

# Boletín Oficial

DE LA PROVINCIA DE BUENOS AIRES

SUPLEMENTO DE 16 PÁGINAS  
Compras (Ley N° 14.815) y Sociedades

## Compras (Ley N° 14.815)

### NOTA:

El contenido de las publicaciones de Compras (Ley N° 14.815), es transcripción literal de los archivos recibidos oportunamente de cada Jurisdicción, conforme Resolución N° 4/16 de la Subsecretaría de Coordinación Gubernamental .

Compra Superior  
Dirección General de Cultura y Educación  
Dirección General de Administración  
(Dirección de Compras y Contrataciones)

### CIRCULAR MODIFICATORIA

**Organismo:** Dirección General de Cultura y Educación.

**Compra Superior:** N° 6/2016 autorizada y aprobada por Resolución N° 527/16.

**Publicación en Boletín Oficial por:** un (1) día.

**Expediente N°:** 5831-1264112/16

**Requiere:** Dirección de Tecnología de la Educación.

**Objeto:** Adquisición de insumos informáticos para implementar el Proyecto de Infraestructura y Sistemas de Conectividad para instituciones educativas

**Modificación:** En virtud de que en el Pliego de Especificaciones Técnicas se han incluido términos en idioma distinto al español, y a los efectos de una correcta comprensión por parte de los potenciales oferentes, se transcriben la totalidad de las mismas, las que reemplazan el Anexo IV oportunamente publicado.

### 1. GENERALIDADES

#### 1.1. Descripción del Proyecto

El Gobierno de la provincia de Buenos Aires a través del Ministerio de Educación presenta el Proyecto de Infraestructura y Sistema de Conectividad para Instituciones Educativas de la Provincia de Buenos Aires, el cual tiene como objetivo la provisión de servicios de Conectividad Alámbrica e Inalámbrica y Videoconferencia dentro de los establecimientos educativos, que sirvan como Infraestructura base de la difusión de contenidos educativos, capacitación docente educación a distancia y aulas inteligentes.

El proyecto aquí descrito cuenta con una topología descentralizada, en la cual todos los establecimientos educativos se conectaran directamente a internet para la consulta de contenido educativo, que será validado y gestionado de forma centralizada a través de la generación de VPNs con el datacenter, donde toda la plataforma será gestionada.

El sitio central contara con una salida a Internet donde se alojaran equipos centrales que permitirán la generación de redes VPN a cada uno de los establecimientos educativos antes referidos, dichas equipos centrales se encontraran en configuración de alta disponibilidad lo cual garantizara la continuidad de la operación.

Asimismo, en el sitio central se contara con la administración y control tanto de equipos remotos como de garantizar la autenticación de usuarios con Active Directory y las facilidades de identificación de usuarios establecida por el Ministerio de Educación para el acceso a portales, contenido e información propia de la institución, también como garantizar la experiencia del usuario en los sitios remotos, ya que los perfiles de usuario creados tanto en el sitio central como en los sitios remotos, permitirá a dichos usuarios tener la misma experiencia de ancho de banda, acceso a aplicaciones, contenido y privilegios en cualquier punto de la red tanto en sitio central como en sitios remotos. En este sitio central se podrá de igual forma, tener un balanceo de cargas de trafico si la conectividad a internet es a través de 2 ISPs diferentes.

Cada sitio remoto contara con equipamiento que permita el acceso a la red VPN garantizando la confidencialidad de la información, Se contara con funcionalidades de Firewall y Filtrado de Contenido como se describirá más adelante en este documento.

Los servicios con los que contara cada sitio remoto serán Acceso a la Red vía Alámbrica e Inalámbrica, Servidor para Almacenamiento de Contenidos y Videoconferencia.

Una característica muy importante a resaltar de esta solución, es que aun y cuando se pierda el acceso a la red VPN vía internet en cada sitio remoto, la red Alámbrica e Inalámbrica continuara en operación y se podrá tener acceso al Servidor de Contenidos instalado en cada sitio.

Otra característica a resaltar es, como cada sitio remoto estará contactado a través de enlaces de internet al sitio central, la información que sea requerida al sitio central viajara de forma segura del sitio central al remoto y viceversa. Si el sitio remoto requiere acceder a alguna página de internet, el usuario saldrá directamente a internet con las reglas y políticas establecidas tanto en el firewall como filtrado de contenidos, lo cual hará más eficiente el uso de ancho de banda en el sitio central.

El sistema de videoconferencia permitirá establecer sesiones de Educación a Distancia, tanto para alumnos como para maestros en cada sitio remoto, se podrán compartir material audiovisual además de la sesión de videoconferencia.

El propósito de esta infraestructura es habilitar a los establecimientos educativos, que forman parte de este alcance, a integrar de forma transparente Aulas Inteligentes en cada uno de ellos.

Al integrar tanto los servicios de autenticación, ancho de banda, control de acceso a aplicaciones, perfiles de usuario, tipo de dispositivo, lugar de acceso, tipo de red accedida (Alámbrica o Inalámbrica) tipo de servicio requerido (Internet o Intranet), políticas y reglas de firewall y filtrado de contenido, mejorara la experiencia del usuario, reforzaran la seguridad de la red y el Ministerio de Educación del Gobierno de la provincia de Buenos Aires cumplirá con el objetivo propuesto inicialmente en el presente documento.

## 1.2. Condiciones Generales

El ADJUDICATARIO deberá proveer, configurar y poner en operación todo el equipamiento pedido en el presente pliego, y realizar las pruebas, puesta en funcionamiento y verificación de calidad de todo el sistema de comunicaciones integrado (comunicación entre dependencias y sitio central).

Los OFERENTES deberán detallar en su OFERTA, todas las subcontrataciones a realizar para cumplir con los trabajos ofertados, indicando razón social de la empresa a sub contratar, alcance y descripción de las tareas para cada caso. Todas las facilidades, prestaciones, características y especificaciones del hardware y software ofertado que sean necesarias para que dicho hardware y software se ajuste a los requerimientos aquí enunciados, deberán estar disponibles (liberadas al mercado) al momento de la apertura de las ofertas. No se aceptarán facilidades o componente alguno que solo estén disponibles en versiones beta de los paquetes de software o a modo de prototipo en el hardware.

Los elementos, unidades funcionales, dispositivos y accesorios estarán constituidos por unidades nuevas, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso, sin admitirse tampoco elementos de segunda calidad o reparados o reacondicionados en fábrica).

A modo de garantizar compatibilidad a lo largo del tiempo y una gestión integral de toda la red, los equipos de comunicaciones (switches, UTM, Access Points y servidores) y equipos de video conferencia a proveer en todos los establecimientos y sitio central, deberán ser de la misma marca y el mismo fabricante.

Los equipos de red, access points, switches Enrutadores y UTM, deben ser gestionados en forma centralizada a modo de servicio brindado con la conexión a internet. La plataforma de gestión será alojada en el sitio central, y desde la misma se controlaran todos los dispositivos.

La solución inalámbrica de red debe de estar equipada con la habilidad de detectar la presencia del dispositivo de usuario, generados por los radios WiFi encendidos en Smartphone, laptops y tabletas.

La gestión y configuración de los equipos UTM, Switches y Access points, a modo gráfico, pudiendo ver detalle de status y configuración del dispositivo haciendo click sobre el icono del mismo.

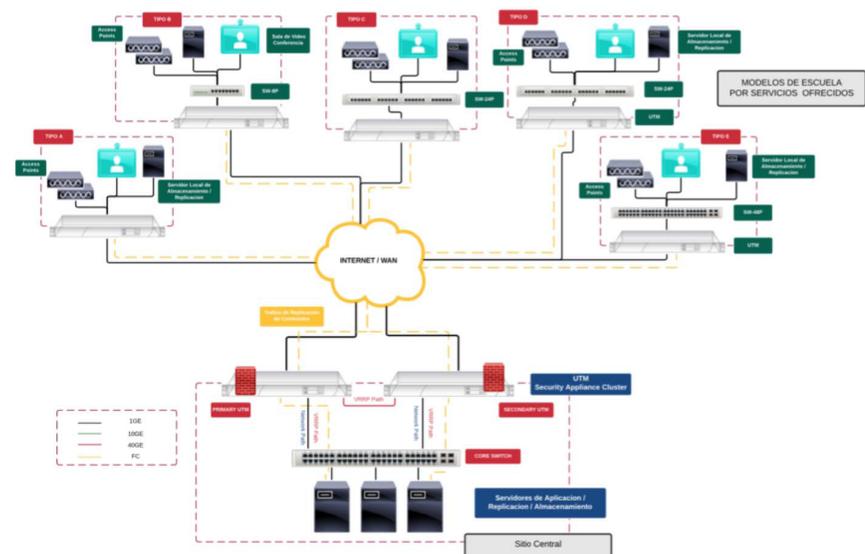
También debe ser posible agregar planos de planta y ubicar los dispositivos en forma activa, además de poder agregar en forma manual los access points que brindan servicio

Todo el equipamiento de red (switches, Access Points, UTM) deberá ser del mismo fabricante y deberá poder gestionarse desde un sistema unificado de gestión.

## 2. PLIEGO DE CONDICIONES TÉCNICAS

### 2.1. Diagrama Esquemático de la Red

El diagrama referencial de la solución propuesta debe basarse en un modelo hub-&-Spoke, donde todos los sitios deberán conectarse a un sitio central desde el cual harán la replicación de las aplicaciones que estén alojadas en el sitio central, como también de la distribución de contenidos dispuestos por el organismo encargado.



Para cada establecimiento se pedirán: Access Points, UTM, switches, equipos de cómputo y equipos de video conferencia.

En el sitio central se pedirán Switches centrales, plataforma de gestión (plataforma de gestión de red + plataforma de control de red), firewalls centrales y MCU.

## 2.2. ESPECIFICACIONES TÉCNICAS

### 2.2.1. PLATAFORMA DE GESTIÓN

El PROVEEDOR deberá proveer, instalar en el datacenter indicado por el comitente, poner en funcionamiento y parametrizar, una plataforma de gestión para la totalidad de equipos, cuyas dos principales funcionalidades sean la gestión y el control de la red, según se detalla a continuación:

#### Plataforma de Management de red

##### Administración

- El sistema usara una arquitectura navegador/servidor (B/S) y soportara el modo de instalación basado en componentes bajo demanda para ajustarse a las necesidades del servicio. El sistema deberá soportar navegadores comerciales de la industria como Internet Explorer, Firefox y Chrome.
- El sistema soportara como mínimo alguno de los siguientes sistemas operativos ampliamente usados en la industria y deberá contar con los últimos parches: Windows Server 2012 R2 standard, standard o Novell SUSE Linux Enterprise Server-Enterprise-11.0 SP3. El fabricante debe proveer tomas de pantalla y ligas que prueben ello en los sitios oficiales de internet.
- El sistema deberá usar software de base de datos reconocido en la industria tales como MySQL, SQL Server 2012 y/o Oracle. Para mejorar la seguridad de toda la solución, el sistema deberá soportar modos de despliegue distribuidos y centralizados para la base de datos. El fabricante debe proveer tomas de pantalla y ligas que prueben ellos en los sitios oficiales de internet.
- El deberá proveer capacidades de administración a gran escala. Un grupo simple del sistema deberá manejar no menos de 18,000 recursos de red.
- El sistema deberá soportar modos de despliegue en clúster de un solo nodo y clúster de dos nodos. El sistema deberá ser instalado tanto en servidores físicos y máquinas virtuales (VMs).
- Todas las interfaces internas y externas de comunicación del sistema deben usar protocolos de seguridad tales como SSHv2, TLS1.0, SSL3.0, IPSec, SFTP y SNMPv3.
- El fabricante debe de proveer una herramienta de endurecimiento de seguridad, incluyendo el sistema operativo y base de datos. La herramienta de endurecimiento de seguridad debe ser provista con el sistema de administración.
- Información clave involucrada tales como passwords y llaves deben de estar encriptados y ninguna información debe ser desplegada en texto plano en el sistema.
- El sistema debe de contar con software antivirus para escaneo de seguridad, este software antivirus debe de ser de marcas reconocidas de la industria tales como Symantec, OfficeScan, McAfee, Avira AntiVir y Kaspersky. El resultado del uso y escaneo por parte de este software antivirus deberá mostrar que el sistema no está infectado por virus o atacado por Caballos Troyanos.
- El sistema debe manejar dispositivos de fabricantes de la industria incluyendo Cisco, Huawei, HPE entre otros.
- El sistema debe de proveer una capacidad de rápida tropicalización en el manejo básico de dispositivos para otros fabricantes y tropicalizar el desarrollo de funciones de manejo avanzadas basadas en las necesidades del servicio.
- El sistema deber manejar uniformemente ruteadores, switches, firewalls, dispositivos WLAN, servidores, almacenamiento, dispositivos de videovigilancia y analizar los servicios. El fabricante debe proveer tomas de pantalla y ligas que prueben ello en los sitios oficiales de internet

- El sistema debe soportar agrupamiento definido por el usuario de objetos administrados (dispositivos y puertos). Para reducir complejidad en la administración, el sistema automáticamente aplica alarmas, desempeño, y políticas de seguridad a los grupos. De esta forma, los administradores no necesitan desarrollar la misma operación para múltiples ocasiones.
- El sistema proveerá capacidades de monitoreo gráfico amigable y desplegar topologías de red. Los usuarios podrán desarrollar operaciones en las topologías, por ejemplo, revisar tráfico, desempeño y acceder a la información de terminales o dividir una región entre varias subregiones. En adición, la información multi dimensional deberá ser desplegada en la o las topologías.
- El sistema permite a los usuarios tropicalizar nodos de topología, tales como dispositivos y enlaces. Los usuarios podrán también ocultar o desocultar nodos de red en las topologías y cambiarlas a sus estilos propios.
- Manejo WLAN
  - El sistema deberá soportar capacidades de configuración de servicios WLAN detallados. Todas las configuraciones WLAN deben ser configuradas en el sistema de administración.
  - El sistema debe soportar monitoreo de WLAN en una base 24/7 y el monitoreo de la topología visible debe ser por regiones.
  - El sistema debe desplegar el status de la red inalámbrica como status del dispositivo, recursos de red, Fuentes de interferencia, región y tipo de servicio. Por ejemplo, uso de canal de AP, estadísticas de usuario y AP por región, estadísticas de tipo de radio cliente, estadísticas de SSID basado en acceso de usuario y desplegar información histórica de acceso de usuario.
  - El sistema debe analizar calidad de la red para usuarios regionales y desplegar información agregada basada en la región en la topología.
  - El sistema deberá proveer detección inteligente del lado de usuarios y fallas en el lado de la red para ayudar a los administradores a rápidamente diagnosticar la causa raíz en múltiples dimensiones, tales como terminal, SSID, AP y AC. El fabricante debe de proveer tomas de pantalla relacionadas a su solución
  - El sistema deberá proveer derechos y administración basada en dominios para los APs.
  - El sistema deberá soportar políticas de administración de conservación de energía, para deshabilitar APs, radios y SSIDs inmediatamente o a un tiempo previamente programado.
- Monitoreo de flujo en tiempo real
  - El sistema deberá soportar monitoreo de la red IP basada en flujos reales de servicio (monitoreo de paquetes no simulado o pruebas) para proveer garantía en tiempo real a servicios clave. Los usuarios pueden habilitar o deshabilitar la función basada en las necesidades del servicio. El sistema deberá desplegar el resultado del monitoreo en topologías en tiempo real. El fabricante debe de proveer tomas de pantalla relacionadas a su solución
  - El monitoreo de la red IP en tiempo real debe ser hecho a nivel de dispositivo, nivel de enlace y nivel de red. El fabricante debe proveer material ilustrando la implementación técnica.
  - El sistema debe monitorear el número de paquetes perdidos y la proporción de paquetes perdidos en enlaces directos entre 2 dispositivos en tiempo real y recoger las estadísticas relacionadas para diferentes prioridades. El sistema deberá desplegar las estadísticas en topologías en tiempo real. El fabricante debe de proveer tomas de pantalla relacionadas a su solución
  - El sistema debe monitorear el número de paquetes perdidos y la proporción de paquetes perdidos en trayectorias de servicio, detectar nodos de red a lo largo de las trayectorias de servicio de reenvío y monitorear el número de paquetes perdidos y la proporción de paquetes perdidos en enlaces entre cada 2 nodos. Esta función ayudara a los administradores a determinar el rango de falla. El fabricante debe de proveer tomas de pantalla relacionadas a su solución.
  - El sistema deberá generar alarmas cuando la proporción de paquetes perdidos en el monitoreo exceda el umbral predefinido, para informar a los administradores del sistema en tiempo real.
- Manejo de Alarmas
  - El sistema debe monitorear las alarmas de los dispositivos de la red completa en una base 24/7 y enviar notificaciones a través de emails o mensajes SMS. Los usuarios pueden tropicalizar el contenido de la notificación.
  - Los detalles de alarmas deberán incluir información relacionada a la falla, por ejemplo, Puerto asociado, falla, topología de enlace, información histórica de tráfico y experiencia en mantenimiento por falla de puerto. El fabricante debe de proveer tomas de pantalla relacionadas a su solución.
  - Todas alarmas que se generen en el momento (un máximo de 20,000 registros) deberá ser desplegada en una sola página.
- Manejo de Performance
  - El sistema deber monitorear el desempeño de la red en tareas bajo una base 24/7. Los usuarios podrán cambiar el umbral de condiciones de desempeño para generar alarmas de

advertencia de eventos críticos, mayores y menores. El sistema comparara y permitirá a los usuarios ver el desempeño histórico de la red. El fabricante debe de proveer tomas de pantalla relacionadas a su solución

- Los usuarios del sistema podrán ver y editar los contadores de desempeño monitoreados y los intervalos de recolección en la página de administración del desempeño. El sistema desplegara las páginas de monitoreo de desempeño, con los parámetros previamente establecidos, tales como las columnas y la longitud de las mismas basado en la cuenta de ingreso al sistema.
- Simulación de Trafico
  - El sistema deberá simular paquetes en una base 24/7 y monitorear contadores de QoS tales como proporción de perdida de paquetes, latencia y jitter en enlaces clave.
  - El sistema deberá proveer muchos tipos de modo de monitoreo y permitir a los usuarios comparar y ver información que monitorea en múltiples dimensiones. Los modos de monitoreo deberán incluir ICMP Echo, ICMP Jitter, UDP Echo, UDP Jitter, TCP, Connect, SNMP, DNS, DHCP, HTTP, FTP, LSP Ping y LSP Trace.
- Análisis de Trafico
  - El sistema deberá analizar tráfico de red IP usando NetFlow, NetStream o SFlow para obtener la distribución de tráfico de red.
  - El sistema deberá permitir a los usuarios ver las hojas de estadísticas de tráfico en diferentes dimensiones, tales como dispositivo, interfaz, aplicación, DSCP, host, sesión, grupo de interfaz, grupo IP, grupo de aplicación y grupo DSCP. El sistema debe analizar el tráfico en la capa de datos por capa y permitir a los usuarios crear tareas de trafico forense basadas en las dimensiones.
  - El sistema deberá permitir a los usuarios, tráfico de origen basada en el host fuente, Puerto fuente, host de destino, puerto de destino, protocolo, interfaz de ingreso, interfaz de egreso, bandera TCP y siguiente salto. El sistema filtrara tráfico origen basado en condiciones de filtro definidas por el usuario para localizar tráfico anormal. El sistema deberá exportar y guardar los resultados de las tareas de tráfico forense.
- Manejo de Seguridad
  - El sistema deberá instalarse en un grupo de servidores, sistemas operativos y bases de datos para implementar una administración unificada de dispositivos de comunicación de datos y firewalls.
  - El sistema permitirá a los usuarios configurar políticas de seguridad, analizar más de 60 tipos de eventos de seguridad y generar reportes y gráficas. El reporte incluirá reportes de ataques DDoS, antivirus, IPS, reportes de comportamiento en línea y reportes de tráfico.
  - El sistema deberá analizar eventos de seguridad en toda la red, verificar políticas, evaluar la salud de las políticas y proveer sugerencia de ajustes.

## Plataforma de control de red

### Administración

- User Management
  - Autenticación a través de cuentas locales y passwords y autenticación asociativa por servidor de dominio Active Directory (AD), servidor LDAP y servidor RADIUS de terceras partes como fuentes de autenticación de identidad.
  - Autenticación a través de asociación de CA/USBKey y servidor RSA
  - Sincronización de usuario basada en OU, grupos de usuarios y atributos de cuenta
  - Asociación simultánea con múltiples servidores AD/LDAP en ambientes multi dominio
  - Función de best effort de servidores AD/LDAP que aseguren la alta confiabilidad cuando el servidor AD/LDAP falle.
  - Administración de grupo de usuarios estructurada en árbol que sea idéntica con la estructura de gestión administrativa en la red viva, que simplifique la administración de usuarios.
  - Administración de Roles: Administradores podrán desarrollar gestión de autorización basada en el rol del usuario.
  - Tecnologías para identificar múltiples tipos de dispositivos, incluyendo SNMP, Usuario-Agente, DHCP y MAC OUI, tipos, sistemas operativos y fabricantes de terminales de acceso a redes inalámbricas que puedan ser identificadas.
  - Agrupación automática y manual basada en el resultado de identificación de tipo de dispositivo.
- Guest Management
  - Permitir que personal administrador y gestores de visitas puedan crear cuentas de visitantes. Los administradores podrán crear una cuenta simple de visitante o cuentas de visitantes en modo batch. Deberá soportar exportación de cuentas de visitantes, impresión y notificación a través de emails y mensajes SMS.
  - Permitir que visitantes puedan aplicar a una cuenta temporal de forma de autoservicio. Después de que los administradores aprueben la aplicación, una notificación puede ser enviada al visitante via web, mensaje SMS o email. A los visitantes se les podrá permitir aplicar para una cuenta sin aprobación.

- Se podrá cambiar cuentas, políticas de generación de passwords, periodo de validez y de información para el registro de visitantes en modo autoservicio.
- Se podrán hacer definiciones propias de páginas de autenticación de múltiples portales y páginas de registro de cuentas, incluyendo palabras desplegadas, instrucciones de usuario, logotipos y agregar imágenes. Soportara función de tropicalización avanzada de edición HTML
- Agregara una página de post autenticación en una política de saltos para cada página de autenticación, saltando la página original y la pagina especificada.
- Usará diferentes páginas de portal de autenticación y páginas de registro basadas en diferentes condiciones como dirección IP de las terminales, AP de acceso tipo de dispositivo y SSID de acceso.
- Proveerá APIs externos para sistemas de terceros para agregar, borrar o modificar una cuenta de visitante.
- **Free Mobility**
  - Proveerá múltiples modos de autenticación tales como 802.1x, MAC, Portal, gateway de seguridad y modos de autenticación VPN, con lo cual se implementara una autenticación unificada en redes cableadas/inalámbricas e internas/externas.
  - Proveer múltiples protocolos de autenticación tales como PAP, CHAP, EAP-MD5, EAP-PEAP-MSCHAPV2, EAP-TLS, EAP-TTLS-PAP y EAP-PEAP-GTC.
  - Proporcionar Administración de Políticas de Seguridad para Acceso a la Red basado en usuario/grupo de usuario/identidad del usuario, lugar de acceso, tipo de dispositivo, grupo de dispositivo, hora de acceso y modo de acceso.
  - Se deberá manejar prioridad de múltiples políticas de autorización. La política de mayor prioridad será preferentemente asignada.
  - Deberá prevenir ataques de MAC spoofing en escenarios de acceso donde terminales tontas son autenticadas en modo de autenticación MAC. Si un dispositivo falso accede la red, el dispositivo real puede ser identificado y el dispositivo falso será aislado o bloqueado.
  - Se deberá contar con división de usuarios y recursos de servicio en diferentes grupos de seguridad. Los administradores podrán desarrollar administración de política de acceso bidireccional, incluyendo grupo de seguridad de usuario a acceso de grupo de seguridad de servicio, acceso a grupo de seguridad inter usuario y grupo de seguridad de servicio a acceso grupo de seguridad de uso.
  - Proveerá autorización rápida de grupo de seguridad basada en escenario. A través de la integración con la topología de la red, los administradores pueden rápidamente cambiar políticas de acceso a la red basadas en condiciones como el rol del usuario, hora de acceso, lugar de acceso, tipo de dispositivo y modo de acceso.
  - Se deberá incluir entrega unificada de políticas de seguridad de grupo para dispositivos asociados, la cual asegure que usuarios puedan tener las mismas políticas de acceso a la red en cualquier lugar. Debe soportar sincronización incremental y despliegue de status síncrono.
  - Se deberá proveer de configuración de ancho de banda de red basada en el usuario y prioridad de servicio después de acceder a la red interna desde una red externa, garantizando una experiencia de calidad en el acceso a la red para usuarios en específico.
- **Aprovisionamiento automático de equipos.**
  - El sistema deberá proveer a través de una interfaz gráfica (GUI) que deberá permitir realizar la planificación completa de la red, generación de configuraciones, correcciones de topología y mostrar procesos de avances de implementaciones que permitan acortar los tiempos de implementación y facilitar la operación.
  - El sistema deberá proveer un modo de aprovisionamiento a través de SMS con routers integrados con un módulo 3G/LTE que permitan simplificar el proceso de implementación
  - Que un solo controlador soporte un máximo de 10,000 usuarios concurrentes y que el sistema completo soporte hasta un máximo de 100,000 usuarios.

**2.2.2. RENGLÓN 1: SWITCHES LAN CENTRAL**

El PROVEEDOR deberá proveer, instalar en el datacenter indicado por el comitente, poner en funcionamiento y configurar, switches de CORE que cumplan con todo lo especificado a continuación:

**ÍTEM 1: Switch Principal para centro de cómputos. (SpineSwitch)**

Cantidad solicitada: 2 (dos)

- Deberá soportar arquitectura Leaf-and Spine.
- Deberá poder operar bajo el rol de Spineswitch.
- Debe permitir conexión de al menos 36 switchesLeaf.
- La capacidad de conmutación será como mínimo de 2.22Tbps.
- Poseer la cantidad de fuentes de alimentación necesarias para que el sistema sea redundante del tipo N+1, es decir, que soporte la caída de una fuente sin resentir el sistema alimentado. Deberá poder conectarse directamente a la red de suministro de energía eléctrica de 220 V - 50 Hz, así como

poseer conexión a tierra.

- Debe incluir la cantidad de dispositivos para ventilación forzada necesarios para asegurar la redundancia de estos dispositivos (tipo N+1).
- Se deberán proveer todos los elementos necesarios para poder instalar el equipo en un gabinete de comunicaciones estándar de 19".

Conectividad:

Cantidad de puertos	Tipo de puertos
Al menos 36	40 G QSFP

- Deberá incluir al menos 4 (cuatro) módulos de fibra de 40GBASE-SRBDi, dúplex MMF con conector LC.

**ÍTEM 2: Switch de acceso para centro de cómputos (LeafSwitch)**

Cantidad solicitada: 2 (dos)

- Deberá soportar arquitectura Leaf-and Spine.
- Deberá poder operar como nodo leaf. (En caso de requerir licencia deberá incluir la misma para la totalidad de los puertos de downlink)
- La capacidad de conmutación será como mínimo de 2.20 Tbps.

Conectividad:

Cantidad de puertos	Tipo de puertos
Al menos 48	10 G SPF+
Al menos 6 UPLINK	40/100 G QSFP28

- Deberá incluir al menos 4 (cuatro) módulos de fibra de 40GBASE-SRBDi, dúplex MMF con conector LC.
- Deben poseer fuente de alimentación redundante del tipo 1+1 y poder conectarse directamente a la red de suministro de energía eléctrica de 220 V - 50 Hz, así como poseer conexión a tierra.
- Dispositivos de ventilación forzada redundantes.
- Se deberán proveer todos los elementos necesarios para poder instalar el equipo en un gabinete de comunicaciones estándar de 19".

**ÍTEM 3: Hardware y Software de Administración SDN**

Cantidad solicitada: 1 (uno)

- Se deberá proveer una arquitectura de Servidores (CLUSTER) para soportar no menos de MIL (1000) puertos, con las siguientes funcionalidades:
  - La capacidad de crear y aplicar políticas de red centradas en aplicaciones.
  - Un marco abierto a través de API ascendentes y descendentes.
  - La integración de servicios de capa 4 a capa 7 de terceros, virtualización y administración. Debe poder administrar equipos de terceros como por ejemplo F5, Citrix, A10, Checkpoint.
  - Visibilidad y telemetría inteligente para aplicaciones y clientes.
  - Visibilidad centralizada a nivel de la aplicación con supervisión del estado de la aplicación en tiempo real en los entornos físicos y virtuales.
  - Operaciones simplificadas en todos los elementos de la aplicación, de red y de seguridad.
  - Deberá permitir filtros de capa 4 entre los dispositivos evitando el uso de un firewall interno.
  - Deberá poder administrar las redes virtuales de los distintos hipervisores como VMARE, Microsoft, KVM y "containers" sin ninguna licencia adicional.
  - Plataforma común para administrar entornos físicos, virtuales y en la nube.
  - API abiertas, estándares abiertos y elementos de código abierto que permiten la flexibilidad del software para los equipos de desarrollo y operaciones (DevOps) y la integración con otros sistemas.
  - En caso de licenciar por equipo, deberá incluirse la licencia para los todos equipos del presente renglón como mínimo.

**2.2.3. RENGLON 2: UTM CENTRAL**

El PROVEEDOR deberá proveer, instalar en el DataCenter indicado por el comitente, poner en funcionamiento y configurar, UN equipo de seguridad que debe ser un sistema integrado de Administración Unificada de Amenazas (UTM por sus siglas en inglés), que en un mismo equipo (una unidad de hardware) incluya las siguientes funcionalidades como mínimo:

- Stateful Firewall
- Filtrado de Contenido
- Antivirus/anti-phishing
- IDS/IPS
- Optimización de enlace WAN
- Antimalware

Administración

- Gestión centralizada desde una consola de administración basada en Web fuera de banda, desde la cual se deberá poder acceder, configurar y monitorear, todos los equipos de seguridad considerados en esta licitación
- Deberán existir mecanismos para agrupar lógicamente la administración de un número determinado de dispositivos UTM para propósitos de empujar cambios simultáneos en sus configuraciones
- La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones educativas
- El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo mas no limitando a nombre de usuario, contraseña, en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet
- La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola
- El nivel jerárquico de los administradores de la consola deberán ser los siguientes:
  - Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todas las redes dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura.
    - El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:
      - Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
      - Resetear contraseñas
      - Crear, editar y borrar redes
      - Agregar nuevos dispositivos a las redes de la organización
    - Administrador de Red: Tendrá visibilidad en aquellas redes de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de red podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
      - Crear, editar y borrar otras cuentas de administrador dentro de la red
      - Crear, editar y borrar redes para las cuales cuente con privilegios

Características físicas del equipo

- Su arquitectura deberá soportar que los módulos de control, de interface y procesamiento sean independientes.
- Poseerá slots de expansión  $\geq 2$
- Deberá contener al menos

(1) Dos x 10GE interfaces

(2) Ocho x GE interfaces

Tendrá fuente de energía redundante y "hot swap" para recambio en caliente.

Requisitos de performance

- El máximo número de conexiones concurrentes deberá ser mayor a 2 millones.
- El throughput de VPN IPSec debe superar los 1 Gbps
- La cantidad de tuneles VPN soportados deberá ser mayor a 5000
- La cantidad políticas de seguridad deberá ser mayor a 12000

Servicios de Red

El equipo propuesto debe contar con los siguientes servicios de red:

- Capacidad de registrarse a su consola de gestión de forma automática para obtención de su configuración y firmware correspondientes
- Múltiples salidas WAN (2 al menos) con encapsulación IP, PPPoE
- Capacidad para perfilar y listar características de los dispositivos que se conecten a través de él, cableados o inalámbricos, vía direcciones MAC o IP
- Servicio incluido de DynamicDNS
- Servicios NAT hacia la red WAN para segmentos de red internos (NAT uno a varios)
- Soporte de creación y manejo de VLAN con IEEE 802.1Q
- Deberá contar con la funcionalidad de crear múltiples ins-

tancias de servidor de DHCP. En caso de que el cliente desee preservar sus DHCPs internos, el equipo deberá de ser capaz de integrarse en modo puente para propagar los servicios de este tipo al interior de la red

- Soporte de NAT 1:1 y Port Forwarding para la publicación de sistemas específicos a Internet
- Soporte para la creación de DMZs , o Zonas Demilitarizadas
- Deberá soportar ruteo estático como mínimo
- Deberá contar con la funcionalidad de AutoVPN para configurar de manera automática túneles de IPSec en las topologías de sitio a sitio, hub-and-spoke y full mesh
- De igual manera deberá soportar sin licenciamiento adicional la creación de Client VPNs, mediante IPSec
- Para los enlaces WAN, el UTM propuesto deberá soportar la configuración de balanceo de enlaces (Load Balancing) para que cuando se habilite, pueda propagar el tráfico sobre los enlaces WAN disponibles en proporciones a especificarse de parte de la licitante
- Adicionalmente y cuando el cliente así lo requiera, el equipo deberá ser configurado para asignar preferencias de enlace de salida para cierto tipo de tráfico, basado en:
  - Tipo de protocolo (TCP o UDP)
  - Rango de direcciones locales, subred o red de clase completa
  - Puerto local (TCP o UDP)
  - Rango de direcciones remotas, subred o red de clase completa
- La asignación de ancho de banda mediante el modelado de tráfico, deberá poderse definir mediante dos mecanismos:
  - Manual
    - Rangos CIDR/IP
    - hostname (URL)
    - Puertos UDP/TCP
    - Combinación de Red, Subnet y puerto
    - Red local (subredes y redes de clase completa en la LAN)
  - Mediante categorías de tráfico
    - Blogging
    - Email
    - Compartición de archivos
    - Juegos
    - Noticias
    - Respaldo en línea
    - Peer-to-peer
    - Redes sociales y compartición de fotos
    - Actualizaciones de programas y antivirus
    - Deportes
    - VoIP y videoconferencia
    - Compartición de archivos vía web
- La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación, por usuarios y por grupo de usuarios
- De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y/o asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz)
- Deberá soportar controles de acceso basado en múltiples elementos, tales como la dirección IP origen, el puerto origen, la dirección IP destino, el puerto destino, el protocolo, tiempo, listas negras, y listas negras dinámicas.
- VPN (Redes privadas virtuales)
  - Deberá soportar: IPSec VPN, GRE VPN y GRE sobre IPSec VPN.
  - Deberá estar provisto con un Software de gestión VPN para configurar y gestionar el Gateway de VPN y los clientes de una manera centralizada.
  - Deberá Soporta IPSec VPN CA authentication.
  - Soportará IPSec VPN hot standby, incluyendo VPN dual-link hot standby que aseguren la continuidad de los servicios VPN
- Deberá soportar la selección inteligente de uplink, el cuál podrá seleccionar una interfaz de salida de forma dinámica, para maximizar la eficiencia de los vínculos y mejorar la experiencia del usuario. Además, deberá ante la caída de un vínculo cambiar a otros vínculos conectados asegurando la alta disponibilidad del servicio.
- Basado en una base de datos de firmas de aplicaciones, el tráfico de la red deberá ser identificado y clasificado, para ser luego ordenado de acuerdo a su prioridad.
  - Anti-virus y Antipishing
    - La solución deberá de contar con un motor de antivirus y antipishing, dicho motor deberá de tener las siguientes capacidades:
      - El fabricante del motor deberá ser parte de los líderes del ultimo cuadrante magico de gartner publicado en febrero de 2016:



- El motor de antivirus y antipishing deberá de soportar la detección en tráfico entrante y saliente http, detectando trojanos y pishing.
- La solución deberá de poder manejar listas blancas usando los siguientes parametros:
  - Listas blancas por URL
  - Listas blancas por ID de evento
- Detección y Prevención de Intrusos
  - La solución deberá poner a disposición de la [Institución], la capacidad de habilitar el módulo de IDS o de IPS conforme lo requiera
  - Deberá permitir la selección del nivel de prevención de amenazas como Alta, Medía y Baja prioridad
  - De igual manera, deberá permitir la inclusión en listas blancas de una o varias firmas de IDS/IPS para removerlas de la acción de bloqueo
  - El motor de IPS/IDS deberá estar basado en SNORT.
  - El motor de IPS/IDS deberá de contar con la capacidad de incluir firmas de tipo SNORT.
  - La solución ofertada deberá de contar con diferentes categorías para la definición de reglas y políticas en el modulo de IPS/IDS:
    - Conectividad:
      - Contiene las reglas que son del año en curso y los dos años anteriores, incluye vulnerabilidades con una puntuación CVSS de 9 o mayor.
    - Balanceado
      - Contiene las reglas que son del año en curso y los dos años anteriores, incluye vulnerabilidades con una puntuación CVSS de 9 o mayor, y se encuentran en una de las siguientes categorías:
        - Malware-CNC:
        - Blacklist:
        - SQL Injection:
        - Exploit-kit:
    - Seguridad
      - Contiene reglas que son de el año en curso y los tres años anteriores, están en busca de vulnerabilidades con una puntuación CVSS de 8 o superior, y se encuentran en una de las siguientes categorías:
        - Malware-CNC:
        - Blacklist:
        - SQL Injection:
        - Exploit-kit:
        - App-detect:
  - La solución ofertada deberá de soportar la definición de listas blancas basadas en firmas de SNORT

- Antimalware  
La solución ofertada deberá de contar con capacidades para la detección de malware y código malicioso de día Zero, que incluya las siguientes características:

- La solución deberá de soportar la inspección sobre el tráfico HTTP de los siguiente tipos de archivos:

- MS OLE2 (.doc, .xls, .ppt)
- MS Cabinet (Microsoft compression type)
- MS EXE
- ELF (Linux executable)
- Mach-O/Unibin (OSX executable)
- Java (class/bytecode, jar, serialization)
- PDF
- ZIP (regular and spanned)\*
- (standardized test file)
- SWF (shockwave flash 6, 13, and uncompressed)

- La solución deberá de soportar la configuración de las siguientes acciones:

- Clean - The file is known to be good.
- Malicious - The file is known to be harmful.
- Unknown - There is insufficient data to classify the file as clean or malicious.

- La solución deberá permitir la re categorización de las disposiciones en caso de que existan cambios en los archivos, dicha reclasificación generara alertas retrospectivas y notificaciones.

- La solución deberá de poseer la capacidad de filtrar búsquedas de eventos maliciosos con los siguientes elementos:

- Red actual
- Detección de malware
- IDS
- Limpio
- Malicioso
- Desconocido
- Bloqueado
- Permitido

- Dichos eventos maliciosos deberán de poder ser filtrados según los siguientes rangos de tiempo:

- Por las ultimas dos horas
- Por el ultimo día
- Por la ultima semana
- Por el ultimo mes

- La solución deberá permitir la búsqueda de eventos maliciosos por:

- Identificación de cliente (Hostname)
- URI
- SHA256 file hash
- ID de regla IPS/IDS

- La solución deberá soportar la generación de informes que contengan la siguiente información:

- Los clientes más afectados por Sistema Operativo
- Los principales orígenes de los ataques (Geo Localización)
- Ranking de las principales amenazas

Vision retrospective de Malware

- Network Address Translation (NAT)
  - Deberá soportar NAT, incluyendo Interface Address Translation (muchos a uno) Static Address Translation (uno a uno) Address Pool Translation (muchos a muchos) y Port Translation (uno a muchos)
  - Deberá soportar extensiones de NAT para la traducción infinita de direcciones IP.
  - Deberá soportar smart NAT (NOPAT-to-PAT) y el NAT deberá soportar los siguientes protocolos: DNS, FTP, H323, MGCP, MMS, MSN, PPTP, QQ, RTSP, SIP, SQLNET, ILS, NETBIOS, RSH, SCCP.
- Link aggregation
  - Deberá soportar 802.3ad link aggregation para unir multiples puertos como un solo Puerto lógico para expandir el ancho de banda.
- Disponibilidad
  - Deberá soportar la sincronización de sesiones.

- Deberá soportar "Hot standby" que permita tomar el control si el dispositivo primario falla.
- Deberá soportar "hot patches and software upgrade" parches y actualizaciones sin interrumpir el servicio.
- Deberá implementar prevención de intrusiones y el resguardo de los servicios de IPsec y NAT en modo "active/standby" junto con el balanceo de carga de red.
- Deberá soportar avisos de contenido HTTP/HTTPS/FTP como defensa ante virus-web
- Deberá soportar DLP(Data leaking Protection)
- Deberá soportar gestión por línea de comandos o consola, basado en seguridad SSHv2
- Control de aplicaciones
- Soportará la visibilidad y control de aplicaciones para monitorear comportamientos específicos de al menos 6000 protocolos de aplicación que podrán ser identificados y controlados, soportar la definición de nuevas aplicaciones

**Filtrado de URLs**

- Deberá soportar librerías tipo servicios-en-la-nube. Con al menos 60 millones de URL que puedan ser identificadas.
  - Deberá permitir organizar las URL en categorías y subcategorías, permitiendo al administrador aplicar restricciones o permisos aplicados por categorías.
  - Deberá proveer listas negras de URL y funciones de listas blancas.

**Servicios de Seguridad**

La solución de UTM debe de incluir las siguientes funcionalidades de seguridad:

- Stateful Firewall
  - La solución deberá soportar la definición de reglas de firewall de capa 3 y capa 7.
    - Mediante las reglas de capa 3, se definirán políticas de acceso por:
      - Protocolo (UDP o TCP)
      - Host, subred o red origen
      - Puerto TCP o UDP origen
      - Host, subred o red destino
      - Puerto TCP o UDP destino
    - Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
      - Blogging
      - Email
      - Compartición de archivos
      - Juegos
      - Noticias
      - Respaldo en línea
      - Peer-to-peer
      - Redes sociales y compartición de fotos
      - Actualizaciones de programas y antivirus
        - Deportes
        - VoIP y videoconferencia
        - Compartición de archivos vía web
    - Políticas basadas en identidad
      - La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Directorio de la Organización
      - Políticas basadas en grupos
        - Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
        - Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna
      - Filtrado de contenido
        - La función de Filtrado de Contenido, deberá estar integrada en el mismo dispositivo UTM
          - Deberá soportar grupo de políticas de filtrado de contenido para la protección de contenido perjudicial para niños.
          - Deberá permitir la creación de forma manual de listas blancas y listas negras de URLs
            - Como parte de las funciones de filtrado, deberá permitir de filtrar el contenido de las búsquedas sobre los principales buscadores en la red, incluyendo Google, Bing y Yahoo
              - Puesto que el acceso a Google particularmente se realiza de forma encriptada, la solución deberá permitir la restricción de este tipo de búsquedas

- Reglas IP's basadas en Geografía
  - Será posible especificar reglas que limiten el tráfico desde / hacia ciertas naciones, o mantener interacciones dentro de una sola nación

**Reportes**

- La solución deberá generar sobre demanda, un reporte de seguridad por la última hora, la última semana, el último mes y sobre un período específico de monitoreo
- Se deberá generar una gráfica en el tiempo de los eventos clasificados por su severidad (Alta, Mediana y baja), así como un listado de los eventos de seguridad detectados en el período de tiempo seleccionado
- Se deberá incluir como reporte la lista de usuarios contabilizados sobre la solución de seguridad, por hora, día, semana y mes identificando el nombre del equipo y/o dirección MAC, última fecha y hora en que se detectó al usuario, la utilización de la red en Bytes, sistema operativo del equipo y dirección IP. Este reporte deberá estar disponible para su descarga en formato CSV or PDF or WORD y/o XML.

**2.2.4. RENGLON 3: CONFERENCIA DE VIDEO**

El PROVEEDOR deberá proveer un servicio de conferencias de video multi-punto que incluya las siguientes funcionalidades como mínimo:

- Compatible con ITU-T H.323, IETF SIP.
- El servicio deberá contar con mecanismos de alta disponibilidad, sin presentar puntos únicos de falla en toda la solución, manteniendo la performance y escalabilidad solicitada. Detallar.
- Deberá soportar H.235 (AES-256), SRTP, TLS
- Deberá soportar 720p30 y ser compatible con 4CIF y CIF.
- Deberá soportar transcodificación de presentaciones para permitir que tanto las terminales HD y SD soporten los protocolos de presentación H.264, H.263, y H.263+
- Deberá soportar AAC-LD, G.722.1, G.722.1C, G.711, G.722, G.728, G.729, e iLBC.
- Deberá permitir a varias terminales (HD o SD) unirse a la misma conferencia
- Deberá soportar conexiones concurrentes de por lo menos 20 participantes a 720p30 por reunión y una capacidad no inferior a 20 reuniones simultáneas
- Deberá ser capaz de añadir una presentación mediante H.239/BFCP

**2.2.5. RENGLON 4: PLATAFORMA DE ADMINISTRACIÓN PARA SOLUCIÓN DE VIDEO CONFERENCIA**

Se deberá proveer junto con los equipos de video conferencia, una plataforma de administración que cumpla con lo siguiente:

- La plataforma de administración debe ser una plataforma de gestión de servicios independiente para la gestión de conferencias, administración de dispositivos, autenticación, control de conferencia y recopilación de estadísticas. La plataforma de administración debe ser de la misma marca del equipo multi-punto y contar con una descripción de sus especificaciones en el sitio web oficial de su proveedor original
- La plataforma de administración debe utilizar la arquitectura navegador / servidor y residir en un servidor físico separado en vez de estar embebido en el servidor web del MCU
- La plataforma de administración deberá ser compatible con IPv4 e IPv6
- La plataforma de administración deberá ser capaz de mostrar la gestión de los dispositivos para que los usuarios puedan obtener rápidamente la información de monitoreo de recursos del sistema en forma de gráficos en una página de administración. La información de monitoreo de recursos del sistema deberá incluir información de monitoreo de los dispositivos, información de monitoreo del sistema y el uso de recursos del sistema (Uso de CPU y uso de memoria)
- La plataforma de administración deberá permitir que los derechos del usuario sean configurados basándose en la estructura organizacional, debiendo soportar por defecto tres tipos de usuario: Administrador del sistema, Administrador de conferencias y usuario común. El administrador del sistema deberá ser capaz de añadir y personalizar otro tipo de usuarios según se vaya requiriendo
- La plataforma de administración deberá soportar la capacidad de remotamente añadir, administrar y manipular en su totalidad la configuración de terminales en tiempo real.
- La plataforma de administración deberá ser capaz de administrar y manipular la configuración de terminales de otros fabricantes tanto local como remotamente en tiempo real.
- La plataforma de administración debe ser capaz de identificar automáticamente dispositivos cuando estos sean añadidos, permitir que los usuarios visualicen y configuren la información del dispositivo una vez que los dispositivos hayan sido identificados. Deberá ser posible hacer respaldos, así como restauraciones remotas de los dispositivos administrados.
- La plataforma de administración debe proveer la administración de alarmas del sistema permitiéndole a los usuarios:

- Ver remotamente la información de las alarmas de los dispositivos que están siendo administrados
- Ordenar las alarmas por tipo
- Obtener el estado de funcionamiento de los dispositivos administrados rápidamente
- La plataforma de administración debe permitir que los registros de incidentes de los dispositivos administrados, tanto nativos como de terceros, se puedan visualizar remotamente.
- La plataforma de administración deberá soportar las funciones de:
  - Unirse a una conferencia ad hoc usando un número de acceso unificado por múltiples MCUs
  - Asignar inteligentemente recursos de MCU para llevar a cabo conferencias
  - La plataforma de administración deberá soportar la definición de URI y llamadas por URI en un dominio o entre dominios.
  - La plataforma de administración deberá soportar la asignación de recursos de conferencia sin prestar atención a la capacidad de puertos de un solo MCU, de manera que cuando uno de ellos no sea capaz de satisfacer los requerimientos de recursos de conferencia, la plataforma pueda entonces automáticamente disponer de recursos de otros MCUs para satisfacer el requerimiento de puertos de conferencia.
  - La plataforma de administración deberá:
    - Generar reportes por participantes en una conferencia y utilización de MCU
    - Generar CDRs, los cuales deberán poder exportarse
    - Proveer múltiples modos para un reporte, tales como tablas, gráficas, etc.
    - La plataforma de administración deberá soportar definir diferentes zonas para las terminales registradas, soportar administración de ancho de banda y control de enrutamiento entre diferentes zonas.
    - La plataforma de administración deberá soportar LDAP.
    - La plataforma de administración deberá integrar software de monitoreo de red en la interfaz web y desplegar información acerca del estado de la red, tal como la pérdida de paquetes, jitter en la red y latencia. También deberá ser posible exportar estadísticas de red para conferencias y sitios y proveer archivos y respaldos de dichas estadísticas.
    - La plataforma de administración debe permitirle a los usuarios visualizar remotamente los mensajes de los sitios administrados en tiempo real en la interfaz web.
    - La plataforma de administración deberá soportar la capacidad de remotamente actualizar en tandas o grupos el o los MCUs y terminales que se encuentran siendo administrados, así como la posibilidad de personalizar la fecha y hora de la actualización. No se aceptarán soluciones en donde se actualice un solo dispositivo a la vez y que además se haga uso de otras herramientas ajenas a la propia plataforma de administración.
    - La plataforma de administración deberá:
      - Permitir a los usuarios personalizar plantillas en tandas o grupos
      - Posibilitar invocar directamente las plantillas que sean configuradas en tandas o grupos para configurar remotamente de una forma rápida
      - Soportar la función de bloqueo de configuración
    - La plataforma de administración deberá soportar las siguientes funciones:
      - Llamar a diversos sitios con el clic de un botón
      - Silenciar y remover el silencio de los micrófonos o altavoces con el clic de un botón
      - Ver el estado de audio de los micrófonos en tiempo real
      - La plataforma de administración debe permitir ajustar rápidamente el video de un sitio durante las conferencias seleccionando un sitio de conferencia para remotamente controlar su cámara (incluyendo controles PTZ y manipular el enfoque de la cámara).
      - La plataforma de administración deberá soportar las funciones de bloquear y desbloquear conferencias.
      - La plataforma de administración deberá soportar bloquear la fuente de video de un sitio
      - La plataforma de administración deberá soportar la función de seleccionar presencia continua o presencia activada por voz, por sitio.
      - La plataforma de administración deberá soportar la programación de conferencias con soporte de grabación. En conferencias con soporte de grabación, los usuarios deberán poder iniciar y detener la grabación y las transmisiones en vivo.
      - Los URLs hacia las grabaciones deberán poder ser enviados por correo electrónico a los sitios

#### 2.2.6. RENGLON 5: ACCESS POINT PARA DEPENDENCIAS

El PROVEEDOR deberá proveer equipos de punto de acceso, que cumplan con las características detalladas en el presente renglón. La cantidad a proveer deberá ser la suficiente para garantizar redundancia de señal en cada una de las aulas, de las 300 dependencias incluidas en el alcan-

ce del proyecto. El sistema deberá realizar ajustes de potencia de los APs en forma automática, para ajustar áreas de cobertura en caso de falla de alguno de los AP.

Para tal fin se debe considerar un promedio de 20 aulas por dependencia, en cada una de las cuales existirá 1(uno) puesto cableado para APs.

Con la solución implementada, en cada aula deberán coexistir las señales de Access Points distintos, pudiendo ser una de ellas la del Access point alojado en el aula, y la otra proveniente del AP en aula contigua.

El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, deberá ser una solución basada en el estándar IEEE 802.11ac, que permita habilitar el acceso de red para los usuarios en general para dispositivos móviles (tablets y smartphones), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, deberán contemplarse como mínimo las siguientes funcionalidades:

- Operación dual-band en 2.4 y 5Ghz
- Estándar de operación IEEE 802.11ac como principal, con soporte de estándares anteriores como 802.11a/b/g/n
- Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet
- Conexión a la red alámbrica en 100BaseT
- Control de Acceso Basado en políticas de agrupación de usuarios, soportando mínimo 256 usuarios por Access Point.

El equipo a proponerse por los participantes, deberá cumplir con las siguientes especificaciones técnicas:

#### Administración

- Gestión centralizada desde una consola de administración basada en Web, desde la cual se deberá poder acceder, configurar y monitorear, todos los equipos de red considerados en esta licitación
- La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones del participante
- El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo mas no limitando a nombre de usuario, contraseña, en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola de gestión deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet
- La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola
- El nivel jerárquico de los administradores de la consola deberán ser los siguientes:
  - Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todas las redes dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura.
    - El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:
      - Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
      - Resetear contraseñas
      - Crear, editar y borrar redes
      - Agregar nuevos dispositivos a las redes de la organización
    - Administrador de Red: Tendrá visibilidad en aquellas redes de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de red podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
      - Crear, editar y borrar otras cuentas de administrador dentro de la red
      - Crear, editar y borrar redes para las cuales cuente con privilegios

#### Características Físicas de los Equipos

El Access Point propuesto debe contar con las siguientes características Físicas:

- Antenas integradas al interior del equipo del tipo omnidireccional
- Alimentación PoE de 24 - 57 V, compatible con IEEE 802.3af ó IEEE 802.3at, asegurando que la alimentación requerida por el equipo, asegure su operación a carga máxima
- Soporte de alimentación con eliminador de DC externo a 12V, 1.5A
- Consumo máximo de potencia de 18W
- Placa para montaje en pared

- o Mínimo acceso de usuarios  $\geq 256$
- o Soporte de configuración de modo centralizado sin necesidad de configuración local por Access Point (zero touch).
- o Soporte Control de Acceso y administración de ancho de banda basado en SSID, Grupo de usuarios, ACL  $\geq 1k$
- o Protección de sobre-tensión  $\geq 4Kv$
- o Alimentación PoE y con Fuente.

**Servicios de Red**

El Access Point propuesto debe contar con los siguientes servicios de red:

- Interfaz de Radio Frecuencia:
  - o Total compatibilidad del estándar IEEE802.11 a/b/g/n/ac, para ambos radios en 2.4Ghz y 5Ghz.
  - o Funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro.
  - o Arreglo MIMO 2x2 con dos tramas espaciales (2 spatial streams)
  - o Selección de ancho de banda de canales de 20 MHz, 40MHz y 80 MHz
  - o Tasa de datos efectiva mínima de 1,167 Gbps
  - o Soporte de Maximal Ratio Combining (MRC)
  - o Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1) y 5.725-5.825GHz (UNII-3)
  - o La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:
    - Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz
    - 5GHz únicamente
    - Ambas bandas pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada
  - o Formación de haz (beamforming)
  - o Agregación de paquetes
  - o Soporte a Cyclic Shift Diversity (CSD)

**Interfaz alámbrica de red:**

- o Una interfaz 100/1000Base-T (RJ-45) con soporte a 48V DC 802.3af para PoE
- o VLAN tagging basado en IEEE802.1q
- o Soporte switchover entre the Media Dependent Interface (MDI) y Media Dependent Interface Crossover (MDI-X)
- o Soporte VLAN trunk en Uplink Ethernet Port
- o Soporte DHCP client, obteniendo direcciones IP por medio de DHCP.
- o Soporte STA isolation en la misma VLAN.
- o Soporte LLDP y/u otro mecanismo de descubrimiento automático

**Calidad de Servicio:**

- o Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
- o Soporte WMM power Saving
- o Soporte limitación de Ancho de Banda basado en usuario.
- o Soporte ajuste de Ancho de banda basado en el número de usuarios y radio environment para mejorar las experiencias del usuario final.
- o Soporte de DSCP 802.1p
- o Modelado de tráfico a nivel de capa 7 (L7)
  - Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se debe soportar la capacidad de restringir o abrir el ancho de banda por usuario y por SSID, QoS de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.
  - o La asignación de ancho de banda mediante el modelado de tráfico, deberá poderse definir mediante dos mecanismos:
    - Manual
      - Rangos IP
      - hostname (URL)
      - Puertos UDP/TCP
      - Red local (subredes y redes de clase completa en la LAN)
    - Mediante categorías de tráfico
      - Blogging
      - Email
      - Compartición de archivos
      - Juegos
      - Noticias
      - Respaldo en línea
      - Peer-to-peer
      - Redes sociales y compartición de fotos

- Actualizaciones de programas y antivirus
- Deportes
- VoIP y videoconferencia
- Compartición de archivos vía web

- La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios.
- De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y asociarse a una etiqueta de Qos mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz).

**Servicios de seguridad**

La solución de Red Inalámbrica debe de incluir las siguientes funcionalidades de seguridad:

- Firewall
  - o La solución inalámbrica de red deberá soportar la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.
    - Mediante las reglas de capa 3, se definirán políticas de acceso por:
      - Protocolo (UDP o TCP)
      - Host, subred o red origen
      - Puerto TCP o UDP origen
      - Host, subred o red destino
      - Puerto TCP o UDP destino
    - Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
      - Blogging
      - Email
      - Compartición de archivos
      - Juegos
      - Noticias
      - Respaldo en línea
      - Peer-to-peer
      - Redes sociales y compartición de fotos
      - Actualizaciones de programas y antivirus
      - Deportes
      - VoIP y videoconferencia
      - Compartición de archivos vía web
  - o Políticas basadas en identidad
    - La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Directorio de la Organización, LDAP o credenciales de Radius del cliente
  - o Políticas basadas en grupos
    - Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
      - Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna
  - o Control de acceso a la red inalámbrica: Access point deberá soportar la creación de 15 SSIDs por Radio, permitiendo para cada uno los siguientes métodos de acceso:
    - Abierta y sin encriptación para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo
    - Llave compartida con anterioridad (Pre-Shared key) con WPA2
    - Control de acceso basado en dirección MAC mediante autenticación Radius
    - WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
      - Un servidor Radius incluido en la misma solución
      - Un servidor Radius externo del cliente contra una base de datos genérica de usuarios o bien integrada con Directorio de la Organización y/o LDAP
    - Con excepción de la autenticación portal captivo deberá ser personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.
      - De igual manera, se deberá contar con la funcionalidad de Walled Garden, que permita el



- El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo mas no limitando a nombre de usuario, contraseña en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet
- La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola .El nivel jerárquico de los administradores de la consola deberán ser los siguientes:
  - Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todas las redes dentro de la organización. Existirán dos tipos de administradores dela organización: (1) Acceso completo y (2) Sólo lectura.
    - El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:
      - Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
      - Resetear contraseñas
      - Crear, editar y borrar redes
      - Agregar nuevos dispositivos a las redes de la organización
  - Administrador de Red: Tendrá visibilidad en aquellas redes de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de red podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
    - Crear, editar y borrar otras cuentas de administrador dentro de la red
    - Crear, editar y borrar redes para las cuales cuenta con privilegios

**Servicios de Red**

El equipo propuesto debe contar con los siguientes servicios de red:

- Capacidad de registrarse a su consola de gestión de forma automática para obtención de su configuración y firmware correspondientes
- Múltiples salidas WAN (2 al menos) con encapsulación IP, PPPoE
- Capacidad para perfilar y listar características de los dispositivos que se conecten a través de él, cableados o inalámbricos, vía direcciones MAC o IP
- Servicio incluido de DNS dinámico.
- Servicios NAT hacia la red WAN para segmentos de red internos (NAT uno a varios)
- Soporte de creación y manejo de VLAN con IEEE 802.1Q
- Deberá contar con la funcionalidad de crear múltiples instancias de servidor de DHCP. En caso de que el cliente desee preservar sus DHCPs internos, el equipo deberá de ser capaz de integrarse en modo puente para propagar los servicios de este tipo al interior de la red
- Soporte de NAT 1:1 y Port Forwarding para la publicación de sistemas específicos a Internet
- Soporte para la creación de DMZs , o Zonas Demilitarizadas
- Deberá soportar ruteo estático como mínimo
- Deberá contar con la funcionalidad de AutoVPN para configurar de manera automática túneles de IPSec en las topologías de sitio a sitio, hub-and-spoke y full mesh
- De igual manera deberá soportar sin licenciamiento adicional la creación de Client VPNs, mediante IPSec
- Para los enlaces WAN, el UTM propuesto deberá soportar la configuración de balanceo de enlaces (Load Balancing) para que cuando se habilite, pueda propagar el tráfico sobre los enlaces WAN disponibles en proporciones a especificarse de parte de la licitante
- Adicionalmente y cuando el cliente así lo requiera, el equipo deberá ser configurado para asignar preferencias de enlace de salida para cierto tipo de tráfico, basado en:
  - Tipo de protocolo (TCP o UDP)
  - Rango de direcciones locales, subred o red de clase completa
  - Puerto local (TCP o UDP)
- Rango de direcciones remotas, subred o red de clase completa Mediante la consola de administración, se debe soportar la capacidad de restringir o abrir el ancho de banda a cada enlace WAN simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades del enlace WAN. La asignación de ancho de banda mediante el modelado de tráfico, deberá poderse definir mediante dos mecanismos: Manual

- Rangos CIDR/IP
- hostname (URL)
- Puertos UDP/TCP
- Combinación de Red,Subnet y puerto
- Red local (subredes y redes de clase completa en la LAN)
- Mediante categorías de tráfico
  - Blogging
  - Email
  - Compartición de archivos
  - Juegos
  - Noticias
  - Respaldo en línea
  - Peer-to-peer
  - Redes sociales y compartición de fotos
  - Actualizaciones de programas y antivirus
  - Deportes
  - VoIP y videoconferencia
  - Compartición de archivos vía web
- La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación, por usuarios y por grupo de usuarios
- De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y/o asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz).

**Servicios de Seguridad**

La solución de UTM debe de incluir las siguientes funcionalidades de seguridad:

- Stateful Firewall
  - La solución deberá soportar la definición de reglas de firewall de capa 3 y capa 7.
  - Mediante las reglas de capa 3, se definirán políticas de acceso por:
    - Protocolo (UDP o TCP)
    - Host, subred o red origen
    - Puerto TCP o UDP origen
    - Host, subred o red destino
    - Puerto TCP o UDP destino
  - Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
    - Blogging
    - Email
    - Compartición de archivos
    - Juegos
    - Noticias
    - Respaldo en línea
    - Peer-to-peer
    - Redes sociales y compartición de fotos
    - Actualizaciones de programas y antivirus
    - Deportes
    - VoIP y videoconferencia
    - Compartición de archivos vía web
  - Políticas basadas en identidad
    - La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Directorio de la Organización
    - Políticas basadas en grupos
      - Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
      - Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna
- Filtrado de contenido
  - La función de Filtrado de Contenido, deberá estar integrada en el mismo dispositivo UTM
    - Deberá soportar grupo de políticas de filtrado de contenido para la protección de contenido perjudicial para niños.
    - Deberá permitir la creación de forma manual de listas blancas y listas negras de URLs
    - Como parte de las funciones de filtrado, deberá permitir de filtrar el contenido de las búsquedas sobre los principales buscadores en la red, incluyendo Google, Bing y Yahoo
      - Puesto que el acceso a Google particularmente se realiza

de forma encriptada, la solución deberá permitir la restricción de este tipo de búsquedas

- Reglas IP's basadas en Geografía
  - Será posible especificar reglas que limiten el tráfico desde / hacia ciertas naciones, o mantener interacciones dentro de una sola nación
- Anti-virus y Antipishing
  - La solución deberá de contar con un motor de antivirus y antipishing, dicho motor deberá de tener las siguientes capacidades:
    - El fabricante del motor deberá ser parte de los líderes del ultimo cuadrante magico de gartner publicado en febrero de 2016:



- El motor de antivirus y antipishing deberá de soportar la detección en tráfico entrante y saliente http, detectando trojanos y pishing.
- La solución deberá de poder manejar listas blancas usando los siguientes parametros:
  - Listas blancas por URL
  - Listas blancas por ID de evento
- Detección y Prevención de Intrusos
  - La solución deberá poner a disposición de la [Institución], la capacidad de habilitar el módulo de IDS o de IPS conforme lo requiera
  - Deberá permitir la selección del nivel de prevención de amenazas como Alta, Media y Baja prioridad
  - De igual manera, deberá permitir la inclusión en listas blancas de una o varias firmas de IDS/IPS para removerlas de la acción de bloqueo
  - El motor de IPS/IDS deberá estar basado en SNORT.
  - El motor de IPS/IDS deberá de contar con la capacidad de incluir firmas de tipo SNORT.
  - La solución ofertada deberá de contar con diferentes categorías para la definición de reglas y políticas en el módulo de IPS/IDS:
    - Conectividad:
      - Contiene las reglas que son del año en curso y los dos años anteriores, incluye vulnerabilidades con una puntuación CVSS de 9 o mayor.
    - Balanceado
      - Contiene las reglas que son del año en curso y los dos años anteriores, incluye vulnerabilidades con una puntuación CVSS de 9 o mayor, y se encuentran en una de las siguientes categorías:
        - Malware-CNC:
        - Blacklist:
        - SQL Injection:
        - Exploit-kit:
    - Seguridad
      - Contiene reglas que son de el año en curso y los tres

años anteriores, están en busca de vulnerabilidades con una puntuación CVSS de 8 o superior, y se encuentran en una de las siguientes categorías:

- Malware-CNC:
- Blacklist:
- SQL Injection:
- Exploit-kit:
- App-detect:

- La solución ofertada deberá de soportar la definición de listas blancas basadas en firmas de SNORT

• Antimalware

La solución UTM ofertada deberá de contar con capacidades para la detección de malware y código maicioso de día Zero, que incluya las siguientes características:

- La solución deberá de soportar la inspección sobre el tráfico HTTP de los siguiente tipos de archivos:

- MS OLE2 (.doc, .xls, .ppt)
- MS Cabinet (Microsoft compression type)
- MS EXE
- ELF (Linux executable)
- Mach-O/Unibin (OSX executable)
- Java (class/bytecode, jar, serialization)
- PDF
- ZIP (regular and spanned)\*
- (standardized test file)
- SWF (shockwave flash 6, 13, and uncompressed)

- La solución deberá de soportar la configuración de las siguientes acciones:

- Clean - The file is known to be good.
- Malicious - The file is known to be harmful.
- Unknown - There is insufficient data to classify the file as clean or malicious.

- La solución deberá permitir la re categorización de las disposiciones en caso de que existan cambios en los archivos, dicha reclasificación generara alertas retrospectivas y notificaciones.

- LA solución deberá de poseer la capacidad de filtrar búsquedas de eventos malicious con los siguientes elementos:

- Red actual
- Detección de malware
- IDS
- Limpio
- Malicioso
- Desconocido
- Bloqueado
- Permitido

- Dichos eventos malicious deberán de poder ser filtrados según los siguientes rangos de tiempo:

- Por las ultimas dos horas
- Por el ultimo día
- Por la ultima semana
- Por el ultimo mes

- La solución deberá permitir la búsqueda de eventos malicious por:

- Identificación de cliente (Hostname)
- URI
- SHA256 file hash
- ID de regla IPS/IDS

- La solución deberá soportar la generación de informes que contengan la siguiente información:

- Los clientes más afectados por Sistema Operativo
- Los principales orígenes de los ataques (Geo Localización)
- Ranking de las principales amenazas

Vision retrospectiva de Malware

- VPN
  - Debe Soportar DES (56-bit), 3DES (168-bit) y AES (128-bit/192-bit/256-bit) encryption/decryption.
  - Debe Soportar MD5, SHA1, y SHA2 authentication.
  - Debe Soportar IPSec VPN con NAT trasversal
  - Debe Soportar una tecnología para establecer un túnel de forma dinámica entre los radios en el modelo de red hub-and-spoke o mesh, como DSVPN.

- Debe tener soporte para selección inteligente de "uplink" en la cual podrá seleccionar una interfaz saliente de manera automática para maximizar la eficiencia de los recursos y mejorar la experiencia de usuario en el acceso a internet. También para el caso en que el vínculo a internet esté caído el servicio permitirá cambiar a otros links lo cual asegure la alta disponibilidad del servicio.
- Debe identificar y clasificar el tráfico de la red según alguna base de firmas de aplicaciones. Luego deberá ordenar el tráfico según su prioridad.
- A través de la función de verificación del estado del vínculo y de la disponibilidad del mismo deberá ajustar el tráfico para asegurar el nivel de servicio de la red.

**Reportes**

- La solución deberá generar sobre demanda, un reporte de seguridad por la última hora, la última semana, el último mes y sobre un período específico de monitoreo
- Se deberá generar una gráfica en el tiempo de los eventos clasificados por su severidad (Alta, Mediana y baja), así como un listado de los eventos de seguridad detectados en el período de tiempo seleccionado
- Se deberá incluir como reporte la lista de usuarios contabilizados sobre la solución de seguridad, por hora, día, semana y mes identificando el nombre del equipo y/o dirección MAC, última fecha y hora en que se detectó al usuario, la utilización de la red en Bytes, sistema operativo del equipo y dirección IP. Este reporte deberá estar disponible para su descarga en formato CSV or PDF or WORD y/o XML.

**2.2.8. RENGLON 7: SWITCHES LAN PARA DEPENDENCIAS**

El PROVEEDOR deberá proveer la cantidad necesaria de Switches LAN, para conectar todos los dispositivos a proveer en todos los establecimientos, y dar redundancia de conexión a los Access point que irradian en mismo aula. Esto es, los Access Points que den señal a un aula en particular deberán estar conectados a switches diferentes en el establecimiento. Los switches deberán cumplir con las siguientes características:

- Capa 2
  - Priorización de tráfico vía Calidad de Servicio 802.1p, con hasta 8 colas de Clase de Servicio (CoS) por puerto
  - Etiquetado de hasta 4094 VLAN's soportando troncales 802.1q
  - Soporte de estándares Spanning Tree y Rapid Spanning Tree 802.1d y 802.1w
  - Soporte de Link Layer Discovery Protocol LLDP 802.1ab
  - Capacidad de agregación de hasta 8 puertos en un enlace lógico vía estándar LACP 802.3ad
  - Capacidad de espejeo de puertos para necesidades de monitoreo continuo de tráfico
  - Puertos 10/100/1000BASE-T Ethernet (RJ45) con soporte de detección crossover y autonegociación de velocidad
  - Soporte de IGMP snooping para filtrado de tráfico multicast
  - Tabla de MAC Forwarding de al menos 16,000 entradas
  - Soporte de PoE 802.3af y PoE+ 802.3at
  - Presupuesto PoE/PoE+ de al menos 740W
  - El equipo deberá soportar asignación de VLAN basado en Puerto, Dirección MAC, IP, subredes.
  - El equipo deberá soportar Guest VLAN o similar.
  - El equipo deberá soportar Jumbo Frames de al menos 9600 bytes
- Virtualización:
  - El equipo deberá soportar ser integrado verticalmente como parte de un nodo virtual administrado conformado por otros switches y Wireless Access point.
- QoS
  - El equipo deberá soportar ingreso y egreso de traffic Shapping y VLAN basado en limitación de Trafico.
  - El equipo deberá soportar por lo menos 400 ACL entries.
  - El equipo deberá soportar flow mirroring
  - El equipo deberá soportar algoritmos de encolado, tales como SP, WRR, DRR, SP + WRR, and SP + DRR

Desempeño

- La capacidad de conmutación del equipo propuesto deberá ser basado en una arquitectura non-blocking, y de al menos 100 Gbps.
- Los equipos deberán contar con una latencia de conmutación de 2.5 microsegundos.

Conectividad

- Los equipos tendrán la opción de conectarse a una fuente de poder redundante externa.
- Hasta 4 1GE SFP uplink ports
- 12, 24 o 48 puertos 10/100/1000Base-T
- IEEE 802.3af y 802.3at
- Outband NMS

- Se requiere contar con soporte de Power over Ethernet + (PoE+) de al menos 25 watts por puerto.
- El equipo deberá soportar stacking o apilado ya sea físico o virtual.

**Administración**

- Los equipos deberán ser administrados centralmente por medio de una plataforma de gestión gráfica basada en web y con una arquitectura fuera de banda
- Los equipos deberán ser capaces de identificar aplicaciones a nivel capa 7, proveyendo reportes detallados del uso de la red a nivel dispositivo individual que esté conectado
- Los equipos deberán incluir mecanismos de clasificación y perfilamiento de los dispositivos que se conecten a ellos, identificando características como fabricante y sistema operativo
- Los equipos deberán soportar el estándar SNMPv1/v2c y v3 para integración con plataformas de gestión de terceros
- Los equipos deberán mantenerse actualizados mediante mecanismos de calendarización de actualizaciones de firmware, haciéndose de forma automática una vez programado
- Los equipos deberá de incluir mecanismos que permitan la configuración de políticas de prendido y apagado de puertos, para ahorro de energía basado en tiempos y calendarios recurrentes.
- Los equipos deberán ser configurados y monitoreados de forma unificada, teniendo la capacidad de aplicar configuraciones a distintos puertos de distintos equipos de forma simultánea.
- La administración, monitoreo y configuración deberá poder hacerse a través de potencialmente miles de equipos, sin importar su ubicación física o topología de cableado físico.
- Los equipos y puertos individuales podrán ser etiquetados administrativamente en la plataforma de gestión, a fin de simplificar la ubicación de los mismos y facilitar la aplicación de configuraciones iguales
- Las etiquetas antes mencionadas podrán tener un esquema jerárquico y/o informativo, por ejemplo, se pueden definir etiquetas: Campus, Edificio 5, Piso 4, IDF 3, Equipo2, Puerto1, VoIP, acceso. Y así ubicar equipos y/o puertos con cualquiera de tales etiquetas o combinación de ellas
- Los equipos deberán soportar el envío de alertas sobre su estatus via email, tales como si el switch está no disponible para la plataforma de gestión por 5 o más minutos, si un puerto se ha deshabilitado por cierto tiempo, o por cambio de velocidad en el puerto o errores en el cable, por decir algunos.
- Se deberá incluir un mecanismo que provea un diagnóstico del estado del cableado en cualquiera de los puertos que usen cobre, que ayude a determinar la longitud del mismo y posibles fallas en cualquiera de sus 4 pares trenzados
- Se podrá hacer lo anterior con un rango de puertos de forma simultánea

**Seguridad**

- El equipo deberá soportar ACL bidireccionales
- El equipo deberá soportar ACL basado en puerto y VLAN.
- El equipo deberá soportar DAI (Dynamic ARP Inspection)
- El equipo deberá soportar DHCP Snooping
- El equipo deberá soportar control de acceso basado en puerto de acuerdo a estándar IEEE 802.1x
- El equipo propuesto deberá tener la capacidad de evitar que BPDUs del protocolo spanning tree puedan ingresar por un puerto que está identificado como puerto de acceso. Cuando el equipo propuesto detecte que existe un intento de introducir un BPDU por un puerto de acceso, el puerto de acceso deberá inhabilitarse temporalmente
- El equipo propuesto deberá tener la capacidad de evitar que BPDUs del protocolo spanning tree, en una métrica superior, puedan ingresar por un puerto en estado "designado" y de tal forma modificar la topología indeseadamente. Cuando el equipo propuesto detecte que esto suceda, el puerto deberá inhabilitarse hasta que tales eventos cesen
- Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches
- El equipo propuesto deberá ser capaz mediante 802.1x de asignar la VLAN a la cual pertenece puerto del switch en donde se conecta el cliente en base a las credenciales que el usuario presenta ante la infraestructura de red
- Bypass de autenticación basada en dirección MAC

**2.2.9. RENGLON 8: EQUIPOS DE CÓMPUTO PARA DEPENDENCIAS**

El PROVEEDOR deberá proveer, configurar y poner en funcionamiento 300 (TRESCIENTOS) almacenamientos que cumplan con lo detallado a continuación:  
Se deberá proveer al menos 1 soporte para sitio para ser montado en Rack con las siguientes especificaciones mínimas:

- Al menos 1 (uno) procesadores de 6 núcleos (Seix core), L3 cache  $\geq$  15 MB, arquitectura x64 (x86 con extensiones de 64bits) siendo: Performance de referencia procesador Intel E5-2600 v4 o superior.
- 16 GB de memoria
- 2\*240G SSD Disk, SSD is the same brand as servers
- 2\*2000G SATA 7.2K rpm
- RAID Cards, RAID 0, 1, 10
- Deberá contar con 4 puertos Gigabit Ethernet base-T para conexión a los switches del establecimiento.
- Deberá contar con un puerto adicional RJ45 (10/100/1000) base T, para gestión fuera de banda (OOB Management)
- Deberá ocupar como máximo 1 unidad de rack (1 RU)
- Soporte de fuente de Alimentación redundante (AC)
- Long-term operating temperature: 5°C to 45°C (41°F to 113°F)
- O en su defecto un almacenamiento cache para guardar datos conservados temporalmente en previsión de ser utilizados nuevamente y ahorrar con ello el tiempo de cálculo, búsqueda o descarga de internet.

### 2.2.10. RENGLON 9: EQUIPOS DE VIDEO CONFERENCIA PARA SALAS EN DEPENDENCIAS

El PROVEEDOR deberá proveer 300 (TRESCIENTOS) equipos de videoconferencia Full HD para Salas de reunión con las siguientes características:

- Deberá soportar SIP y H.323
- Códec físico en hardware (no basado en PC) que convierta cada pantalla plana (LCD o LED) en un flexible sistema de videoconferencia Full HD vía un conector HDMI
- Cámara Full HD 1080p con zoom de 5x o superior
- Micrófono
- Control Remoto
- Tv led 42" con entrada HDMI
- Enviar video en HD hasta 720p30 como mínimo, y tener la capacidad de upgrade vía software para enviar video a 1080p
- Compartir documentos hasta 720p15 como mínimo.
- Compartir documentos desde PC a través de WIFI
- Contar con una entrada de video analógica con la finalidad de compartir el contenido de una PC mediante su salida de monitor VGA.

C.C. 216.793

## Sociedades

### JARBO S.A.

POR 1 DÍA - Acta de Directorio N° 07 del 12/03/2016 y Acta de Asamblea N° 06 del 06/09/2016, cambio de sede social a Avenida Doctor Ricardo Balbín 5860, localidad y partido de Merlo, Provincia de Buenos Aires. "Artículo Segundo: Que a los efectos de lo dispuesto por el artículo 11, inciso segundo de la Ley 19.550 (t.o. 1984), fijan el domicilio se su sede social, domicilio legal y fiscal, en la Av. Doctor Ricardo Balbín 5860, de la localidad y partido de Merlo, Provincia de Buenos Aires." Presidente: Lucas Rene Fernández, DNI 26.062.825, CUIT 23-26062825-9, domiciliado en la calle Mario Bravo 645 de la localidad y partido de Merlo, Provincia de Buenos Aires; Director Suplente: Andrea Soledad Navarro, DNI 32.618.241, CUIT 27-32618241-4, domiciliada en la calle Mario Bravo 645 de la localidad y partido de Merlo, provincia de Buenos Aires; por el término de 3 ejercicios, representación Presidente. Contador Público, Luis O. Sánchez autorizado.

S.I. 42.846

### PETROISLAND S.A.

POR 1 DÍA - 1) Cristian Eduardo Elia, argentino, 10/02/1972, D.N.I. 22.352.567, C.U.I.T. 23-22352567-9, casado, comerciante, domiciliado en la calle Laprida 567 de la localidad y partido de San Isidro, Provincia de Buenos Aires y María Eugenia Sánchez Ortíz, argentina, 28/04/1973, D.N.I. 23.251.272, C.U.I.T. 27-23251272-0, casada, comerciante, domiciliado en la calle Laprida 567 de la localidad y partido de San Isidro, Provincia de Buenos Aires. 2) 3 de noviembre de 2016. 3) "Petroisland S.A." 4) Avenida Andrés Rolón 1076 la Localidad y Partido de San Isidro, Provincia de Buenos Aires. 5) Objeto Social: a) Explotación, en cualquier punto del país, de estaciones de servicios para automotores, servicio de mecánica ligera, gomería, polirubro y la venta de toda clase de combustibles líquidos y gaseosos, lubricantes, repuestos y accesorios para los mismos. b) Inmobiliarias: Compra, venta permuta, alquiler, arrendamiento y en general todo tipo de operaciones comerciales sobre inmuebles, incluso la intermediación en la realización de estas actividades. c) Industrial: Industrialización, comercialización, fabricación, provisión, compra, venta, importación, exportación, distribución, consignación, comisión y representación al por mayor y menor de materiales e insumos para la industria de la construcción. d) Construcción de edificios, estructuras metálicas o de hormigón, obras civiles y todo tipo de obras de ingeniería y arquitectura de carácter público o privado. e) Agropecuaria: Compra, venta, consignación, acopio, distribución, fraccionamiento, transporte de cereales, granos, semillas, frutas y cítricos y todos sus derivados. La explotación en todas sus formas de establecimientos agrícolas, ganaderos, avícolas, apícolas, hortalizas y de granjas, la agricultura en todas sus etapas desde la siembra hasta la cosecha. f) Comercial: Compra, venta, permuta, distribución, intermediación, consignación, transporte, importación y exportación de los productos, mate-

rias primas, industrializadas o no, vinculados con las actividades enunciadas en el presente objeto social. 6) 99 años desde inscripción registral. 7) \$ 100.000. 8) Directorio compuesto del número de miembros que fije la Asamblea Ordinaria, entre un mínimo de uno y un máximo de seis Directores Titulares e igual o menor número de Directores Suplentes. La sociedad prescinde de la sindicatura, la fiscalización de la misma será ejercida por los accionistas conforme a lo prescripto por los Arts. 55 y 284 de la LSC 19.550. Presidente: Cristian Eduardo Elia; Director Suplente: María Eugenia Sánchez Ortíz. Duración de sus funciones tres ejercicios. 9) Representación legal a cargo del presidente. 10) 30 de junio de cada año. Dr. Luis Oscar Sánchez, Contador Público.

S.I. 42.847

### CIVIAL S.A.

POR 1 DÍA - Modificaciones estatutarias y constitutivas 1) Instr. Privado Acta Asamblea Extraordinaria del 17/10/2016. 2) sede social: Hipólito Yrigoyen 148 Zárate, Part. Zárate, Bs. As. 3) Duración: 99 años a partir inscripción de la presente. 4) Capital: \$ 4.900.000 representados por 4900 acc. nominativas, no endosables, de 5 votos por acción. 5) Accionistas: José Luján López, CUIT 20-08189115-0, arg., casado, DNI 8.189.115, Ing. Civil, domiciliado en presidente; Ángel María Rocchia, CUIT 20-06445612-2, arg., casado, DNI 6.445.612, Ing. Civil, domiciliado en Rivadavia 1619, Zárate, Part. Zárate, Bs. As., designado Director Suplente. 6) Objeto: a) Constructoras: Mediante la construcción de edificios, inmuebles urbanos y rurales, obras viales de todo tipo, desagües, gasoductos, diques y todo tipo de obras de Ingeniería Civil, Ingeniería Eléctrica, Ingeniería Mecánica o Arquitectura de carácter público o privado. b) Comerciales: Mediante la comercialización por compraventa, representación, alquiler, "Leasing" o distribución de maquinarias y elementos destinados a la industria de la construcción y minería y compraventa, representación y distribución de materiales de utilización en la industria de la construcción y minera. Y también mediante la compra, venta, permuta, consignación, alquiler, "leasing", distribución, producción, importación, explotación de materiales, máquinas, equipos, accesorios e implementos relacionados con la industria de la construcción y minera y los derivados de la misma. c) Minera: Mediante la adquisición y explotación de minas de cualquier categoría y canteras de suelos seleccionados, piedra y todo tipo de minerales, de venta de sus productos y la elaboración de los mismos, pudiendo a ese fin adquirir o enajenar minas y todo derecho minero, dentro o fuera del país; hacer manifestación de hallazgos y/o descubrimientos de minerales, solicitar cateos, socavaciones y restauraciones, minas vacantes, servidumbres y cualquier otro derecho de los establecidos en el Código de Minería. d) Financieras: Mediante la realización de operaciones financieras por aporte de capitales propios, a personas, sociedades por acciones, existentes o a crearse, para negocios realizados o a realizarse bajo las condiciones que se estime conveniente con o sin garantía real o personal. La Sociedad Anónima mencionada no desarrollar actividades comprendidas en la Ley de Entidades Financieras, u otras por lo que se requiera el concurso del ahorro público. e) Inmobiliaria: mediante la adquisición, venta, loca-

ción, sublocación, y/o permuta de todo tipo de bienes inmuebles urbanos y rurales, la compraventa de terrenos y su subdivisión, fraccionamiento de tierras, urbanizaciones con fines de explotación, renta o enajenación, inclusive por el régimen de Propiedad Horizontal. 7) Administración directorio de 1 a 5 miembros por 3 años titulares, e igual o menor número de suplentes. 8) Se prescinde de sindicatura, fiscalización a cargo accionistas. 9) representación legal Presidente, o vicepresidente en su caso. 10) Cierre Ejercicio: 31/8 Dr. Jesús Adriano Camejo, Contador Público Nacional, Autoriz. Acta Asamblea del 17/10/2016.

Z-C. 83.839

### ABREGO Y GONCALVES S.A.

POR 1 DÍA - Matrícula 20.970 Dirección Personas Jurídicas Prov. Buenos Aires. Cambio de razón social o denominación social. Art. 10 inc. b) Ley 19.550. Por Acta Asamblea Extraordinaria N° 35 de fecha 27/07/2016 se decidió unánimemente cambiar la denominación Social por "Orlando Goncalves S.A.", reformándose artículo primero del Estatuto Social. Fdo.: Orlando J. Goncalves Ferreira, Presidente.

Z-C. 83.846

### DROGUERÍA LUMA S.A.

POR 1 DÍA - Exp. 21.209 Leg. 10/71611. Por Asamblea del 22/09/2016, se decide por unanimidad la reelección del Directorio actual, quedando conformado de la siguiente manera: Presidente: Marcelo Foglia, argentino, 09/12/1954, DNI 11.134.448 ingeniero, casado, con domicilio real y especial en Av. Mitre 686, 5°, 57, Loc. y Part. Avellaneda, Prov. de Bs. As. Vicepresidente: Oscar Rocco, argentino, nacido el 13/08/1952, DNI 10.210.719, empresario, divorciado, con domicilio real y especial en B° Luján del Sol Ruta N° 7 Km. 73 L38/93, Loc. y Part. Luján Prov. Bs. As. Director: Sergio Javier Lamelza, argentino, 15/05/1970, DNI 21.534.708, empresario, casado con domicilio real y especial: A. Williams 1735, Loc. y Part. Hurlingham, Prov. de Bs. As.; Director Suplente: Karina Susana Suárez, argentina, 18/01/1973, DNI 23.217.129, licenciada, soltera, con domicilio real y especial: Boulevard San Martín 2740, Loc. El Palomar, Part. 3 de Febrero, Prov. de Bs. As. José Luis Marinelli, Abogado.

C.F. 32.333

### GRUPO ITTEL S.R.L.

POR 1 DÍA - Se comunica que el 25/10/2016, por reunión de socios unánime Grupo Ittel S.R.L., ha resuelto reformar el Artículo Cuarto del contrato social el que queda redactado de la siguiente manera: "Artículo Cuarto: Objeto: La sociedad tendrá por objeto dedicarse por cuenta propia, de terceros o asociada a terceros, en el país o en el extranjero, a las actividades que a continuación se detallan: I) Desarrollo, mantenimiento, configuración, diseño, administración, compraventa, alquiler, comercialización, fabricación, instalación, concesión, control y gestión de redes informáticas, telecomunicacio-

nes, estructuras portantes, software, equipamiento e infraestructura de red de telecomunicaciones, de energías convencionales y renovables. II) Diseño, control, y ejecución de obras civiles, tendidos de redes de telecomunicaciones tanto alámbricas como móviles, y a la realización de todo tipo de obras de ingeniería, y cableado tanto en interiores y exteriores; III) Controles y estudios electrónicos, ambientales, de suelo y estructurales. IV) Prestación de todo tipo de servicios de consultoría, capacitación y asesoramiento en todo lo referente a los rubros precedentemente mencionados, especialmente servicios profesionales en tecnología y telecomunicaciones. La sociedad podrá realizar la financiación de las operaciones sociales obrando como acreedor prestatario y realizar todas las operaciones necesarias de carácter financiero permitidas en la legislación vigente, siempre con dinero propio. No realizará las comprendidas en la Ley de Entidades Financieras o cualquier otra que se dicte en lo sucesivo en su reemplazo requiera de la intermediación del ahorro público. La sociedad directa o indirectamente podrá realizar otras actividades conexas o afines con su objeto social sin más limitaciones que las establecidas en la ley general de sociedades y este estatuto. Asimismo las actividades que así lo requieran serán realizadas por profesionales debidamente capacitados y con título habilitante a tales efectos. A tales fines tiene plena capacidad jurídica para adquirir derechos, contraer obligaciones y ejercer todos los actos que no sean prohibidos por las leyes o por este contrato." Fernando Gastón Poblet, Socio Gerente.

C.F. 32.335

### PROYECTOS PATAGÓNICOS S.R.L.

POR 1 DÍA - Por Reunión de socios unánime y escritura 139 pasada al folio 302 del Registro 2045 CABA a cargo de la Escribana Juliana Marina Venturelli, ambas de fecha 25 de agosto de 2016, el socio Christian Gustavo Ariel Cándido cedió sus 500 cuotas sociales a Aldo Beitia. Se aceptó la renuncia del socio Gerente Christian Gustavo Ariel Cándido y procedieron a Renovar el nombramiento de Socio Gerente Fernando Estanislao Zarate y también al nombramiento del nuevo Socio Gerente señor Aldo Beitia, DNI 18.826.494. Los Gerentes constituyen domicilio especial en la sede social sita en la calle José Ignacio Gorriti 1121, Francisco Álvarez, Partido de General Rodríguez, Provincia de Buenos Aires. Juliana Marina Venturelli, Escribana.

C.F. 32.337

### BEDERMAN & CÍA. S.A.

POR 1 DÍA - 1) Abel Jorge Roldán, DNI 17.998.256, 22/06/1966, contratista, soltero, calle Juncal 2676, localidad y partido de San Fernando, Prov. Bs. As.; Gerónimo Roldán, DNI 5.302.779, 24/09/1934, comerciante, casado, calle Juncal 2676, localidad y partido de San Fernando, Prov. Bs. As.; Mirtha Nélica Bamann, DNI 20.241.817, 10/03/1968, comerciante, divorciada, calle Crisólogo Larralde 1677 de la localidad y partido de Tigre, Prov. Bs. As. Todos argentinos. 2) 04/11/2016. 4) Juncal 2676, localidad de San Fernando, Partido de San Fernando, Provincia de Buenos Aires. 5) Objeto: Constructora: Estudio, proyecto, dirección y ejecución de obras de ingeniería y arquitectura. Construcción de edificios, estructuras metálicas o de hormigón, obras civiles y todo tipo de obras de ingeniería y arquitectura de carácter público o privado. Realizar refacciones, mejoras, remodelaciones, instalaciones eléctricas, mecánicas y electromecánicas, y en general, todo tipo de reparación de edificios, casas, galpones y locales comerciales. Decoración, empapelado, lustrado, pintura y equipamiento de todo tipo de inmuebles. B) Inmobiliaria: Compra, venta, permuta, explotación, alquiler, arrendamiento, organización, colonización, subdivisión, remodelación, loteo, parcelamiento, administración, explotación, operaciones de "leasing", fideicomiso u otro modo de adquirir el dominio perfecto o imperfecto, usufructo o cualquier otro derecho real o personal, actual o que se incorpore a la legislación en el futuro, e incluso los que resultan de las leyes de Propiedad Horizontal y Prehorizontalidad, sobre bienes inmuebles propios o ajenos, urbanos, suburbanos, semiurbanos o rurales y el fraccionamiento, urbanización y/o loteo de bienes inmuebles. 6) 99 años. 7) \$ 100.000. 8) 1 a 5 directores titulares por un plazo de 3

ejercicios. Se designó Presidente: Gerónimo Roldán; Vicepresidente: Mirtha Nélica Bamann; Director suplente: Abel Jorge Roldán. 9) Presidente o vicepresidente en su caso. Fisc.: Art. 55. 10) 28/02. Martín A. Fandiño, Abogado.

C.F. 32.342

### CORDOVA GROUP INC S.R.L.

POR 1 DÍA - 1) Luis Miguel Rafael Godoy Ormezzano (Gerente), DNI 94.754.511, 24/10/1972, Ingeniero mecánico; Daniela Pardo Cárdenas, DNI 94.743.816, 21/08/1981, Ingeniera en producción. Ambos Venezolanos, casados, Domiciliados en Av. Bartolomé Mitre 710 Unidad Funcional 14 del Barrio cerrado "La Cuesta" de la localidad de Manzanares, Partido de Pilar, Prov. Bs. As. 2) 26/10/2016. 4) Av. Bartolomé Mitre 710 Unidad Funcional 14 del Barrio cerrado "La Cuesta" de la localidad de Manzanares, Partido de Pilar, Prov. Bs. As. 5) Objeto: Prestación de todo tipo de servicios relacionados con la industria petrolera, gammagrafía industrial, realización de equipos mediante el uso de instrumentos con fuentes radiactivas. Importación, exportación y comercialización de fuentes radiactivas selladas, abiertas y de todo tipo de productos relacionados con la industria del petróleo y sus derivados y similares. 6) 99 años 7) \$ 30.000 8) Gerentes plazo: indeterminado, domicilio especial: la sede. 9) Representación individual e indistinta. Fisc. Art. 55 Ley 19.550. 10) 30/09. Martín A. Fandiño, Abogado.

C.F. 32.343

### SEMBAUER S.A.

POR 1 DÍA - Por acta de Asamblea Extraordinaria del 12/10/16 se fija en el Art. 4 que cada acción otorga derecho a 1 voto, Jorge Alejo Pandini, Notario.

L.Z. 50.000

### LOS CASPRES S.A.

POR 1 DÍA - Por acta de Asamblea Extraordinaria del 3/11/16 se reforma el Art. 1 del estatuto, cambiando la denominación social a "Hüls Gesellschaft S.A.". Contador Público, Juan Carlos Vacarezza.

L.Z. 50.007

### LAS NUEVAS MARGARITAS S.R.L.

POR 1 DÍA - Se comunica a todo efecto legal que la Srita. Vivas Sonia Debora, DNI 34.818.659, argentina, comerciante, soltera, nacida el 7/03/1989, cede, vende y transfiere: la cantidad de 15.000 cuotas sociales de \$ 1 valor nominal cada una a la Srita. Vivas Alba Agustina Abril, DNI 40.913.692, argentina, comerciante, soltera, nacida el 4/10/1997. En el cargo de Gerente queda designado el Sr. Vivas Ángel Julián. Dr. José Luis Andrada, Contador Público.

L.Z. 50.020

### DESARROLLO SANTA MÓNICA S.R.L.

POR 1 DÍA - Acta Reunión de Socios 30/07/13 Artículo 4º: El capital social se fija en la suma de tres millones setecientos sesenta y cinco mil setecientos sesenta y dos pesos (\$ 3.765.762), dividido en 3.765.762 cuotas de Un Peso, valor nominal cada una, con derecho a un voto por cuota, totalmente suscriptas por cada uno de los socios. Contadora Pública, Claudia Silvina Fernández.

L.Z. 50.022

### COLEGIO LINCOLN DE ÁREA 60 Sociedad de Responsabilidad Limitada

POR 1 DÍA - 1) Stella Maris Palacio, arg., DNI 13.577.500, nació 20/03/1957, empresaria, CUIT 27-13577500-8, soltera, hija de Atilio Ali Palacio y Ángela María Scarpato con domicilio en Florida N° 1394, localidad y pdo. de Lanús, Prov. de Bs. As., y Susana Patricia Cataldi, arg., DNI 13.942.569, nació 18/05/1959, empre-

saria, CUIT 27-13942569-9, soltera hija de Juan Carlos Cataldi y Elsa Montero, con domicilio en Cura Brochero N° 3369, localidad de Tortuguitas, pdo. de Malvinas Argentinas, Prov. de Bs. As.; 2) Inst. Privado del 02/11/2016; 3) Den.: Colegio Lincoln de Área 60 Sociedad de Responsabilidad Limitada; 4) Dom. Social: Alberdi N° 386, localidad y pdo. de Quilmes, Prov. Bs. As.; 5) Objeto: Dedicarse por cuenta propia o de terceros o asociada a terceros a la dirección y administración de un Instituto Educativo de Enseñanza Programática y Extraprogramática de Jardín Maternal, Jardín de Infantes, nivel inicial, primaria o educación general básica, E.G.B., polimodal y/o medio especial y lo tercería, basándose en las leyes y reglamentos vigentes en el ámbito de la República Argentina, pudiendo instalar y administrar, una o más sedes educativas; 6) Duración: 99 años desde insc.; 7) Capital Social: \$ 400.000; 8) Adm. rep. legal y uso firma social Gerentes, sean socios o no; 9) Cierre de ejercicio: 30 de diciembre de cada año. La sociedad prescinde de fiscalización, la cual será realizada por los socios. Dra. Julia Pereira Díaz, Abogada Autorizada.

L.Z. 50.027

### COOPASOS Sociedad de Responsabilidad Limitada

POR 1 DÍA - Edicto complementario. Conforme Art. 10 Inc. a) de la Ley 19.550. Diego Gerardo Cuartas y Juan Francisco Barreto, por escritura pasada ante la escribana Laura Faroppa con fecha 8/11/16; establecen que los artículos 3 y 14 del contrato social, quedarán redactados de la siguiente manera: "Artículo 3º. Tendrá por objeto el desarrollo por cuenta propia o de terceros, todo lo relacionado con: A) La actividad gráfica y de imprenta; compra, venta, industrialización, exportación e importación de maquinaria; el desarrollo y la comercialización de todo tipo de material gráfico y papel, procesado de impresión, litografía de formularios, diarios, revistas y publicaciones; fabricación de cuadernos, encuadernación. Fabricación, importación, exportación y distribución de insumos gráficos, materias primas, productos electrónicos, electromecánicos y de bienes muebles en general relacionados con la industria. Explotación en todas sus formas de artículos de librería, papelería, fabricación de sellos de goma, fotocopias y todas actividades vinculadas, de exportación e importación, compra y venta de artículos afines. Realización de toda actividad conexas o vinculada a las artes gráficas, diseño y diseño publicitario. Para su cumplimiento la sociedad tendrá plena capacidad jurídica para realizar todo tipo de actos y operaciones relacionadas con su objeto, pudiendo celebrar a tales fines contratos de compra, venta, edición, concesión, leasing, locación, otorgando las franquicias que resulten menester. B) Publicidad: la realización por cuenta propia, de terceros o asociada a terceros, en el país o en el exterior, de las siguientes operaciones: creación, planeamiento, producción, difusión y administración de campañas de publicidad, propaganda, promoción, relaciones públicas y otras vinculadas con las mismas, efectuando contrataciones en revistas, periódicos, folletos, radio, televisión, cine, vía pública y/o cualquier otro medio de difusión. Actuar como agencia de publicidad, en forma integral y en todos sus aspectos y modalidades. Realizar trabajos de gestión de marcas en internet y redes sociales. La explotación de espacios publicitarios públicos y privados. La prestación de servicios y asesoramiento empresario, artístico, comercial, industrial, y de publicidad. Realizar la comercialización mediante la compraventa, consignación, representación de programas y/o espacios publicitarios de cualquier medio de difusión, así como de redes de computación relacionadas con la publicidad. C) Desarrollo de la Actividad Inmobiliaria y Financiera: Compra, venta, permuta, arrendamiento, explotación y administración de todo tipo inmuebles urbano o rurales; la sistematización, subdivisión y urbanización de tierras, e inmuebles edificados o a edificarse, como así mismo todas las operaciones comprendidas en la leyes y reglamentos de Propiedad Horizontal y Prehorizontalidad; afectar sus propiedades a sistemas de Fideicomiso, actuar como fiduciante, fiduciario, fideicomisario o beneficiario. Préstamos y/o aportes e inversiones de capitales a otras sociedades por acciones, realizar financiaciones y operaciones de crédito en general con cualquiera de las garantías previstas en la legislación vigente o sin ellas o realizar operaciones financieras en general. D) Contratar y ser proveedora del Estado Nacional, Provincial y

Municipal; pudiendo asociarse con terceros, tomar representaciones y comisiones, tanto en el país como en el extranjero. La sociedad tendrá plena capacidad para adquirir derechos, contraer obligaciones y ejercer todos los actos que no sean prohibidos por las leyes o por el presente contrato. La sociedad no tendrá por objeto la realización de actividades comprendidas en la Ley de Entidades Financieras." "Artículo 14: La fiscalización de la sociedad se llevará a cabo conforme lo normado por el artículo 55 de la Ley 19.550." Esteban Casas, Abogado.  
L.P. 29.608

### DUAL SHOES & ACCESSORIES S.R.L.

POR 1 DÍA - Constitución: 1) Instrumento Privado del 08/11/2016. 2) Domicilio: Las Heras; N° 40, Bragado, Bs. As. 3) Duración 90 años desde su inscripción. 4) Socios: Azanza, Marisa, argentina, profesora en Cs. de la educación, casada en 1ras. nupcias con Pablo José Etchecopar, DNI 26.222.297, CUIT 27-26222297-2, nacida el 01/03/1978, domiciliada en calle Las Heras N° 40, de la localidad de Bragado, Bs. As.; y Etchecopar, Marcos Darío, argentino, empleado, soltero, nacido el día 16/11/1989, DNI 34.668.728, CUIT 20-34668728-3, domiciliado en calle Alfonsina Storni N° 140, Mechita, Pdo. de Bragado, Bs. As. 5) Tiene por objeto la realización por sí, por terceros o asociadas, a terceros, en el país o en el extranjero la siguiente actividad principal: 1) Comercial: comprar y vender por mayor y menor, importar, exportar, distribuir, transportar, almacenar y en general comercializar de cualquier otra manera toda clase de calzados para damas, caballeros y niños incluyendo calzados deportivos y ortopédicos, artículos de marroquinería y talabartera, artículos textiles incluyendo remeras, camisas y pantalones y todo otro artículo para vestir, artículos de bijouterie y perfumes y de manera secundaria; 2) Inmobiliaria: Mediante la compra, venta, permuta, explotación, arrendamiento, administración y construcción de inmuebles urbanos, y rurales, loteos y fraccionamientos, incluso todas las operaciones comprendidas en las leyes y reglamentos sobre la Propiedad Horizontal, y la realización de toda clase de estudios, proyectos, construcciones civiles, industriales, públicas o privadas; 3) Financiera: Por medio de inversiones o aportes de capital a personas físicas y/o jurídicas por acciones, constituidas o a constituirse, sean nacionales, o no, para operaciones realizadas o a realizarse o en curso de realización, préstamos a interés y financiaciones en general y toda la clase de créditos, garantizados por cualquiera de los medios previstos en la legalización vigente; sin garantías. Se excluyen expresamente las operaciones comprendidas en el título segundo de la Ley 21.526 de entidades financieras, y toda otra que requiera el concurso público. En todos los casos estos actos serán realizados con dinero de la sociedad. Para el cumplimiento de su objeto la sociedad tiene plena capacidad jurídica para adquirir derechos y contraer obligaciones inclusive las prescritas por el artículo 1881 y concordantes del código civil y artículo 5 del libro II, título X del código de comercio; 4) Transporte: El transporte nacional o internacional de toda clase de bienes muebles, mercaderías, materias primas, semovientes, por cuenta propia o ajena, de terceros; en participación con terceros; 6) Capital: \$ 60.000, dividido en 600 cuotas sociales de \$ 100 c/u. 7) Socio Gerente y representante legal: Etchecopar, Marco Darío. 8) Duración mandato: duración de la sociedad 9) Resoluciones: se toman por mayoría que represente más de la mitad del capital. 10) Fiscalización, a cargo de los socios no gerentes. 11) Cierre del ejercicio: 30 de junio de cada año. Contador Público, Pablo José Etchecopar.  
L.P. 29.610

### NAFIL OESTE S.A.

POR 1 DÍA - Por Inst. Púb. 17/10/16. Dom.: Colectora Gaona Sur 5602, Moreno, Bs. As. Acc.: Oviedo Sergio Omar, arg., solt., DNI 14.855.514, nac. 18/11/61, comerc., dom. Almafuerde 3901, dto. 829 S: 2, Country Club Banco Provincia, Fco. Álvarez, Moreno, Bs. As., Morrone Pablo Fabián, arg., solt., DNI 36.697.888, nac. 14/04/92, inversionista, dom. Maipú 1341, Barrio Privado El Casco, Moreno, Bs. As., Morrone Julián Ariel, arg., solt., DNI 38.855.563, nac. 17/02/95, inversionista, dom. Maipú 1341, Barrio Privado El Casco, Moreno, Bs. As.

Obj.: las sig. activ.: 1) Comercial: Comercializ., repres., consign. de automát., camiones, acoplados, motos, tractores, maquinarias e implem. agrícolas y rodados de todo tipo, de fabric. nac. o extran., repuestos, instrum., herram., combust., lubricantes, neumáticos y acces. p/automot. 2) Industrial: Expl. de talleres de reparac. y serv. de autom., camiones, motos, acoplados, tractores y rodados. 3) Inmobiliaria: Compra y venta de bienes inmuebles, urbanos o rurales, incluyendo los compren. en L. Prop. Horiz. y clubes de campo, pudiendo efec. subdiv., urbaniz. y saneam., diseños de parques y jardines y realizar s/predios, propios o no, mejoras o construc. p/localización o enajen. Admin. de prop. inmuebles, propios o de 3ros. Cap.: \$ 2.200.000. Adm.: Direct. e/1 y 5 Dir. Tit. e igual o menor N° de Supl. Durac. 3 ejerc., uso firma y rep. leg. pte. o Vicep. caso de vacanc., imped. o aus. Pte.: Oviedo Sergio Omar, Vicepr. Morrone Pablo Fabián Dir. Sup. Morrone Julián Ariel. Repres. legal: corresp. al presid. Fiscal. acc. s/ art. 55 y 284. Cierre ej. 31/12. Starico Laura G., Contadora Pública.  
Mn. 64.265

### TEXTIL FARINA HNOS. S.A.

POR 1 DÍA - Const. S.A. Inst. Púb. 21/10/16. Dom.: Malarredo 398, Villa Tesei, Hurlingham, Bs. As. Acc.: Farina Adriana Soledad, arg., soltera, nac. 02/04/85, comerciante, DNI 31.765.010, domic. Malarredo 398, Villa Tesei, Hurlingham, Bs. As.; Farina Eliana Sabrina, arg., soltera, nac. 24/05/79, licenc. trabajo social, DNI 27.162.143, domic. Del Socorro 19, Villa Tesei, Hurlingham, Bs. As.; Farina Loana Débora, arg., soltera, nac. 26/02/90, comerciante, DNI 35.121.021, domic. Don Cristóbal 3626, Villa Tesei, Hurlingham, Bs. As.; Huanca Ester Verónica, arg., soltera, nac. 25/05/86, comerciante, DNI 32.466.452, domic. Segundo Sombra 2302, Villa Udaondo, Ituzaingó, Bs. As.; Farina Diego Víctor, arg., soltero, nac. 07/08/75, cortador, DNI 24.836.179, domic. Segundo Sombra 2202, Parque Leloir, Ituzaingó, Bs. As.; Farina Alan Emiliano, arg., casado, nac. 10/01/92, comerciante, DNI 36.902.582, domic. Segundo Sombra 2202, Parque Leloir, Ituzaingó, Bs. As.; Durac. 99 años Obj.: p/cta. prop. o de 3° o asoc. a 3°, dentro o fuera de Arg. a- Industr. y comercializ.: fabric. y de ropas, lencería, ropa interior, trajes de baños, remeras, camisetas, prendas de indument., de vestir, unifor. escolares, acces., fibras, tejidos, hilados, ropas de bebés y niños, buzos y camperas, camisas, remeras, medias; tejidos, art. de punto, sus acces. y deriv., bijouterie, pasaman.; industrializ. toda clase de materias primas, nac. o extranj.; de todo género de seda, nailon y sus deriv., algodones; fabricac. de hebillas, botones y equiv.; fabric. de hilados y tejidos establec. y explot. fábricas de hilados, de tejidos, de tintorería, de estamp. y apresto de géneros y sus afines, ya sea adq. las exist. o creándolas nuevas. b- Repres. y mandato: Mediante la realiz. en el país y/o en el ext. de toda clase de mandatos, c/s represen., inclusive de carácter fiduciario, en las condiciones perm. p/ leyes y reglament. vig., efectuando operac. de represent., comis., consignac., administ., gestión y promoción de negocios e invers. de cualq. naturaleza. Cap.: \$ 400.000. Adm: Direct. e/ 1y 5 Dir. Tit. e igual o menor N° de Supl. Durac. 3 ejerc., uso firma y rep. leg. pte. o Vicep. caso de vacanc., imped. o aus. Pte.: Farina Adriana Soledad Dir. Sup. Farina Eliana Sabrina. legal: resp. al presid. Fiscal. acc. s/ art. 55 y 284. Cierre ej. 30/09. Claudia V. Belascuain, Contadora Pública.  
Mn. 64.266

### INDUMENTARIA SEGURA S.R.L.

POR 1 DÍA - Por Acta de reunión de socios se decide cambio de sede social a Estanislao del Campo N° 1466, Dto. 4, localidad de Villa Sarmiento, Partido de Morón, Provincia de Buenos Aires. Martín Horacio Pardo, Contador Público.  
Mn. 64.267

### ANDORA MED S.R.L.

POR 1 DÍA - Por Acta de Socios del 20/05/2016 se acepta el cambio de sede social de la calle Av. Gral. Paz 660 de la localidad de Ciudadela, Pdo. Tres de Febrero,

Prov. Bs. As. al de la calle Elías Bedoya 3796 de la localidad de Remedios de Escalada, Pdo. Lanús, Prov. Bs. As. Evangelina Paola Guerrero, Contadora Pública.  
Mn. 64.291

### ANDORA MED S.R.L.

POR 1 DÍA - Por Acta de Socios del 01/09/2016 se decide ampliar el objeto social y en consecuencia reformar el Art. 4° del estatuto social, quedando redactado de la siguiente manera: La sociedad tendrá por objeto dedicarse por cuenta propia o de terceros o asociada a terceros, tanto en el país como en el extranjero al servicio de ambulancia, de atención y traslado de pacientes (servicio médico extra hospitalario) y centro de atención hospitalario de diagnósticos y prácticas ambulatorias clínico-quirúrgicas de baja y mediana complejidad (hospital de día). La sociedad contratará el servicio de profesionales con título habilitante para todas las actividades que así lo requieran. Para el ejercicio de sus actividades la sociedad tiene plena capacidad para adquirir derechos, contraer obligaciones, celebrar toda clase de contratos, adquirir y disponer toda clase de bienes inclusive registrables y operar con instituciones bancarias. Evangelina Paola Guerrero, Contadora Pública Nacional.  
Mn. 64.292

### REPUESTERA ESCOBAR S.R.L.

POR 1 DÍA - Por Instrumento privado se constituyó la Sociedad de Responsabilidad Limitada Repuestera Escobar S.R.L. siendo sus socios Héctor Ariel Burruchaga, D.N.I N° 29.396.646, de nacionalidad argentina, de estado civil soltero, de profesión empleado con domicilio Avenida Presidente Juan Domingo Perón 5730 de la localidad de Benavidez del Partido de Tigre de la Provincia de Buenos Aires, Dallana Brosso González de nacionalidad uruguaya D.N.I. N° 93.788.304, de estado civil soltera de profesión empleada con domicilio Avenida Presidente Juan Domingo Perón 5730 de la localidad de Benavidez del Partido de Tigre de la Provincia de Buenos Aires. Por Instrumento Privado se constituyó el 14 de septiembre de 2016. La Sociedad de Responsabilidad Limitada Repuestera Escobar S.R.L. destinada a la venta y distribución de repuestos de Automotores con domicilio Social Ruta 9 N° 1039 de la localidad de Escobar del Partido de Escobar de la Provincia de Buenos Aires el plazo de duración será de 99 años a partir de su inscripción. El Capital Social se fija en la suma de pesos doce mil pesos, que se divide en 1200 cuotas iguales de pesos diez (\$ 10) cada una, las que son totalmente suscriptas por los socios Las cuotas son suscriptas en las siguientes proporciones el Señor Héctor Ariel Burruchaga, 1140 cuotas por la suma de pesos once mil cuatrocientos y la Señora Dallana Brosso González 60 cuotas por la suma pesos seiscientos \$ 600. La Administración y representación de la sociedad estará a cargo de un gerente que ejercerán dicha función, por el término de tres años los que podrán ser reelegidos requiriendo simple mayoría. La fiscalización de la sociedad estará a cargo de los socios conforme las estipulaciones del art. 159 de la Ley de Sociedades Comerciales. La Representación Legal estará a cargo de Héctor Ariel Burruchaga Documento Nacional de Identidad Número 29.396.646, CUIT 20-29396646-0 con domicilio en Avenida Presidente Juan Domingo Perón 5730 de la localidad de Benavidez del Partido de Tigre de la Provincia de Buenos Aires. El ejercicio económico de la sociedad cerrará el día 30 de junio de cada año, debiendo confeccionar un balance donde surjan las ganancias y pérdidas, el cual será puesto a disposición de los socios con no menos de 10 días de anticipación a su consideración en la Asamblea. En la ciudad de Escobar a los 28 días de octubre de 2016.  
L.M. 197.811

### WALFER S.R.L.

POR 1 DÍA - Por Acta de reunión unánime de socios del 26/10/16. Gerente: José Alberto Galeano, argentino, 10/3/77, soltero, 26.234.398, empresario, domicilio Beliera 3754, Barrio Santa Teresa, Pilar, Prov. Bs. As. Julio Querzoli, Contador Público.  
L.M. 197.815