de la zona de seguridad a intervenir, al realizar una intervención en la red, al instalar o configurar el equipamiento

asociado a la solución o al realizar cualquier trabajo relacionado y materia de estas especificaciones.

h) El OFERENTE deberá proponer modificaciones en las configuraciones, ya sea por buenas prácticas o tendientes a la integración de la zona de seguridad con la red de Metro.

REQ26. Una vez ejecutada la Puesta en Marcha, el OFERENTE deberá realizar una exhaustiva revisión de las configuraciones y políticas para minimizar los riesgos de seguridad junto con la optimización de las reglas aplicadas (eliminación de objetos, servicios duplicados, eliminación de políticas no utilizadas, identificar reglas o ACL que anulen otras, políticas permisivas o de alto riesgo), reordenamiento de las mismas para garantizar el mejor aprovechamiento de la performance del equipo.

4.2.SUBSISTEMA DE GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO A LA RED

A continuación se describen las actividades generales que el OFERENTE deberá ejecutar en el ámbito del Proyecto dar cumplimiento a los requerimientos del Subsistema de Gestión de Identidades y Control de acceso a la Red.

REQ27. La solución de Gestión de Identidades y Control de acceso a la Red deberá ser instalada en una plataforma virtual en modalidad de HA, en el data center de la subgerencia TIC, descrita en el punto 4.4.1, para lo cual se requiere el suministro del software de Gestión de Identidades y Control de acceso a la Red para ser instalado en VM.

REQ28. La solución de Gestión de Identidades y Control de acceso a la Red deberá contar con las siguientes funcionalidades:

a) Licenciamiento Base para 250 EndPoint.
b) Licenciamiento Plus para 250 Endpoint.
c) Subscripción y licenciamiento Plus por 3 años para 250 Endpoint.
d) Licenciamiento Avanzado para 250 Endpoint.
e) Subscripción y licenciamiento Avanzado por 3 años para 250 Endpoint
f) Licenciamiento Plus para conexiones remotas seguras por 3 años para 250 usuarios
g) Licenciamiento y subscripción Plus para conexiones remotas seguras por 3 años para 250 usuarios.

REQ29. La solución de Gestión de Identidades y Control de acceso a la Red deberá ofrecer servicios de autenticación, autorización, auditoría y perfilamiento (AAA). Cada uno de los servicios mencionados se puede describir de la siguiente forma:

a) Autenticación: el sistema debe permitir el ingreso de las credenciales de un usuario, y debe poder permitir integrarse con MS Active Directory, LDAP y RADIUS. Con este mecanismo se puede determinar la identidad del usuario.
b) Autorización: la plataforma debe poder identificar a que grupo o rol pertenece un usuario específico. Con esto, se pueden asociar políticas de seguridad específicas para el rol de forma escalable.
c) Auditoría: se deben soportar mecanismos de registros de la actividad de los usuarios en términos de ingreso o salida de la red.
d) Perfilamiento: el sistema debe identificar a los distintos dispositivos que se conectan a la red de forma automática, y asignar los accesos a la red según se definan.

REQ30. La solución de Gestión de Identidades y Control de acceso a la Red deberá ofrecer un esquema de alta disponibilidad, tanto para el sistema de gestión como para el mecanismo que tome las decisiones de ingreso o no a la red. La alta disponibilidad debe operar en capa 3 para los nodos que forman parte del sistema.

REQ31. La solución de Gestión de Identidades y Control de acceso a la Red debe tener las facilidades para ser implementada en un modelo centralizado o distribuido.

REQ32. La solución de Gestión de Identidades y Control de acceso a la Red deberá integrarse con la infraestructura de redes cableadas e inalámbricas propuestas y existentes en la red de Metro.

REQ33. La solución de Gestión de Identidades y Control de acceso a la Red deberá contar con la funcionalidad de implementarse en redes alámbricas, inalámbricas o mixtas.

REQ34. La solución de Gestión de Identidades y Control de acceso a la Red deberá utilizar un protocolo de control de la plataforma de red que debe basarse en RADIUS.

REQ35. La solución de Gestión de Identidades y Control de acceso a la Red deberá sustentarse en 802.1X para operar, haciendo uso del supplicant nativo del sistema operativo.

REQ36. La solución a ser implementada debe ser capaz de hacerse cargo de múltiples escenarios asociados a 802.1X citados a continuación:

a) Usando credenciales de Windows de usuarios, contra la infraestructura de MS AD existente, a modo de SSO en laptops y desktops corporativos.
b) Soporte de autenticación basada en certificados digitales, RADIUS externos, LDAP y plataformas OTP.
c) Autenticación basada en MAC para dispositivos que no soporten 802.1X.
d) Autenticación basada en portal web personalizable, con soporte en español.
e) Autenticación con múltiples dispositivos por puerta, por VLAN, por SSID.
f) Secuencias de mecanismos de autenticación definibles. Por ejemplo, primero autenticación por MAC, luego 802.1X.
g) Mecanismo de re-autenticación CoA (Change Of Authorization) basada en el estándar de la IETF, RFC 3576 o 5176.
h) Soporte de múltiples variantes de EAP, al menos: EAP-FAST, EAP-TLS, EAP-MD5, PEAP MSCHAPv2, EAP-GTC, EAP-Chaining.
i) Soporte de 802.1X machine-authentication y user-authentication.
j) Integración con Microsoft Active Directory del Ministerio para la autenticación de los usuarios, sin requerir privilegios de administrador.
k) Debe soportar 802.1AE, MacSec, SGT y SGACL.

REQ37. La solución de Gestión de Identidades y Control de acceso a la Red deberá forzar que la seguridad establecida sea en la red, y la solución no debe estar basada en esquemas anexos o externos como puramente DHCP (ej: forzando segmentos /30 entre GW y usuarios), o la instalación de un agente.

REQ38. La solución de Gestión de Identidades y Control de acceso a la Red deberá ejecutar las acciones para que los usuarios no-autenticados hagan ingreso con acceso limitado para mitigar riesgos, y luego de ser autenticados se les asignen los permisos de acceso a la red de acuerdo a la categorización (ejemplo: visita, usuario corporativo, externo).

REQ39. La solución de Gestión de Identidades y Control de acceso a la Red deberá soportar los siguientes mecanismos de enforcement para control de tráfico de usuarios:

a) Asignación de VLANs.
b) Asignación de listas de acceso desde el servicio AAA hacia el controlador inalámbrico, referenciando el nombre de la lista de acceso configurada localmente en el controlador inalámbrico (named-ACLs).
c) Asignación de listas de acceso desde el servicio AAA hacia los switches de acceso de la red, ya sea referenciando el nombre de la lista de acceso configurada localmente en los switches, o aplicando ACLs directamente a las puertas de los switches de manera centralizada desde la solución AAA. (ACL descargables).
d) Asignación de SGT (Security Group Tag).

REQ40. La solución de control de acceso deberá permitir definir excepciones basadas en MAC (o bien OUIs) para dispositivos como impresoras, teléfonos IP, Access-Points, scanners, cámaras de videovigilancia, entre otros dispositivos.

REQ41. En relación a la gestión de invitados, la solución de control de acceso deberá :

a) Proveer un mecanismo de autenticación por medio de un portal web personalizable.
b) Desplegar las credenciales de los invitados en un sistema centralizado, cuyos administradores deben ser autenticados contra MS AD.
c) Entregar una o múltiples cuentas para las cuentas de invitados donde se podrá crear, modificar y definir políticas de claves y nombre de usuario configurables.
d) Soportar el auto-registro de invitados.
e) Contar con mecanismo de auditoría para invitados, registrar entradas y salidas.
f) Soportar el despliegue de las políticas de uso aceptable a la red al usuario final.

g) Permitir la desconexión en demanda de usuarios.

h) Contar con un mecanismo que tome en consideración la sesión completa del invitado y no tan solo la transacción de autenticación, con un identificador apropiado.

i) Permitir la configuración de diferentes portales (Hotspot, gestionado, Usuario/Password, etc.).

REQ42. La solución de control de acceso deberá soportar la inclusión de mecanismos de automatización de descubrimiento de direcciones MAC para dispositivos que no correspondan a PCs (ej: impresoras, teléfonos IP, Access-Points, Scanners, Cámaras de Videovigilancia, etc.), de manera de facilitar su aprovisionamiento. Del mismo modo, este mecanismo debe poder determinar si alguno de los dispositivos deja de comportarse como tal, para prevenir impersonificaciones ilícitas de dispositivos dentro de la red, aumentando la seguridad del sistema.

REQ43. La solución de control de acceso deberá soportar múltiples perfiles de dispositivos que se alimenten de variados mecanismos de información de la red: RADIUS, DHCP, SNMP, CDP, mecanismos de captura de tráfico, entre otros. Adicionalmente, se deben poder crear perfiles de dispositivos personalizables. Las reglas de perfilamiento para la identificación deben soportar múltiples dispositivos y marcas, y su actualización debe ser automática, sin requerir upgrades de software.

REQ44. La solución de control de acceso deberá soportar un mecanismo de aprovisionamiento y reportería de usuarios invitados. Las cuentas de usuarios deben poder definirse con expiración según fecha/hora, definiendo políticas de password de estos usuarios y con un sistema de gestión de fácil uso. Deben soportarse dos mecanismos: uno en la que un usuario que pertenece a la organización crea la cuenta del invitado fijando una fecha de expiración, y otra en la que es el mismo usuario quien se auto-provisiona la cuenta de acceso a través de un portal web.

REQ45. La solución de control de acceso deberá contar con un API, de carácter abierta para desarrollos externos y estar apropiadamente documentada, de manera de poder extender sus funcionalidades iniciales según se requiera, basada en Web Services (WS).

REQ46. La solución de control de acceso deberá contar con una consola de gestión basada en HTTP, sobre un protocolo seguro como HTTPS. No se aceptarán aplicaciones cliente-servidor basadas en Java.

REQ47. La solución de control de acceso deberá contar con un dashboard que entregue visibilidad efectiva al operador de la plataforma, incluyendo datos como tiempo promedio de remediación, gráficos de uso de recursos de la plataforma, número de autenticaciones fallidas, entre otros.

REQ48. La solución de control de acceso deberá incluir un sistema de reportes que incluya información sobre dispositivos en cumplimiento, no cumplimiento, información desde donde se están conectando, nombre de usuario, MAC, dirección IP, VLAN, Switch de acceso, puerta de acceso, sistema operativo y otros campos relevantes.

REQ49. La solución de control de acceso deberá soportar la generación de plantillas en el sistema de Administración basados en las políticas de Seguridad previamente establecidas.

REQ50. La solución de control de acceso deberá permitir crear reglas de políticas de autorización deben basadas en al menos los siguientes atributos y sus combinaciones:

a) Rol de usuarios (obtenible desde MS AD).
b) Método de acceso: cableado, inalámbrico, vía VPN.
c) Hora y fecha.
d) Lugar.
e) Tipo de dispositivo (ej: tableta, Smartphone, PC, etc.).
f) Estado de cumplimiento con la política de seguridad definido.
g) Atributos de usuarios alojados en un directorio LDAP.

REQ51. La solución de control de acceso deberá asignar una VLAN al usuario final y aplicar una lista de acceso dinámica asociada al puerto donde el usuario o dispositivo final se está conectando. Tecnología de referencia: dACL – Downloadable Access Control List o named-ACL en base al resultado de la política de autorización, basada en los atributos previamente mencionados.

REQ52. La solución de control de acceso deberá permitir adicionalmente, asignar un nivel de calidad de servicio vía RADIUS y otros parámetros relevantes al usuario.

REQ53. La solución de control de acceso deberá contemplar una herramienta que entregue visibilidad y trazabilidad de potenciales casos en los que la autenticación no sea exitosa, entregando la traza paso a paso en el árbol de decisión, detalles del usuario final, dirección IP, MAC, puerta, VLAN, rol, dispositivo de acceso, fecha y hora.

REQ54. La solución de control de acceso deberá contar con flexibilidad para implementar el punto de enforcement de forma centralizada en un escenario en el que existen múltiples hops o saltos hasta el usuario final en una red capa 3 (soluciones que requieran implementar un appliance por segmento en capa 2 no son deseables).

REQ55. La solución de control de acceso deberá restringir el acceso a equipos que no cumplan con las políticas definidas, mitigando riesgos de seguridad.

REQ56. La solución de control de acceso deberá interoperar con escenarios que incluyan telefonía IP.

REQ57. La solución de control de acceso deberá permitir la carga individual de MAC addresses de excepción o bien cargas masivas usando archivos de texto separados por coma.

REQ58. La solución de control de acceso deberá estar posicionada como líder por reconocidos analistas de la industria tecnológica.

REQ59. El contratista deberá entregar documentación relevantes al menos en los siguientes puntos:

a) Mejores prácticas de implementación en redes inalámbricas
b) Guías de diseño e implementación para iniciativas como BYOD (Bring Your Own Device)
c) Compatibilidad con equipos inalámbricos existentes asegurado por el proveedor

REQ60. En términos de soporte para dispositivos móviles y el soporte de Bring Your Own Device (BYOD) la solución de control de acceso deberá:

a) Permitir el onboarding de los dispositivos móviles, en términos de carga de supplicant 802.1X si aplicase, aplicación del perfil de conectividad adecuado para conectarse, e instalación de certificado digital en el dispositivo móvil.
b) Permitir la integración con plataformas externas de Mobile Device Management, de al menos 6 proveedores. Debe permitir que se definan reglas para validar que el dispositivo móvil cumpla con ciertas políticas antes de hacer ingreso a la red.
c) Permitir que el mismo usuario pueda dar de alta o de baja sus dispositivos móviles.
d) Definir un máximo de dispositivos móviles a ser registrados por cada usuario.

REQ61. La solución de Gestión de Identidades y Control de Acceso a la Red deberá tener la capacidad de integrarse con fabricantes de MDM (Mobile Device Manager) mediante llamadas a "REST API", de esta manera a través de la conexión entre ambas soluciones se permita validar información detallada disponible en la base de datos de MDM.

REQ62. La solución de Gestión de Identidades y Control de Acceso a la Red para tener un mayor control, deberá ejecutar validaciones de cumplimiento por cada conexión VPN desde dispositivos móviles, la información que la solución MDM deberá poner a disposición de la solución de Gestión de Identidades y Control de Acceso a la Red (a través de la API) es la siguiente:

a) DeviceRegisterStatus
b) DeviceCompliantStatus
c) DiskEncryptionStatus
d) PinLockStatus
e) JailBrokenStatus
f) Manufacturer
g) IMEI
h) SerialNumber
i) OsVersion
j) PhoneNumber

k) MDMServerName
l) MDMServerReachable
m) MEID
n) Model
o) UDID

4.3.SUSBSISTEMA DE GESTIÓN DE DISPOSITIVOS MÓVILES

En términos de la administración de dispositivos móviles el OFERENTE deberá suministrar e instalar un MDM (Mobile Devices Management) que sea capaz de entregar las siguientes funcionalidades:

REQ63. El MDM deberá soportar el soporte de múltiples dispositivos como por ejemplo Android, Blackberry, iOS, Tizen, Windows Phone, Laptops (Chromebook, OS X, Windows).

REQ64. El MDM deberá contar con licencia para 200 dispositivos y con opción para el crecimiento futuro.

REQ65. El MDM deberá contar con características de una tecnología abierta, compatible con .NET, Microsoft SQL, Windows Server, por el contrario de aplicaciones o soluciones de tipo caja negra que impiden la gestión de la solución.

REQ66. El MDM deberá estar basado en estándares.NET, MS SQL y plataformas de desarrollo HTML 5 o superior.

REQ67. El MDM deberá contar con la opción de instalar el software de antivirus, herramientas de administración del sistema y parches de seguridad en el servidor EMM (Enterprise Mobility Management), además de servicios de monitoreo (software de 3eras partes, SCOM (System Center Operations Manage), Syslog, etc.).

REQ68. El MDM deberá contar con funcionalidades para soportar API REST de forma de extender los flujos de trabajo.

REQ69. El MDM deberá entregar una conformación de arquitectura segura por niveles (servidor de base de datos de forma segura en la red interna y no en DMZ).

REQ70. El MDM deberá contar con funcionalidades de una solución tipo servidor de aplicaciones compatible con configuraciones de Alta Disponibilidad y Recuperación de Desastres.

REQ71. El MDM deberá bloquear o rechazar conexiones directas (no seguras) con LDAP y PKI desde Internet.

REQ72. El MDM deberá entregar funcionalidades de despliegue múltiple para los dispositivos gestionados.

REQ73. El MDM deberá soportar el portafolio de aplicativos corporativos y de negocio, módulo de cumplimientos, y de SEG (Secure Email Gateway) para entrega de contenido seguro de correo electrónico, gestión y acceso de los dispositivos.

REQ74. El MDM deberá soportar la integración con la infraestructura corporativa, en términos de manejo de LDAP, AD, autoridades de certificados, VPN, Exchange, PKI, etc.

REQ75. El MDM deberá soportar la integración nativa y directa a proveedores de servicios de certificados de Microsoft CA (sin necesidad de SCEP)

REQ76. El MDM deberá soportar la integración nativa con Entrust PKI, OpenTrust CMS Mobile, Symantec MPKI, Verisign MPKI (sin necesidad de SCEP).

REQ77. El MDM deberá ejecutar de forma automática la renovación de certificados antes de que expiren.

REQ78. El MDM deberá emitir certificados a los dispositivos y aplicaciones.

REQ79. El MDM deberá permitir la visibilidad completa a la información de certificados tal como certificados instalados, revocados y los que van a caducar por un tablero de administración de certificados

REQ80. El MDM deberá soportar la agrupación de dispositivos y usuarios en base a unidades de negocios, grupos de organización, ubicaciones geográficas, propietarios del dispositivo, etc.

REQ81. El MDM deberá soportar la personalización de marca por grupo (del registro del dispositivo, portal de autoservicio, catálogo de aplicaciones, la consola de administración, las aplicaciones nativas).

REQ82. El MDM deberá contar con un sistema de reportes avanzados, alertas, despliegue de diagramas, utilización y creación de DataMart para el análisis de los datos e inteligencia empresarial.

REQ83. El MDM deberá contar con un Framework SDK, para incorporar capacidades adicionales de gestión de dispositivos para aplicaciones internas, protección avanzada contra la pérdida de datos y autenticación de cada dispositivo.

REQ84. El MDM deberá contar con funcionalidades de incorporar dispositivos vía SMS, correo electrónico, enlace URLs, etc.

REQ85. El MDM deberá contar con soporte para dispositivos corporativos y dispositivos personales de empleados.

REQ86. El MDM deberá contar con soporte para registro de dispositivos de forma individual o masiva.

REQ87. El MDM deberá contar con soporte en autenticación de usuarios y dispositivos federada como SAML 2.0 (Security Assertion Markup Language), básico o basado en servicios asociados al directorio corporativo.

REQ88. El MDM deberá contar con una modalidad de configuración centralizada e instantánea de las políticas, parámetros, certificados y el acceso a las cuentas corporativas.

REQ89. El MDM deberá contar con una modalidad de despliegue inalámbrico de las aplicaciones corporativas y de negocio.

REQ90. El MDM deberá permitir realizar la verificación y autorización de dispositivos por medio de un acceso seguro a las cuentas y recursos corporativos.

REQ91. El MDM deberá permitir la protección del dispositivo, de la información que está contenida, tanto personal como corporativa, mediante mecanismos como cifrado y códigos de acceso.

REQ92. El MDM deberá permitir el bloqueo de funciones del dispositivo y la aplicación de restricciones al mismo.

REQ93. El MDM deberá permitir limitar el registro de dispositivos en base a organización LDAP, grupos y atributos (cantidad máxima de dispositivos por usuario).

REQ94. El MDM deberá permitir limitar el registro a plataformas de dispositivos validadas, modelo, sistema operativo y propiedad del dispositivo.

REQ95. El MDM deberá permitir asignar automáticamente la clasificación de dispositivos en sub-grupos, por ejemplo Nivel 1 de soporte local y Nivel 3 de soporte global.

REQ96. El MDM deberá permitir el control sobre el uso no autorizado de dispositivo basado en las políticas corporativas, configuración, aplicaciones, uso de terceros, entre otros.

REQ97. El MDM deberá permitir la ejecución de automatización de políticas corporativas para dispositivos no compatibles, no registrados o en modalidad de remediación/infracción.

REQ98. El MDM deberá permitir el control de estado y estadísticas de dispositivos y redes.

REQ99. El MDM deberá permitir la administración remota para Android, MAC OS X y Windows.

REQ100. El MDM deberá permitir el control de mensajería centralizado para personalizar todos los mensajes del sistema como correo electrónico, SMS, y Push Notification.

REQ101. El MDM deberá permitir el seguimiento de la actividad del usuario, como las descargas de aplicaciones, voz, SMS, uso de datos de acuerdo a los umbrales corporativos, listas blancas o listas negras.

REQ102. El MDM deberá permitir el control del acceso al sistema y la actividad de los usuarios en la consola mediante registros de eventos detallados por dispositivo registrado.

REQ103. El MDM deberá permitir el manejo de alertas y reglas corporativas automatizadas para la ejecución de acciones de red globales o en dispositivos específicos, acciones por usuarios o en el sistema.

REQ104. El MDM deberá permitir la asignación de aplicaciones y políticas en base al usuario, el dispositivo y la propiedad del dispositivo.

REQ105. El MDM deberá permitir la integración con AppleCare para ver estado de la garantía y la información del dispositivo (sólo para los dispositivos corporativos).

REQ106. El MDM deberá permitir la elaboración de informes con distribución configurable, y automatizada a los destinatarios de interés.

REQ107. El MDM deberá permitir el despliegue de informes de política preconfigurados (cumplimiento, gestión de activos, aplicaciones, correo electrónico, telecom, contenido, documentos, certificados, etc.)

REQ108. El MDM deberá permitir el despliegue de informes en tiempo real de datos del dispositivo.

REQ109. El MDM deberá permitir el registro de eventos centralizado para guardar todos los eventos del dispositivo y administrativos (logins, cambios de políticas, actualizaciones de aplicaciones, cambios de configuración, etc.)

REQ110. El MDM deberá permitir la administración de inventarios de activos móviles en forma automatizada y a demanda.

REQ111. El MDM deberá permitir la detección de dispositivos comprometidos (jailbreak, rooteados u otra denominación).

REQ112. El MDM deberá permitir la ejecución de acciones como Wipe fuera de línea para la detección comprometida.

REQ113. El MDM deberá permitir la implementación de una modalidad Kiosco para restringir el dispositivo a ejecutar sólo aplicaciones aprobadas (Android y iOS (con una única aplicación)).

REQ114. El MDM deberá permitir el soporte para dispositivos compartidos (un dispositivo que varios usuarios pueden iniciar sesión y recibir su contenido respectivo).

REQ115. El MDM deberá permitir la integración con Android for Work.

REQ116. El MDM deberá permitir la integración con APIs de los principales Fabricates (KNOX, LG, Moto, Sony, Panasonic, Samsung, etc).

REQ117. El MDM deberá permitir el soporte de Windows 10 que incluye una implementación optimizada (configuración rápida, inscripción en volumen, agregar cuenta de trabajo), Health attestation, acceso condicional, políticas de cifrado, integración con Windows Hello y Passport, administración de actualizaciones.

REQ118. El MDM deberá permitir el soporte de acceso asignado en Windows Phone para personalizar y controlar lo que el usuario tiene acceso en el dispositivo.

REQ119. El MDM deberá permitir el soporte del programa de Apple Device Enrollment Program y VPP para iOS y Mac OS X.

REQ120. El MDM deberá permitir la actualización y aprovisionamiento de nuevas políticas, configuraciones, certificados, aplicaciones, software y acceso a las cuentas corporativas (por ejemplo): Exchange Active Sync, Wi-Fi, VPN, CA, LDAP, entre otros.

REQ121. El MDM deberá permitir la aplicación de configuraciones, aplicaciones, software o comandos remotos de bloqueo/eliminación a pedido, en un horario programado o la próxima vez que se registre un dispositivo o grupo de dispositivos.

REQ122. El MDM deberá tener la funcionalidad de contenerización para aplicaciones de correo, calendario, y contactos.

REQ123. El MDM deberá permitir el soporte para Autenticación de dos factores (2FA) para correo electrónico (certificado y Usuario/Contraseña).

REQ124. El MDM deberá contar con soporte para correo S/MIME (iOS y Android).

REQ125. El MDM deberá permitir el soporte de aplicaciones en modalidades de Lista blanca / negra / requerida de aplicaciones u otros filtros necesarios para la administración.

REQ126. El MDM deberá permitir el soporte para diferentes políticas de implementación (a demanda, instalación automática, configuraciones VPN, etc.) para diferentes grupos de usuarios

REQ127. El MDM deberá permitir el despliegue de aplicaciones unificado para permitir a los usuarios acceder a cualquier aplicación - nativa, web o remota - en cualquier dispositivo.

REQ128. El MDM deberá permitir el soporte para múltiples versiones de aplicaciones (diferentes dispositivos pueden utilizar diferentes versiones).

REQ129. El MDM deberá permitir Auto-configurar aplicaciones (configuración de URL, códigos de grupo, direcciones de correo electrónico, claves de licencia) para simplificar la inscripción.

REQ130. El MDM deberá permitir forzar la autenticación del usuario antes de utilizar la aplicación (por ejemplo, iniciar sesión con credenciales corporativas).

REQ131. El MDM deberá permitir automáticamente detectar el estado comprometido al iniciar la aplicación - restringir el uso de la aplicación cuando se detecta.

REQ132. El MDM deberá soportar autenticación por medio de Single-Sign On para aplicaciones empresariales con App Wrapping.

REQ133. El MDM deberá tener la funcionalidad de configurar códigos de acceso y requisitos de seguridad

REQ134. El MDM deberá asegurar datos de la empresa y aplicar el cifrado de datos.

REQ135. El MDM deberá contar con la funcionalidad de personalización de marca del contenedor.

REQ136. El MDM deberá contar con Integración mediante API's con Fabricantes de herramientas de Gestión de Identidades y Control de acceso a la Red.

REQ137. El MDM deberá permitir la visualización de diagnósticos a los dispositivos de manera remota para identificar problemas.

REQ138. El MDM deberá permitir la asistencia remota a usuarios móviles y comunicación desde la consola a través de mensajes SMS.

REQ139. El MDM deberá permitir el control remoto de dispositivos para solucionar problemas con mayor eficiencia.

REQ140. El MDM deberá entregar capacidades de administración remota a través de un portal de autoservicio para los usuarios poder gestionar sus propios dispositivos y acceso corporativo (GPS, Política y gestión de la Seguridad, la visibilidad de cumplimiento).

REQ141. El MDM deberá entregar configuraciones de privacidad para no recolectar datos del dispositivo sensibles.

REQ142. El MDM deberá entregar funcionalidades de visualización de las actividades relacionadas con la privacidad para los usuarios para ver lo que los administradores pueden acceder en sus dispositivos.

REQ143. El MDM deberá contar con una funcionalidad de personalizar información de soporte y de los informes.

REQ144. El MDM deberá contar con funcionalidades de administración de problemas e incidentes mediante un sistema integrado de administración de casos.

REQ145. EL OFERENTE deberá proporcionar el Certificado Digital Valido en Internet requerido para la conexión de los dispositivos móviles.

4.4. SUBSISTEMA DE CORRELACIÓN DE EVENTOS (SIEM)

En términos del software requerido para la instalación del Subsistema de Correlacionador de Eventos SIEM (System Information Event Manager) este sistema deberá realizar las acciones de detección de actividades sospechosas que amenazan los sistemas de una empresa y resolverlas de forma inmediata por medio de alguna configuración automatizada. El subsistema SIEM dentro de sus características tiene la capacidad de procesar una gran cantidad de registros de eventos, enviando alertas sobre los fallos de seguridad encontrados en el sistema en tiempo real y las actividades sospechosas que están ocurriendo en la plataforma de datos de TI y permite colectar, indexar y proteger los datos generados por sus sistemas de información (Sistemas Operativos, sistemas de bases de datos, transacciones en el main frame, Firewalls, Routers, aplicativos, ATMs, IPS/IDS, etc.).

REQ146. El Subsistema de Correlación de eventos deberá colectar e indexar cualquier tipo de datos generado por los sistemas de TI en tiempo real, pudiendo tomar datos de cualquier tipo de fuente, formato y ubicación.

REQ147. El Subsistema de Correlación de eventos y datos deberá ser una plataforma única de software y contar con una arquitectura flexible y escalable.

REQ148. El Subsistema de Correlación de eventos deberá alimentarse del módulo de big data el cual tiene una base de datos no relacionada, y deberá tener rápido acceso a los logs (originales) que gatillan las alertas en el sistema a partir de los eventos de seguridad.

REQ149. El Subsistema de Correlación de eventos deberá contar con una arquitectura flexible y escalable.

REQ150. El Subsistema de Correlación de eventos deberá contar con bitácoras de eventos generados por sus sistemas operativos, servidores de aplicación, servidores Web, Bases de datos, aplicaciones hechas en casa, eventos recibidos de dispositivos de seguridad y de red.

REQ151. El Subsistema de Correlación de eventos deberá utilizar un tratamiento universal para los datos recolectados, capturando, leyendo y generando índices para su posterior identificación almacenamiento.

REQ152. Subsistema de Correlación de eventos deberá tener la capacidad de generar a partir de la información (lenguaje de máquina) generar dashboard de desempeño de aplicativos o eventos de interés.

REQ153. El Subsistema de Correlación de eventos deberá permitir una vez que los datos de TI estén indexados, estos se encontrarán disponibles para realizar descubrimientos, hacer investigaciones de seguridad y/o desempeño, monitoreo de red y aplicaciones, crear reportes de cumplimiento, dashboard de desempeño, así como cualquier otro proceso.

REQ154. El Subsistema de Correlación de eventos deberá poder trabajar en dos modalidades:

a) Captura sin agente, en esta se puede configurar el SIEM para escuchar de manera permanente en un puerto TCP o UDP (se recomienda TCP) o bien para que busque los eventos desde una carpeta compartida en la red o bien para que a través del protocolo WMI interrogue a servidores con plataforma Microsoft respecto a las métricas.

b) Usando un Agente, que es un componente que se instala en los servidores que generan los datos o que pueden colectar datos de otros sistemas. El agente deberá consumir como máximo el 5% de los recursos de los servidores en donde se instala.

REQ155. El Subsistema de Correlación de eventos deberá contar con un lenguaje de búsqueda robusto, efectivo y sencillo de entender permitiendo la búsqueda por cualquier palabra o frase contenida en los eventos de seguridad.

REQ156. El Subsistema de Correlación de eventos deberá contar con funcionalidades para utilizar condiciones y operaciones lógicas permiten refinar las búsquedas.

REQ157. El Subsistema de Correlación de eventos deberá contar con funcionalidades para rastrear transacciones o incidentes de seguridad entre múltiples sistemas.

REQ158. El Subsistema de Correlación de eventos deberá permitir crear reportes y vistas que permitan entender mejor los procesos que monitorean.

REQ159. El Subsistema de Correlación de eventos deberá permitir localizar en el tiempo los momentos en que se presente un mayor número de eventos permitiendo identificar tendencias, niveles máximos y anomalías. Además con el SIEM se podrá ejecutar un proceso de Drill Down que consiste en buscar de manera profunda la causa raíz de los incidentes, enfocándose solo en aquellos eventos que son importantes para el proceso de investigación.

REQ160. Es requisito excluyente que la plataforma SIEM posea característica de respuesta adaptativa el cual utiliza el software como "centro neurálgico de seguridad" o “Security Nerve Center” para conectar la inteligencia de múltiples tecnologías de seguridad. El software deberá tener la capacidad de integrarse con diferentes fabricantes a fin de automatizar de manera proactiva acciones automáticas que sean programables.

4.4.1. INFRAESTRUCTURA Y PLATAFORMA DE MAQUINA VIRTUAL

En términos del hardware requerido para la instalación del Subsistema de Gestión de Identidades y Control de acceso a la Red y el Subsistema de Gestión de dispositivos móviles se

requiere que el OFERENTE suministre e instale en el data center corporativo de Metro S.A. una infraestructura y plataforma de Máquina Virtual (VM) Hiperconvergente, que sea capaz de unificar en un solo sistema las capacidades de software virtualizado, capacidad de cómputo y acceso a la red.

REQ161. La infraestructura de Máquina Virtual Hiperconvergente deberá contar en su arquitectura base o mínima con capacidad agregada en cómputo de servidores con las siguientes características.

Ítem	Descripción	Cantidad Unitaria	Cantidad Total Requerida
CPU	2.20 GHz E5-2630 v4/85W 10C/20MB Cache/DDR4 2133MHz	2	6
MEMORY	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	8 (256 GB)	24 (768 GB)
HARD DISK	1.2 TB 12G SAS 10K RPM SFF HDD	6 (7,2 TB)	18 (21,6 TB)
Interconexión de RED Hiperconvergencia	2X Switches Layer 2 hardware forwarding at 960 Gbps or 714.24 million packets per second (mpps) / 1+1 PS Redundancy / 48 port 1/10G SFP+ (16 licensed only)	1 SW	2 SW

Tabla 2: Capacidad de crecimiento de cómputo HW infraestructura de Máquina Virtual Hiperconvergente.

REQ162. La infraestructura de Máquina Virtual Hiperconvergente deberá contar con una capacidad agregada de cómputo, valores que están indicados antes de la de-duplicación y compresión.

REQ163. La capacidad de cómputo total de la infraestructura de Máquina Virtual Hiperconvergente deberá ser de hasta 8 nodos o servidores , de acuerdo a la siguiente tabla:

Ítem	Descripción	Cantidad Unitaria	Cantidad Total Requerida
CPU	2.20 GHz E5-2630 v4/85W 10C/20MB Cache/DDR4 2133MHz	2	16
MEM	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	16 (512 GB)	128 (4096 GB)
HDD	1.2 TB 12G SAS 10K RPM SFF HDD	6 (7,2 TB)	48 (57,6 TB)
Interconexión de RED Hiperconvergencia	2X Switches Layer 2 hardware forwarding at 960 Gbps or 714.24 million packets per second (mpps) / 1+1 PS Redundancy / 48 port 1/10G SFP+ (16 licensed only)	1 SW	2 SW

Tabla 3: Capacidad Máxima de cómputo HW infraestructura de Máquina Virtual Hiperconvergente.

REQ164. La infraestructura de Máquina Virtual Hiperconvergente deberá proporcionar de-duplicación para redundancia de los datos y compresión para la optimización de la capacidad de almacenamiento.

REQ165. EL OFERENTE deberá proporcionar sobre la plataforma hiperconvergente la virtualización de cada solución requerida, además de proveer alta disponibilidad de cada aplicativo que resida en el sistema, finalmente deberán proveer integración de los diferentes componentes de software tal y como se indica en el punto 4.5, para lo cual el ambiente a virtualizar corresponde a:

a) Gestión de Identidades y Control de acceso a la Red en HA de Aplicativo.
b) Solución MDM con Front-End (Certificado) y BackEnd (Base de Datos) en HA de Aplicativo.
c) Certificado valido para MDM (vínculo con dispositivos móviles).
d) Herramienta de Correlación de Eventos (SIEM) en HA de Aplicativo.
e) Consola de Gestión de Firewalls.
f) Cualquier otra máquina virtual que requiera la solución.

REQ166. EL OFERENTE deberá contemplar los licenciamientos a nombre de Metro S.A, sistemas operativos y componentes necesarios y para la correcta operación del proyecto, de acuerdo a lo requerido en el punto 4.5 y en base a lo indicado en la Tabla 4.

REQ167. El hardware de la máquina virtual deberá contar con una arquitectura flexible y escalable.

Ítem	Código	Descripción	Cantidad
1	VS6-OEPL-AK-C	VMware vSphere 6 with Operations Management Enterprise Plus Acceleration Kit for 6 processors	1
2	VS6-OEPL-AK-3G-SSS-C	Basic Support/Subscription VMware vSphere with Operations Management Enterprise Plus Acceleration Kit for 6 processors for 3 years	1
3	CAL Windows	Licenciamiento Microsoft Windows Server 2012R2 (3 Server's)	3
4	CAL Windows	Licenciamiento Microsoft SQL Server 2012 (1 instancia / Cluster-Mirroring)	1

Tabla 4: Licencias para hardware de Máquina Virtual

Ítem	Especificación
Chassis	1RU of rack space for the node
Processors	2 Intel Xeon processor E5-2600 v4 family CPUs (For a complete list of processor options, refer to the node's technical specifications documents.)
Interconnect	2 Intel Quick Path Interconnect (QPI) channels per processor, each capable of 8.0 and 9.6 gigatransfers per second (GTPS)
Chip set	Intel C610 series
Memory	▪ 24 DDR4 DIMM slots ▪ Support for DDR4 registered DIMMs (RDIMMs) ▪ Advanced error-correcting code (ECC) ▪ Independent channel mode ▪ Lockstep channel mode
PCIe slots	2 PCIe 3.0 slots: ▪ Riser 1: 1 full-height, 3/4-length slot with x24 connector and x16 lane ▪ Riser 2: 1 half-height, half-length slot with x24 connector and x16 lane
Embedded network interface card (NIC)	Dual 1-Gbps Intel i350 Ethernet ports
mLOM	Cisco UCS VIC 1227
Power Supplies	Hot-pluggable, redundant 770W power supplies
FlexFlash SD cards	▪ 2 internal 64-GB FlexFlash drives (SD cards) ▪ Support for Utility mode with out-of-band updates of utility partitions
IMC	▪ Integrated baseboard management controller (BMC) ▪ IPMI 2.0 compliant for management and control ▪ One 10/100/1000 Ethernet out-of-band management interface ▪ Command-line interface (CLI) and web GUI management tool for automated, lights-out management ▪ Keyboard, video, and mouse (KVM) console
Front-panel connector	One KVM console connector (supplies 2 USB connectors, 1 VGA connector, and 1 serial connector)

Ítem	Especificación
Front-panel locator LED	Indicator to help direct administrators to specific servers in large data center environments
Additional rear connectors	Additional interfaces including a VGA video port, 2 USB 3.0 ports, an RJ45 serial port, a 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports
Software support	▪ vSphere Enterprise and vSphere Enterprise Plus ▪ ESX 6.0 U1 patch 1 ▪ Cisco UCS Manager 2.2

Tabla 5: Especificaciones Infraestructura y Hardware Máquina Virtual

4.5. INTEGRACIÓN DE LAS PLATAFORMAS

En términos de la integración de los Subsistemas descritos en el presente documento de especificaciones de la Solución de Seguridad, Metro S.A. requiere los servicios de implementación de estas Subsistemas con una interacción e integración transversal y centralizada, para lo cual, cada una de Subsistemas descritos en los puntos anteriores, Seguridad Perimetral, Gestión de Identidades y Control de acceso a la Red, Gestión de Dispositivos Móviles, Correlación de Eventos y la Infraestructura y Plataforma de Máquina Virtual, infraestructura y plataforma que alojará los Subsistemas de Gestión de Identidades y Control de acceso a la Red, MDM y Correlación de Eventos; esta misma integración general para la solución global de Seguridad.

REQ168. El OFERENTE deberá integrar las cada Subsistema para que la Solución de Seguridad del P63 opere correctamente. La solución en términos referenciales deberá ser conformada de acuerdo a la siguiente figura.

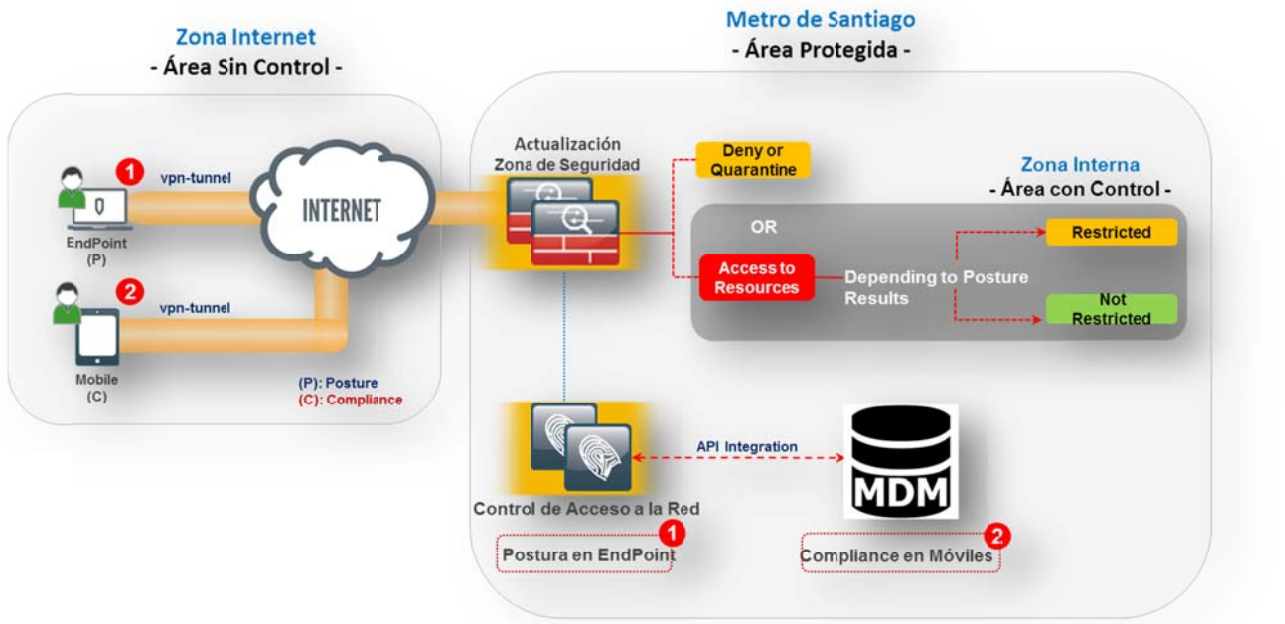

Figura N° 2: Diagrama conceptual solución de Seguridad.

REQ169. El OFERENTE deberá ejecutar las actividades necesarias para que Metro tenga la interacción e integración de forma global y específica de las herramientas descritas en los puntos 4.1, 4.2, 4.3, 4.4.1 y 4.4.1, de forma tal de que se realice correctamente la autenticación, autorización y auditoría (AAA).

REQ170. El OFERENTE deberá ejecutar las actividades necesarias para lograr la interacción e integración de los accesos tanto internos como externos para cada requerimiento de conexión de los de forma tal de que valide cada Endpoint (Dispositivo móvil, equipo portátil, estación de trabajo) en términos de Autenticación, autorización y auditoría (AAA).

4.6. REQUERIMIENTOS GENERALES

REQ171. El OFERENTE deberá suministrar, instalar, configurar, integrar y poner en funcionamiento todo el equipamiento y subsistemas necesario y declarados en el presente documento en el data center corporativo de la subgerencia TIC, ubicada en edificio Corporativo de Metro S.A. Para lo cual Metro requiere que el contratista adjudicado cumpla con la siguiente programación:

a) 15 de agosto 2017, instalación de Subsistemas del punto N° 4.1, 4.2 y 4.3

b) 15 de agosto 2017, instalación de Subsistemas del punto N° 4.1, 4.2, ambos subsistemas operando completamente.
c) 15 de septiembre 2017, instalación de Subsistema del punto N° 4.3, operando.
d) 11 de noviembre de 2017, instalación de Subsistema del punto N° 4.4 y operando completamente 15 diciembre de 2017.

Nota: se entenderá que el plazo entre la puesta en operación de las letras b) y c) podrá ser utilizado por el contratista adjudicado a razón de realizar las configuraciones o tunning necesarios para que la operación, ajustes y configuraciones, permitan que los subsistemas operen correctamente.

REQ172. El OFERENTE deberá ejecutar las actividades de interconexión de las nuevas herramientas (NGFW, Gestión de Identidades y Control de acceso a la Red, MDM y Correlacionador de Eventos) con el equipamiento de CORE mediante cable FTP Cat 6A o jumper de FO en caso de ser necesario.

REQ173. El OFERENTE, podrá realizar trabajos diurnos y nocturnos, para el caso de los diurnos es posible realizar toda actividad que no tenga relación con intervención de la red. Para el caso de los trabajos nocturnos se deberá coordinar con Metro cualquier tipo de trabajo que considere una intervención o corte de servicio en la zona de seguridad.

REQ174. El OFERENTE deberá ofrecer un diseño que sea capaz de ofrecer crecimiento, escalabilidad y alta disponibilidad (HA) para la Solución de Seguridad.

REQ175. Todo el equipamiento debe tener origen por compra directa al fabricante efectuada por Partners autorizados en Chile para tales efectos o de distribuidores autorizados por el Fabricante para su venta y distribución en territorio nacional (Chile). Además, el contratista deberá validar y resguardar que el equipamiento a instalar no se encuentre en estado EoS, EoL u otra definición de obsolescencia equivalente del fabricante. De lo contrario deberá utilizar las últimas versiones homologadas de software y equipamiento disponible sin anuncio de obsolescencia del fabricante.

REQ176. Podrán participar todos los Canales Autorizados en Chile por el fabricante para la venta y distribución de equipamiento de comunicaciones, donde el Partner deberá al menos contar con una certificación de Partner Premier del Fabricante.

REQ177. El CONTRATISTA deberá contar con Ingenieros certificados en al menos lo siguientes items:

- CCNP Security
- Cisco CISE (Implementing and Configuring Cisco Identity Service Engine)

REQ178. Los servicios de SOPORTE deben ser prestados por Partners en territorio chileno autorizados por el Fabricante para tales efectos.

REQ179. Todo el equipamiento adquirido deberá contar con un soporte por parte del Fabricante en modalidad 24x7x4 por un período de 3 años, o un mecanismo equivalente entregado por el Partner que garantice el SLA solicitado (24x7x4). En caso de presentar una modalidad de soporte entregado por el Partner, el OFERENTE deberá entregar el procedimiento de registro de reporte e incidencia frente a un problema o incidencia con alguno de los subsistemas que componen la solución de seguridad.

REQ180. El equipamiento debe ser entregado a lo más dentro de los siguientes 30 días corridos de recibida la Orden de Compra por el OFERENTE ADJUDICADO.

REQ181. El OFERENTE deberá realizar una actividad de Skill Transfer consistente en 40 horas de capacitación en el uso global de la plataforma, que incluya: NGFW, Administración y Gestión de la VM, Gestión de Identidades y Control de acceso a la Red, MDM y Correlación de Eventos para un máximo de 20 de profesionales.

REQ182. El OFERENTE deberá considerar la provisión de un soporte local que consista en la atención de un Ingeniero de soporte de segundo nivel para atender necesidades de resolución de problemas, incidencias o soporte especializado. Para ello Metro requiere un SLA de 1 hora de tiempo de respuesta y 4 horas de tiempo de solución. Para lo anterior el OFERENTE deberá entregar el protocolo de ingreso de tickets y los datos de contacto para el registro y formalización de las solicitudes.

REQ183. El OFERENTE ADJUDICADO es el responsable único de la totalidad de los suministros para cumplir con la correcta operación de la Solución de Seguridad, tanto en equipamiento, componentes, configuraciones, cableado, garantías, soporte y otros incluidos en la presente licitación.

5. OBLIGACIONES DE METRO

METRO se comprometerá a cumplir los siguientes enunciados:

a) Coordinar los permisos de trabajo solicitados en horario laboral de lunes a viernes entre 09:30 a 18:30.
b) Gestionar los permisos de trabajo del OFERENTE de acuerdo al listado de personal entregado.
c) Entregar las facilidades de acceso a dependencias de METRO.
d) Entregar las facilidades de acceso al Data Center de Metro, ubicado en Alameda 1414, Edificio Corporativo SEAT, Piso N°3.
e) Entregar la información necesaria de los equipos de la zona de seguridad para facilitar las actividades análisis de datos y homologación.
f) Entregar un espacio y alimentación en un rack ubicado dentro del Data Center.

6. LISTADO DE EQUIPAMIENTO

De acuerdo a lo solicitado en los puntos anteriores del presente documento de especificaciones técnicas, el listado de equipamiento solicitado como suministro por METRO corresponde a:

a) Subsistema de Seguridad Perimetral

Ítem	Código	Descripción	Cantidad
1	ASA5585-S20F20-K9	ASA 5585-X SSP-20, FirePOWER SSP-20,16GE,4GEMgt,1AC,3DES/AES	2
2	CAB-C2316-C19-IT	CEI 23-16 to IEC-C19 14ft Italy	4
3	ASA5585-PWR-AC	ASA 5585-X AC Power Supply	2
4	SF-ASA-X-9.2.2-K8	ASA 9.2.2 Software image for ASA 5500-X Series,5585-X,ASA-SM	2
5	ASA5585-20CTRL-LIC	Cisco ASA5585-20 Control License	2
6	ASA5585-BLANK-HD	ASA 5585-X Hard Drive Blank Slot Cover	4
7	ASA-SSP-20-INC	ASA 5585-X Security Services Processor-20 with 8GE	2
8	ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2
9	ASA5585-PWR-AC	ASA 5585-X AC Power Supply	2
10	ASA-SFR-20-INC-K9	ASA 5585-X FirePOWER SSP-20, 8GE	2
11	SF-ASA-FP5.4-K9	Cisco FirePOWER Software v5.4 for ASA 5500-X	2

Tabla 6: Listado de Equipamiento Solución Seguridad Perimetral

b) Subsistema de Gestión de Identidades y Control de acceso a la Red

Ítem	Código	Descripción	Cantidad
1	R-ISE-VM-K9=	Cisco Identity Services Engine VM (eDelivery)	2
2	L-ISE-BSE-250=	Cisco Identity Services Engine 250 EndPoint Base License	1
3	L-ISE-PLS-S-250=	Cisco ISE 250 Endpoint Plus Subscription License	1
4	ISE-PLS-3YR-250	Cisco ISE 3-Yr 250 Endpoint Plus License	1
5	L-ISE-APX-S-250=	Cisco ISE 250 Endpoint Apex Subscription License	1
6	ISE-APX-3YR-250	Cisco ISE 3-Yr 250 Endpoint Apex License	1
7	L-AC-PLS-3YR-G	Legacy Ordering Method - Cisco AnyConnect / 3-Yr Plus	1
8	AC-PLS-3YR-250-S	Cisco AnyConnect 3-Yr 250 User Plus License	1
9	AC-PLS-3YR-250	Cisco AnyConnect 3-Yr 250 User Plus Subscription	1
10	L-AC-PLS-S-3Y-250	Cisco AnyConnect 3-Yr 250 User Plus (ASA License Key)	99999

Tabla 7: Listado de Equipamiento Solución Gestión de Identidades y Control de acceso a la Red.

c) Subsistema de Gestión de Dispositivos Móviles

Ítem	Código	Descripción	Cantidad

1	V-GMS-OPL-D-3G-C	VMware AirWatch Green Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	200

Tabla 8: Listado de Equipamiento Solución Gestión de Dispositivos Móviles

d) Infraestructura y Plataforma de Máquina Virtual

Ítem	Código	Descripción	Cantidad
1	HX-SP-220M4E2-FI	UCS SP HX220c Capacity + Addnl 2xFI reqd	1
2	UCS-HX-FI48P	UCS SP Hyperflex System 6248 FI w/ 12p LIC	2
3	UCS-ACC-6248UP	UCS 6248UP Chassis Accessory Kit	2
4	N10-MGT014-HX	UCS Manager v3.1 for HyperFlex	2
5	UCS-FI-DL2	UCS 6248 Layer 2 Daughter Card	2
6	UCS-BLKE-6200	UCS 6200 Series Expansion Module Blank	2
7	UCS-FAN-6248UP	UCS 6248UP Fan Module	4
8	SFP-10G-SR	10GBASE-SR SFP Module	8
9	DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+, LC	8
10	UCS-PSU-6248UP-AC	UCS 6248UP Power Supply/100-240VAC	4
11	CAB-9K10A-IT	Power Cord, 250VAC 10A CEI 23-16/VII Plug, Italy	4
12	HX-SP-220M4S-BE2	UCS SP HX220c Hyperflex System w/2xE52630v4,8x32Gmem	3
13	HX-CPU-E52630E	2.20 GHz E5-2630 v4/85W 10C/20MB Cache/DDR4 2133MHz	6
14	HX-MR-1X322RV-A	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	24
15	HX-HD12TB10K12G	1.2 TB 12G SAS 10K RPM SFF HDD	18
16	HX-SD480G12S3-EP	480GB 2.5 inch Ent. Performance 6GSATA SSD(3X endurance)	3
17	HX-SD120GBKS4-EV	120 GB 2.5 inch Enterprise Value 6G SATA SSD	3
18	HX-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	3
19	UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	3
20	HX-SD-64G-S	64GB SD Card for UCS Servers	6
21	UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	6
22	CAB-9K10A-IT	Power Cord, 250VAC 10A CEI 23-16/VII Plug, Italy	6
23	UCSC-HS-C220M4	Heat sink for UCS C220 M4 rack servers	6
24	HX220C-BZL-M4	HX220C M4 Security Bezel	3
25	UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)	3
26	SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	6
27	HX-SAS12GHBA	Cisco 12Gbps Modular (non-RAID) SAS HBA	3
28	HX-VSP-FND-D	Factory Installed - vSphere SW (End user to provide License)	3
29	HX-VSP-FND-DL	Factory Installed - VMware vSphere6 Fnd SW Download	3
30	HXDP-001-3YR=	Cisco HyperFlex HX Data Platform SW 3 year Subscription v1.8	3
31	HXDP001-3YR	Cisco HyperFlex HX Data Platform SW Subscription 3 Year v1.8	3

Tabla 9: Listado de Equipamiento Hardware Máquina Virtual

Ítem	Código	Descripción	Cantidad
1	VS6-OEPL-AK-C	VMware vSphere 6 with Operations Management Enterprise Plus Acceleration Kit for 6 processors	1
2	VS6-OEPL-AK-3G-SSS-C	Basic Support/Subscription VMware vSphere with Operations Management Enterprise Plus Acceleration Kit for 6 processors for 3 years	1
3	CAL Windows	Licenciamiento Microsoft Windows Server 2012R2 (3 Server's)	3
4	CAL Windows	Licenciamiento Microsoft SQL Server 2012 (1 instancia / Cluster-Mirroring)	1

Tabla 10: Licencias para hardware de Máquina Virtual