

**ISSSTELEON**Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

FICHA TÉCNICA PARA LA RENOVACIÓN DE EQUIPOS DE CÓMPUTO, SERVICIOS DE REDES INFORMÁTICAS Y DE TELEFONÍA

A) Computadora de escritorio - Personal de Administración

Cantidad	Características
104	<p>SISTEMA OPERATIVO: Windows 10 pro 64 bits PROCESADOR: Intel core i5-9500t 9a. generación MEMORIA: 8 GB, DDR4, 2666 mhz GRAFICOS DE VIDEO: Uhd graphics 630 con memoria compartida para gráficos DISCO DURO: 256 GB de estado solido PUERTOS: Parte delantera: 1 conector de auriculares; 1 USB 3.1 Gen 1 (de carga); 1 USB 3.1 Gen 2; 1 conector de auriculares Parte trasera: 1 RJ-45; 2 DisplayPort™ 1.2; 2 USB 3.1 Gen 1; 2 USB 2.0 DISPOSITIVOS DE ENTRADA: Teclado compacto profesional USB; Ratón óptico USB DIMENSIONES: 17,7 x 17,5 x 3,4 cm PESO: 1,25 kg FACTOR DE FORMA: Desktop Mini</p> <p>GESTIÓN DE SEGURIDAD: DriveLock; Sensor de cubierta; Agente de Gestión de Seguridad; Gestor de credenciales; Password Manager; Autenticación de encendido; Seguridad del registro de arranque maestro; Contraseña de encendido (vía BIOS); Autenticación de prearranque; Inhabilitación de puerto SATA (vía BIOS); Habilitación/inhabilitación de serie (vía BIOS); Contraseña de configuración (vía BIOS); Admite candados para chasis y dispositivos de bloqueo con cable; Controlador de seguridad de punto final , TPM 2.0 que se incluye con Windows 10. Certificación Common Criteria EAL4+. Certificación FIPS 140-2 de nivel 2; Habilitación/inhabilitación de USB (vía BIOS)</p> <p>FUNCIONES DE GESTIÓN: Utileria de configuración de BIOS; Cloud Recovery; Paquetes de controladores; Image Assistant; Kit de integración Management para Microsoft System Center Configuration Management; System Software Manager; Actualización de BIOS a través de la nube o de la red (función BIOS)</p> <p>SOFTWARE (NO FREEWARE O SHAREWARE):</p> <ul style="list-style-type: none"> • Software de borrado seguro que permita eliminar de forma permanente la información contenida en el disco duro del equipo. • Software de seguridad que permita crear sesiones de navegación aislada basada en hardware, el cual permita que un sitio web no pueda infectar el sistema. • Software antimalware independiente al Windows Defender, que permita detectar posibles





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

amenazas en archivos y eliminarlos de forma automática.

GARANTÍA: 4 años de garantía con tiempo de solución de 4 horas, cobertura contra daños accidentales

MONITOR

TAMAÑO DE PANTALLA: 21.5"

RELACIÓN ANCHO/ALTO: 16:9

RESOLUCION: FHD (1920 x 1080)

SEPARACION ENTRE PÍXELES: 0,248 mm

BRILLO /TÍPICO): 250 nits

RELACION DE CONTRASTE: 1000:1

TIEMPO DE RESPUESTA: 5 ms encendido/apagado

FUNCIONES DE LA PANTALLA: antirreflejante / modo de luz azul baja

SEGURIDAD FISICA: preparado para bloqueo de seguridad

CONECTOR DE ENTRADA: 1 VGA / 1 HDMI 1.4

PESO: 2.85 KG

DIMENSIONES MINIMAS (ANCH. X PROF. X ALT.): 50,5 x 42 x 31,02 cm

CONSUMO DE ENERGÍA: 19 W (máximo), 18,5 W (típico), 0,5 W (en espera)

INTERVALO DE HUMEDAD EN FUNCIONAMIENTO: Del 20 al 80% sin condensación



B) Computadora portátil - Alto Desempeño

Cantidad	Características
10	<p>PROCESADOR: Intel core i5-8265u 8a. generacion 1.6 ghz (hasta 3.9 ghz) con tecnologia turbo boost, 6 mb l3 de caché y 4 nucleos</p> <p>SISTEMA OPERATIVO: Windows 10 pro 64</p> <p>MEMORIA: 8 GB SDRAM DDR4-2400</p> <p>RANURAS DE MEMORIA: 2 SODIMM</p> <p>ALMACENAMIENTO: 256 GB de estado solido pcie® nvme</p> <p>GRAFICOS: UHD 620</p> <p>PANTALLA: Pantalla de retroiluminacion WLED FHD IPS antirreflectante, de 14" en diagonal, 250 nits, 45% de ntsc (1920 x 1080)</p> <p>PESO: A PARTIR DE 1.84 KG</p> <p>DIMENSIONES MÍNIMAS: 32,6 x 23,43 x 1,79 CM</p> <p>CAMARA: Camara WEB HD de 720p</p> <p>DISPOSITIVO APUNTAADOR: Clickpad que admite gestos multitáctiles</p> <p>FUNCIONES DE AUDIO: Audio de Bang & Olufsen, altavoces estéreo duales, micrófono digital frontal HP de doble matriz, teclas de función para aumentar y reducir el volumen, conector combinado de micrófono/auriculares, audio HD</p> <p>PUERTOS: 1 USB 3.0, 1 lector de tarjeta inteligente</p> <p>GESTION DE SEGURIDAD: Absolute Persistence Module; Agente de gestión de seguridad; Device Access Manager; Manageability Integration Kit; Autenticación de encendido; Secure Erase; Support Assistant; Sure Recover; Sure Recover con Embedded Reimaging; Sure Start; Seguridad de registro de arranque maestro; Microsoft Security Defender; Autenticación de prearranque; Ranura con cierre de seguridad; Chip de seguridad incorporado Trusted Platform Module TPM 2.0</p> <p>PRUEBAS: Al menos 19 MIL-STD 810H</p> <p>BIOS: Inglés o español, propietario del fabricante o con derechos reservados para el fabricante, almacenado en Flash ROM, actualizable vía red, vía USB o a través del sistema operativo, que tenga manejo de Plug and Play en aquellos dispositivos que lo permitan.</p> <p>El BIOS debe tener la capacidad de auto reparación a través de un respaldo en un chip integrado a la tarjeta madre sin requerir de una conexión a internet.</p> <p>SOFTWARE (NO FREEWARE O SHAREWARE):</p> <ul style="list-style-type: none"> • Software de seguridad para la protección al acceso no autorizado a datos confidenciales o a credenciales del usuario con la capacidad de cifrar archivos, carpetas o una unidad lógica dentro del disco duro. • Software de borrado seguro con licenciamiento a perpetuidad. No freeware o shareware. • Software de seguridad que permita crear sesiones de navegación aislada basada en hardware, el cual permita que un sitio web no pueda infectar el sistema.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Software de protección antimalware en tiempo real, adicional al Windows defender incluido en el sistema operativo.

COLOR DEL PRODUCTO: Plata turbo

GARANTIA: 4 años de garantía con tiempo de solución de 4 horas, cobertura contra daños accidentales



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

C) Computadora portátil - Coordinadores

Cantidad	Características
25	<p> PROCESADOR: Intel core i5-8265u 8a. generacion 1.6 ghz (hasta 3.9 ghz) con tecnologia turbo boost, 6 MB l3 de caché y 4 nucleos SISTEMA OPERATIVO: windows 10 pro 64 MEMORIA: 8 gb SDRAM DDR4-2400 RANURAS DE MEMORIA: 2 SODIMM ALMACENAMIENTO: 256 GB DE estado solido pcie® nvme GRAFICOS: UHD 620 PANTALLA: Pantalla de retroiluminacion wled de 14" en diagonal (1366 x 768) PESO: A partir de 1.734 kg DIMENSIONES MÍNIMAS: 34 x 24 x 2,09 cm CAMARA: Camara web HD de privacidad PUERTOS: 1 puerto rj-45, 1 puerto vga, 1 puerto hdmi, 1 puerto usb 3.0 y 1 puerto usb-c DISPOSITIVO APUNTADOR: Clickpad que admite gestos multitáctiles FUNCIONES DE AUDIO: Altavoces dobles estéreo y micrófono dual </p> <p> GESTIÓN DE SEGURIDAD: Absolute Persistence Module; DriveLock y Automatic DriveLock; Secure Erase; Autenticación de encendido; Autenticación de prearranque; Lector Smart Card; El chip de seguridad integrado Trusted Platform Module 2.0 se suministra con Windows 10 (certificación Common Criteria EAL4+); Sure Click; Windows Defender; Sure Start Gen5; Client Security Gen5; Sure Sense </p> <p> FUNCIONES DE GESTIÓN: Paquetes de controladores; System Software Manager (SSM); BIOS Config Utility (BCU); Kit de integración Manageability </p> <p> PRUEBAS: Al menos 19 MIL-STD BIOS: Inglés o español, propietario del fabricante o con derechos reservados para el fabricante, almacenado en Flash ROM, actualizable vía red, vía USB o a través del sistema operativo, que tenga manejo de Plug and Play en aquellos dispositivos que lo permitan. El BIOS debe tener la capacidad de auto reparación a través de un respaldo en un chip integrado a la tarjeta madre sin requerir de una conexión a internet. COLOR DEL PRODUCTO: Plata </p> <p> GARANTIA: 4 años de garantía con tiempo de solución de 4 horas, cobertura contra daños accidentales </p>





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

D) Computadora portátil - Subdirección

Cantidad	Características
4	<p> PROCESADOR: Intel core i5-8265u 8a. generacion 1.6 ghz (hasta 3.9 ghz) con tecnologia turbo boost, 6 MB l3 de caché y 4 nucleos SISTEMA OPERATIVO: windows 10 pro 64 MEMORIA: 8 gb SDRAM DDR4-2400 RANURAS DE MEMORIA: 2 SODIMM ALMACENAMIENTO: 256 GB DE estado solido pcie® nvme GRAFICOS: UHD 620 PANTALLA: Pantalla de retroiluminacion wled de 14" en diagonal (1366 x 768) PESO: A partir de 1.734 kg DIMENSIONES MÍNIMAS: 34 x 24 x 2,09 cm CAMARA: Camara web HD de privacidad PUERTOS: 1 puerto rj-45, 1 puerto vga, 1 puerto hdmi, 1 puerto usb 3.0 y 1 puerto usb-c DISPOSITIVO APUNTADOR: Clickpad que admite gestos multitáctiles FUNCIONES DE AUDIO: Altavoces dobles estéreo y micrófono dual </p> <p> GESTIÓN DE SEGURIDAD: Absolute Persistence Module; DriveLock y Automatic DriveLock; Secure Erase; Autenticación de encendido; Autenticación de prearranque; Lector Smart Card; El chip de seguridad integrado Trusted Platform Module 2.0 se suministra con Windows 10 (certificación Common Criteria EAL4+); Sure Click; Windows Defender; Sure Start Gen5; Client Security Gen5; Sure Sense </p> <p> FUNCIONES DE GESTIÓN: Paquetes de controladores; System Software Manager (SSM); BIOS Config Utility (BCU); Kit de integración Manageability </p> <p> COLOR DEL PRODUCTO: Plata </p> <p> PRUEBAS: Al menos 19 MIL-STD BIOS: Inglés o español, propietario del fabricante o con derechos reservados para el fabricante, almacenado en Flash ROM, actualizable vía red, vía USB o a través del sistema operativo, que tenga manejo de Plug and Play en aquellos dispositivos que lo permitan. El BIOS debe tener la capacidad de auto reparación a través de un respaldo en un chip integrado a la tarjeta madre sin requerir de una conexión a internet. </p> <p> GARANTIA: 4 años de garantía con tiempo de solución de 4 horas, cobertura contra daños accidentales </p>



**ISSSTELEON**Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León**E) Computadora portátil - Dirección**

Cantidad	Características
5	<p>PROCESADOR: Procesador Intel® Core™ i5 de 10.ª generación: 1035G1</p> <p>SISTEMA OPERATIVO: Windows 10 PRO 64</p> <p>MEMORIA: 8 GB de RAM LPDDR4x</p> <p>ALMACENAMIENTO: Unidad eMMC: 128 GB</p> <p>GRAFICOS: Intel UHD graphics</p> <p>PANTALLA: Pixelsense DE 12.4" táctil</p> <p>RESOLUCION: 1536 X 1024</p> <p>PESO: 1.110 G (2,44LB)</p> <p>DIMENSIONES MÍNIMAS: 278,18 mm x 205,67 mm x 15,69 mm (10,95" x 8,10" x 0,62")</p> <p>CAMARAS, VIDEO Y AUDIO: Cámara de alta definición de 720p HD f2.0 (frontal), dos micrófonos de estudio de campo lejano, Altavoces Omnisonic con Dolby® Audio™</p> <p>PUERTOS: 1 puerto Usb-C, 1 puerto Usb-A, conector de auriculares 3,55 mm 1 puerto surface connect</p> <p>RED INALÁMBRICA: Tecnología bluetooth wireless 5.0, wi-fi 6 compatible con 802.11ax</p> <p>EXTERIOR: Parte superior de aluminio, base sistema de policarbonato de resina compuesta con fibra de vidrio y 30% de contenido reciclado posterior al consumidor.</p> <p>GESTIÓN DE SEGURIDAD: Firmware del TPM, proteccion de nivel empresarial con inicio de sesion de un solo toque de windows hello, inicio de sesión de un solo toque con el boton de inicio/apagado con lector de huellas digitales.</p> <p>COLOR DEL PRODUCTO: platino</p> <p>GARANTIA: 4 años de garantía con tiempo de solución de 4 horas, cobertura contra daños accidentales</p>

SERVICIOS PROFESIONALES COMPUTO

Etapa	Descripción
Preparación de equipo	Creación y planchado imágenes de SO Windows con el software requerido en los equipos adquiridos.
Envío de equipos	Envío de euipos a instalaciones del cliente
Migración de usuarios	Entrega e instalación de equipos a usuarios conservando los documentos de su perfil en el equipo a retirar.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Retiro de equipos	Retiro y resguardo de equipo.
Entrega de equipo	Entrega de equipo retirado al cliente. Inventario y etiquetado

CENTRO DE DATOS

Cantidad	Características
2	<p>Servidor de Rack</p> <p>PROCESADOR: Intel Xeon-Silver 4214R (2.4GHz/12-core/100W)</p> <p>NÚMERO DE PROCESADORES: 2</p> <p>NÚCLEO DE PROCESADOR DISPONIBLE: 12, por procesador</p> <p>VELOCIDAD DEL PROCESADOR: 2.4 GHZ</p> <p>TIPO DE FUENTE DE ALIMENTACIÓN: 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit</p> <p>MEMORIA, ESTÁNDAR: 32GB (4x32GB) Dual Rank x4 DDR4-2933</p> <p>TIPO DE MEMORIA: ddr4 smart memory</p> <p>UNIDADES DE DISCO DURO INCLUIDAS: 6 unidades de disco duro incluidas con capacidad de 2,4TB SAS SFF a 10KRPM cada una</p> <p>TIPO DE UNIDAD ÓPTICA: Opcional a través de la bahía de soportes universal</p> <p>CARACTERÍSTICAS DE LOS VENTILADORES DEL SISTEMA: 4 ventiladores estándares de un rotor incluidos</p> <p>CONTROLADOR DE RED: 1 adaptador ethernet 1gb de 4 puertos con tarjeta stand-up opcional</p> <p>CONTROLADOR DE ALMACENAMIENTO: 1 smart array 2gb más batería de almacenamiento inteligente y 1 smart array</p> <p>DIMENSIONES Maximas (ALTO X ANCHO X FONDO): 44,55 X 73,03 X 8,74 CM</p> <p>PESO: 14,76 KG</p> <p>ADMINISTRACIÓN DE INFRAESTRUCTURA: standard con aprovisionamiento inteligente (integrado), puerto de administracion remota por interfaz grafica</p> <p>GARANTÍA: - la garantía del servidor incluye tres años de garantía en piezas, tres años de mano de obra y tres años de cobertura de soporte a domicilio</p> <p>Para efectos del servicio de soporte, se debe:</p> <ul style="list-style-type: none"> • Dotar al del acceso al portal de soporte web del fabricante. -Integrar con la propuesta las líneas telefónicas de atención de soporte del fabricante. • Entrega con la propuesta a Instituto de Seguridad y Servicios Sociales de los Trabajadores al Servicio del Estado de Nuevo León la documentación mediante la cual





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

el fabricante especifica el procedimiento y los pormenores de la atención para soporte, garantía y mantenimiento.

La solución que se le entregue a Instituto de Seguridad y Servicios Sociales de los Trabajadores al Servicio del Estado de Nuevo León debe incluir servicios de soporte durante 3 años a partir de la entrega y puesta en funcionamiento, de acuerdo con las siguientes características:

- Accesos telefónicos las 24 hrs, todos los días, incluidos los días festivos, al centro de recepción de llamadas del fabricante, para soporte (o su equivalente) por parte del fabricante.
- Envíos a sitio de técnicos o piezas de repuesto a las instalaciones de la Institución
- Asistencia para la solución remota de problemas comunes de soporte del proveedor y en consecuencia con el fabricante
- Solución de problemas en el sitio dentro de las 4 horas siguientes al reporte del caso de soporte toda vez se haya evaluado y determinado que es necesario el apoyo de campo para un solución por parte del proveedor y en consecuencia del fabricante.
- Se debe ofrecer mantenimiento preventivo anual del proveedor y fabricante
- Servicio de monitoreo a equipo por parte del proveedor contando con un número telefónico local en español y levantamiento de ticket 24x7 durante 36 meses.
- Servicio de Ingeniero certificado por el fabricante para atender al Instituto de Seguridad y Servicios sociales de los Trabajadores al Servicio del Estado de Nuevo León 24 x7 para temas de soporte proporcionado celular del ingeniero para una respuesta más inmediata del proveedor.

Software de virtualización para servidores

El software de virtualización que incluye 3 años de soporte ilimitado 24x7. Soporte para la reparación, configuración y solución de problemas

Incluye: Consola de administración centralizada para la administración y gestión de servidores virtuales que ofrece una plataforma centralizada para el control de los entornos virtuales con la que se podrá automatizar y proporcionar una infraestructura virtual en la nube híbrida con total confianza.

Características de la consola de administración centralizada:

- Extensibilidad y escalabilidad en la nube híbrida
- Control y visibilidad centralizados
- Gestión mejorada
- Optimización proactiva
- Elementos nativos



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Funciones principales de la plataforma de virtualización:

- Migración en vivo de máquinas virtuales en ejecución entre servidores físicos de un mismo ambiente virtual de manera ininterrumpida y con integridad
- Programador de recurso distribuidos
- Alta disponibilidad proactiva
- Almacenamiento optimizado para máquinas virtuales
- Características de almacenamiento basadas en políticas y en API
- Compatibilidad con almacenamiento nativo 4 K
- Memoria persistente de la plataforma
- Migración dinámica de cargas de trabajo
- Protección de máquinas virtuales y datos
- Cifrado a nivel de máquina virtual
- Compatibilidad con TPM 2.0.
- Virtual TPM 2.0
- Conformidad con FIPS 140-2
- Garantía del tiempo de actividad del sistema
- Uso compartido de los recursos del centro de datos
- Seguridad de los puntos de acceso
- Tolerancia a fallos
- Clon instantáneo
- Gestión centralizada de redes
- Equilibrio de carga
- Priorización de los recursos para las máquinas virtuales
- Rápida implementación y distribución
- Gráficos acelerados para las máquinas virtuales
- Compatibilidad de suspensión, reanudación, y varias v GPU por máquina virtual e instantánea para v GPU de NVIDIA
- Detección automatizada de recursos de aplicaciones, intención y comunicación
- Inteligencia contextual de estado de aplicaciones
- Respuesta coordinada o automatizada a amenazas de seguridad
- Informes de vulnerabilidades prioritarias de todo el centro de datos

- Copia de seguridad y replicación

- Copia de seguridad y recuperación: datos respaldados y recuperables con varias opciones de copia de seguridad y recuperación granular.



- Automatización: preparar, probar y organizar la estrategia de recuperación ante desastres para proteger aplicaciones críticas.
- Portabilidad de la nube: la nube es parte de la estrategia del centro de datos, realizar copias de seguridad y recuperación desde, hacia y dentro de la nube para obtener portabilidad y ahorrar costos.
- Gobierno y cumplimiento: gestionar de forma eficaz copias de seguridad a partir de pruebas virtuales para garantizar que las copias de los datos sean recuperables, seguras y compatibles.

Características :

- Opciones de recuperación y respaldo virtual y físico en la nube
- Replicación de máquina virtual (VM) basada en imágenes desde una VM o respaldo
- Administración e implementación integradas para Linux y para Microsoft Windows
- Capacidades de capacidad de almacenamiento ilimitadas con repositorio de copia de seguridad escalable y soporte de almacenamiento de objetos Cloud Tier
- Restauración directa en 2 pasos en AWS, Microsoft Azure
- Laboratorio de datos: Recuperación verificada, cumplimiento de seguridad y pruebas virtuales sandbox
- Explorer para-Microsoft Exchange, Microsoft Active Directory, Microsoft SharePoint, Microsoft SQL Server y Oracle
- Instantáneas de almacenamiento e integración avanzada de almacenamiento
- Complementos empresariales para SAP HANA y Oracle RMAN
- API de integración de datos y API de almacenamiento universal
- WAN incorporada Aceleración que incluye un modo de gran ancho de banda
- Cifrado, compresión y de duplicación
-

Servicios profesionales para el centro de datos

Instalación e interconexión de Infraestructura.

- Traslado de equipos a centro de datos
- Desembalaje y armado de equipos de Rack
- Montaje de servidores en rack
- Energización de equipos y conexión de red

Configuración de Infraestructura.

- Configuración de puerto de administración remota
- Configuración inicial de puerto de administración remota y firmware

Instalación y configuración de plataforma de virtualización

- Instalación de prerrequisitos en servidores de rack



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

	<ul style="list-style-type: none"> • Instalación completa de plataforma de virtualización con todas las herramientas y funciones incluidas • Configuración de direccionamiento IP • Migración de cargas de trabajo a la nueva plataforma desde el ambiente actual • Pruebas de funcionamiento y comunicación de cargas de trabajo <p>Instalación de software de replicación y respaldo</p> <ul style="list-style-type: none"> • Instalación de servidor de herramienta Backup and Replication • Despliegue de cargas de trabajo para replicación • Instalación de repositorios de respaldo • Creación de "Jobs" de replicación • Monitoreo en tiempo real de progreso de replicación <p>Transferencia de conocimiento</p> <ul style="list-style-type: none"> • Documentación de proceso de migración de cargas de trabajo • Transferencia de conocimiento del proceso de migración • Sesión de capacitación en el uso de consola de administración centralizada para 1 administrador <p>Retiro de equipos</p> <ul style="list-style-type: none"> • Inventario de equipo retirado • Transportación y almacenamiento de equipo retirado <p>Soporte</p> <ul style="list-style-type: none"> • Soporte y monitoreo a infraestructura servidores • Soporte y monitoreo a herramienta de replicación y respaldo • Soporte y monitoreo a plataforma de virtualización <p>Etiquetado</p> <ul style="list-style-type: none"> • Obtener documento de ubicación de dispositivos • Etiquetado de racks y dispositivos <p>Documentación</p> <ul style="list-style-type: none"> • Entrega de documento y diagrama de ubicación • Sesión de entrega





RED INALÁMBRICA

Controlador Wireless

Cantidad	Características
1	<p>Controlador de acceso inalámbrico. Dispositivo autónomo (no debe ser un módulo que requiera ser instalado en un chasis) Debe incluir mínimo:</p> <ul style="list-style-type: none"> • 12 puertos 10/100/1000Base-T, Auto-MDIX, IEEE 802.3at PoE+ • 4 puertos 10/100/1000Base-T, Auto-MDIX • 2 puertos SFP" <p>Al menos:</p> <ul style="list-style-type: none"> • Un interfaz serial RJ45 • Un Interfaz MicroUSB <p>Wireless El Controlador Inalámbrico debe ofrecer al menos:</p> <ul style="list-style-type: none"> • Un crecimiento al menos hasta 32 APs de la misma marca. • El crecimiento debe darse únicamente a través de licenciamiento, no debe requerir cambios en el hardware del equipo. • Los APs soportados deben ser tanto para interiores como para exteriores." <p>El Controlador ofertado debe incluir todo cuanto requiera para atender al menos a 2,048 clientes inalámbricos concurrentes. El controlador ofertado debe incluir todo cuanto requiera para poder conmutar al menos 4Gbps de tráfico inalámbrico centralizado. El controlador ofertado debe incluir el servicio de portal local para al menos 2,048 usuarios. El controlador ofertado debe incluir el servicio de autenticación Triple "A" (AAA) para al menos 2,048 usuarios. El controlador ofertado debe soportar al menos 64 SSIDs configurados. El controlador ofertado debe soportar al menos 2.000 Listas de Control de Acceso (ACLs). "Debe cumplir al menos los siguientes estándares de la industria:</p> <ul style="list-style-type: none"> • IEEE 802.11a • IEEE 802.11b • IEEE 802.11d • IEEE 802.11e • IEEE 802.11g • IEEE 802.11h



- IEEE 802.11i
- IEEE 802.11k
- IEEE 802.11n
- IEEE 802.11s D1.06 draft
- IEEE 802.11w
- IEEE 802.11ac"

"Debe ofrecer al menos los siguientes servicios:

- Ajuste automático de potencia de los radios.
- Detección en tiempo real de interferencias.
- Conmutación inteligente y en tiempo real del canal.
- Balanceo inteligente de clientes entre múltiples APs.
- Mecanismos para ofrecer tiempos iguales de transmisión a los clientes.
- Identificación de fuentes de interferencia RF que permita detectar y clasificar señal inalámbrica.
- Evaluación de calidad de canal.
- Redirección de usuarios que puedan trabajar en 5GHz a esta banda.
- Asignación dinámica de clientes a diferentes VLANs.
- Visibilidad unificada de red alámbrica e inalámbrica utilizando al menos LLDP.
- Configuración automática de APs.
- Aplicación de políticas basadas en el SSID o perfil de usuario.
- Capacidad para agrupar APs.
- Capacidad para actualizar el sistema operativo de los APs.
- Capacidad para seleccionar la ganancia de la antena.
- Roaming rápido.
- Roaming en Capa 3."

"El Controlador debe soportar al menos los siguientes tipos de manejo para el tráfico inalámbrico:

- Tráfico centralizado, esto es, el tráfico inalámbrico debe pasar primero por el Controlador antes de pasar a la red alámbrica.
- Tráfico distribuido, esto es, el tráfico inalámbrico puede ir directo del AP hacia la red alámbrica."

"Debe ofrecer al menos:

- QoS de extremo a extremo al menos a través de DiffServ e IPv6 QoS.
- Priorización IEEE 802.1p.
- CoS basado dirección IP, ToS, protocolos de L3, número de puertos TCP o UDP, puerto origen y DiffServ.
- Perfiles de QoS."



"Debe ofrecer al menos:

- AAA
- Login vía 802.1x y RADIUS.
- Autenticación basada en web para clientes que no soportan 802.1x.
- Autenticación por dirección MAC.
- WEP, WPA, WPA2.
- Control de acceso de usuarios definidos por el administrador en APs específicos."

"El controlador inalámbrico debe contar con servicios integrados de Firewall, al menos basado en:

- Filtrado de paquetes basado en Listas de Control de Acceso.
- Filtrado de paquetes específicos por aplicación."

"Debe integrar un Wireless IDS (Intrusion Detection System) que permita detectar al menos:

- Inundaciones.
- Spoofing.
- Ataques por debilidad.
- Identificar en forma automática APs y estaciones.
- Base heurística de conocimiento.
- Protección contra ataques de tipo honeypot.
- Seguridad reforzada STA.
- Detección de ataques DoS.
- Distribución de políticas a dominios virtuales de seguridad."

"Debe ofrecer al menos:

- Validación de la relación dirección IP y MAC de usuarios para evitar ataques de suplantación.
- Aislamiento de usuarios para provisión de servicios diferenciados por grupos.
- Integración con servicios de control de admisión a la red.
- PKI.
- Guest VLAN.
- SSL
- SSHv2
- RFC 1851 ESP
- RFC 2246 TLS
- RFC 2401 Security Architecture
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2548 Microsoft RADIUS Attributes
- RFC 2716 PPP EAP TLS Auth
- RFC 2865 RADIUS Authentication



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- RFC 2867 RADIUS for Tunnel Protocol
- RFC 3394 AES
- RFC 3576 Dynamic Authorization
- RFC 3579 RADIUS Support for EAP
- RFC 3580 IEEE 802.1X RADIUS"

"Debe soportar al menos los siguientes esquemas de redundancia y respaldo:

- 1+1.
- N+1.
- N+N.

El cualquiera de los esquemas, la validación de los APs debe ser automática, ofreciendo un servicio continuo ante la falla de uno de los Controladores."

IP

"Debe ofrecer al menos:

Enrutamiento estático IPv4 e IPv6.
RIPv1/v2 , OSPF"

"Debe cumplir al menos los siguientes estándares de la industria:

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET
- RFC 894 IP over Ethernet
- RFC 950 Standard Subnetting
- RFC 959 FTP
- RFC 1122 Host Requirements
- RFC 1141 Internet checksum
- RFC 1144 Compressing TCP/IP headers
- RFC 1256 ICMP Router Discovery
- RFC 1305 NTPv3
- RFC 1321 MD5
- RFC 1334 PPP PAP
- RFC 1350 TFTP Protocol revision 2
- RFC 1812 IPv4 Routing
- RFC 1944
- RFC 1994 PPP CHAP
- RFC 2104 HMAC



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- RFC 2246 The TLS Protocol v1.0
- RFC 2474 DS Field in IPv4 & IPv6
- RFC 2475 DiffServ
- RFC 2284 EAP over LAN
- RFC 2644 Directed Broadcast Control
- RFC 2864
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3164 Syslog
- RFC 3168 ECN to IP
- RFC 3268 AES for TLS
- RFC 3619 EAPS
- RFC 3636 Medium Attachment Units"

"Debe cumplir al menos los siguientes estándares de la industria:

- RFC 1112 IGMP
- RFC 2236 IGMPv2
- RFC 2934 PIM MIB para IPv4
- RFC 4541 IGMP and MLD Snooping"

"Debe cumplir al menos los siguientes estándares de la industria:

- IPv6 Host.
- Dual stack IPv4 - IPv6.
- MLD snooping.
- Listas de Control de Acceso para IPv6.
- Calidad de servicio (QoS) para IPv6.
- RFC 1981 IPv6 MTU Discovery
- RFC 2375 IPv6 Multicast Assignments - RFC 2328 OSPFv2
- RFC 2460 IPv6 Specification
- RFC 2463 ICMPv6
- RFC 2464 IPv6 over Ethernet
- RFC 2466 MIB for IPv6 - ICMPv6
- RFC 2526 Reserved IPv6 Anycast
- RFC 2553 Socket Interface
- RFC 3315 DHCPv6 (client and relay)
- RFC 3484 Default Address Selection
- RFC 3513 IPv6 Addressing Architecture
- RFC 3542 Advanced Sockets API
- RFC 3587 IPv6 Global Unicast Address



- RFC 3596 DNS Extension for IPv6
- RFC 4193 IPv6 Unicast Addresses
- RFC 4443 ICMPv6
- RFC 4541 IGMP & MLD Snooping Switch
- RFC 4861 IPv6 Neighbor Discovery
- RFC 4862 IPv6 Add Autoconfiguration
- RFC 5095 Deprecation of Type 0"

"Al menos:

- NAT muchos a uno.
- NAT uno a uno.
- Conexión con APs en oficinas remotas donde se haya realizado traslación de direcciones."

"Debe cumplir al menos los siguientes estándares de la industria:

- Certificate and Certificate Revocation List

(CRL) Profile

- RFC 1829 The ESP DES-CBC Transform
- RFC 2403 HMAC-MD5 within ESP and AH
- RFC 2404 HMAC-SHA within ESP and AH
- RFC 2405 ESP DES-CBC
- RFC 2407 Interpretation for ISAKMP
- RFC 2451 ESP CBC-Mode Cipher
- RFC 3280 Internet X.509 Public Key
- RFC 3602 The AES-CBC Cipher Algorithm
- RFC 3748 EAP"

"Debe soportar al menos:

- SNMP v1
- SNMP v2c
- SNMP v3"

PoE/PoE+

- IEEE 802.3af.
- IEEE 802.3at."

Mínimo 150w

En todos los puertos.

Hardware y Energía

El equipo debe soportar al menos:

- Debe soportar una alimentación en AC de 90 VAC a 264 VAC con 47 Hz a 63 Hz.
- El consumo máximo no debe ser superior a 190W."



	<p>"Cumplir al menos:</p> <ul style="list-style-type: none"> • UL 60950-1 • CAN/CSA 22.2 No. 60950-1 • IEC 60950-1 • EN 60950-1 • FDA 21 CFR Subchapter J • EN 55022 Class A • CISPR 22 Class A • ICES-003 Class A • AS/NZS CISPR 22 Class A • EN 61000-3-2 • EN 61000-3-3 • VCCI-3 CLASS A • VCCI-4 CLASS A • ETSI EN 300 386 • FCC Part 15 (CFR 47) CLASS A"
--	---

Control de acceso a redes

Cantidad	Características
1	<p>La solución debe de dar soporte para 500 sesiones y tener la capacidad de crecer hasta 50.000 sesiones RADIUS activas concurrentes por cada appliance</p> <p>Deberá incluir en el licenciamiento base los siguientes servicios:</p> <ul style="list-style-type: none"> • 802.1X • Autenticación por MAC Address • TACACS+ • Enforcement a través de SNMP • Perfilamiento de dispositivos • Integraciones con terceros mediante REST APIs <p>La política de seguridad deberá permitir tomar en consideración elementos contextuales como: horario, ubicación, tipo de dispositivo, versión de SO y nombre del dispositivo, entre otros</p> <ul style="list-style-type: none"> • Soporte para Assessment de postura, perfilamiento y autenticación web en ambientes de red multi-vendor y basado en protocolos estándar RADIUS y RADIUS CoA



- Deberá controlar el acceso de usuarios y dispositivos a través de la red cableada (switches), inalámbrica (access points y controladores WiFi) y VPN (firewalls y concentradores VPN) de manera unificada
- '- Deberá soportar la aplicación de políticas contextuales mediante servicios AAA: RADIUS, RADIUS CoA, TACACS+ y SNMP
- '- Deberá incluir sin costo adicional un componente de monitoreo y reportería con información en tiempo real e histórica sobre usuarios y dispositivos conectados, alertas, detalle de autenticación y autorización, consumo de anchos de banda

Deberá soportar los siguientes métodos de perfilamiento:

- Activo: Nmap, WMI, SSH, SNMP
 - Pasivo: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, Puerto 'SPAN', HTTP User-Agent, IF-MAP
 - Integrados y de terceros: Desde la solución de BYOD y de chequeo de postura, EMM/MDM, Rapid7, Cisco device sensor.
- '- La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria

Acceso de externos via Portal Cautivo (Invitados, contratistas, clientes)

- '- Deberá proveer la opción de autoregistro con confirmación de cuenta vía impresión de ticket, SMS o e-mail, para asegurar que los datos ingresados por los usuarios sean válidos
- '- Deberá permitir que antes de que un usuario externo se pueda conectar, el acceso deba ser aprobado por un usuario corporativo (auto-registro con sponsor)
- '- Deberá permitir que la validez de las cuentas de invitados sea configurable en base a tiempo, anchos de banda utilizados, horario de conexión, entre otros
- '- Deberá permitir la personalización total del portal cautivo con logos, publicidad, videos, encuestas, etc
- '- Deberá proveer la opción de acceder a la red a través de las redes sociales Facebook, Twitter, linkedin y Google
- '- Deberá ajustar de manera automática el tamaño del portal, de acuerdo al dispositivo con el cual se conectan los usuarios
- '- Deberá proveer encriptación del tráfico sobre una red abierta mediante el estándar PEAP-Public
- '- Deberá permitir la asignación de políticas de acceso basadas en roles, para poder asegurar anchos de banda, acceso a recursos específicos y duración de las conexiones, de acuerdo al tipo de invitado
- '- Deberá permitir la integración con sistemas gestión de huéspedes, pacientes y cobro, tales como: Micros Opera PMS, Protel PMS, Silverbyte Optima PMS, Agilysis Visual One PMS, etc



- 'Deberá permitir realizar Caching de direcciones MAC por cierta cantidad de tiempo, para evitar que los usuarios recurrentes tengan que introducir constantemente sus credenciales
- 'Deberá permitir asignar accesos basados en roles a los operadores que crean o modifican las cuentas de usuarios

Protocolos y Frameworks soportados

- 'La solución deberá soportar al menos los siguientes protocolos para los servicios AAA:
- RADIUS, RADIUS CoA, TACACS+, autenticación web, SAML 2.0
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1 y 2, EAP-MD5
- OAuth2
- Autenticación de Máquina en dominio Windows
- SMB v2/v3
- Autenticación vía MAC (para dispositivos que no soportan 802.1x)
- Online Certificate Status Protocol (OCSP)
- SNMP generic MIB, SNMP private MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF)

La solución deberá soportar las siguientes fuentes de autenticación sin licenciamiento o plugins adicionales:

- Microsoft Active Directory
- RADIUS
- Cualquier directorio basado en protocolo LDAP
- MySQL, Microsoft SQL, PostGRES, Oracle 11g y cualquier servidor SQL ODBC-compliant
- Servidores de Token
- Base de datos interna
- Kerberos
- Microsoft Azure Active Directory (viaSAML y OAuth2.0)
- - Google G Suite

El sistema deberá soportar los siguientes estándares RFC:



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- RFC 2246 The TLS Protocol Version 1.0
- RFC 2248 Network Services Monitoring MIB
- RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 ISAKMP
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2548 Microsoft Vendor-specific RADIUS Attributes
- RFC 2759 Microsoft PPP CHAP Extensions, Version 2
- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices
- RFC 3079 Microsoft Point to Point Encryption
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
- RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
- RFC 3748 Extensible Authentication Protocol (EAP)
- RFC 3779 X.509 Extensions for IP Addresses and AS Identifiers
- RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
- RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4308 Cryptographic Suites for IPsec
- RFC 4346 TLS Protocol
- RFC 4514 Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
- RFC 4518 Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
- RFC 4809 Reqs for IPsec Certificate Mgmt Profile
- RFC 4849 RADIUS Filter Rule Attribute
- RFC 4851 EAP-FAST
- RFC 4945 PKI Profile for IKE/ISAKMP/PKIX
- RFC 5216 The EAP-TLS Authentication Protocol
- RFC 5246 The Transport Layer Security (TLS) Protocol
- RFC 5280 Internet X.509 Public Key Infrastructure



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- RFC 5281 EAP-TTLSv0
 - RFC 5282 Authenticated Encryption and IKEv2
 - RFC 5755 Internet Attribute Certificate Profile for Authorization
 - RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile
 - RFC 6818 Updates to the Internet X.509 Public Key
 - RFC 6960 X.509 Internet Public Key Infrastructure
 - RFC 7030 Enrollment over Secure Transport
 - RFC 7296 Internet Key Exchange Protocol Version 2
 - RFC 7321 ESP y AH
 - RFC 7468 Textual Encodings of PKIX, PKCS, and CMS Structures
 - RFC 7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation
 - RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA)
 - RFC 8247 The Internet Key Exchange v2 (IKEv2)
-
- Deberá tener la capacidad de adicionar de manera modular servicios de: Enrolamiento de dispositivos personales en entornos corporativos (BYOD) y Postura de Seguridad sobre PCs corporativos
 - El licenciamiento deberá ser perpetuo
 - Deberá tener la capacidad de integración via REST-based APIs, de manera nativa y sin costo adicional de licenciamiento, con soluciones de Seguridad Perimetral (Ej: CheckPoint, Palo Alto, Fortinet, etc), MDM/EMM (Ej: Citrix, MobileIron, AirWatch), sistemas de gestión de tickets (Ej: Service Now, y múltiples factores de autenticación (Ej: DUO, RSA SecurID), UEBA (IntroSpect)
 - Se requiere que la solución aplique el control de acceso y segmentación basada en tipo de dispositivo/usuario, para evitar el uso de múltiples VLANs para aplicar políticas de seguridad
 - La solución deberá soportar perfilamiento para despliegues con direccionamiento IP fijo
 - La solución deberá soportar autenticación via social login con Facebook, LinkedIn, Google y Twitter
 - El portal cautivo deberá ser capaz de integrarse con soluciones de PMS, pago por uso y publicidad
 - Se requiere que la solución pueda aplicar políticas de acceso, perfilamiento y autenticación sin necesidad de habilitar privilegios de administración sobre los equipos
 - Se requiere que la solución pueda perfilar y categorizar los dispositivos que se conectan a la red sin licenciamiento adicional
 - La Alta disponibilidad debe permitir modalidad activo/activo; la propuesta deberá incluir al menos 2 servidores
 - Se requiere que el failover en caso de fallas sea automático, sin necesidad de realizar tareas manuales



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

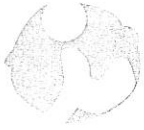
- La solución deberá soportar SAML tanto como SP e IdP y el protocolo Oauth para habilitar Single Sign On con aplicaciones y portales externos
- La solución deberá soportar bases de dato SQL como fuente de autenticación sin necesidad de agregar licenciamiento o plugins adicionales
- El portal cautivo deberá ser altamente personalizable

La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria



PUNTO DE ACCESO INALÁMBRICO

Cantidad	Características
11	<p>Access Point 802.11ac Wave 2 con conectores para antenas externas. Debe registrarse a una controladora. 1.3 Gbps de transferencia máxima, se recomienda posicionar en lugares de baja densidad de dispositivos.</p> <p>Con Controlador</p> <p>Punto de acceso (Access Point, AP) de red inalámbrica para interiores.</p> <p>Los APs deben incluir al menos: - Doble radio. - Soporte para doble banda. - MU-MIMO 3x3. - Hasta 1.3 Gbps desempeño - Al menos 16 SSID. - Asignación y selección de canal de manera automática, así como los niveles de potencia del ap - Soporte hasta de 256 clientes asociados por radio"</p> <p>Los APs deben soportar al menos los siguientes estándares de la industria:</p> <ul style="list-style-type: none"> • IEEE 802.11a • IEEE 802.11b • IEEE 802.11g • IEEE 802.11n • IEEE 802.11ac • IEEE 802.3af • Wi-Fi Alliance Certified (WiFi 6) <p>El Ap debe soportar un channel bandwidth de hasta 80 MHz (VHT80) y 3 spatial streams (3SS) para ambas comunicaciones SU y MU-MIMO</p> <p>Los Aps deben soportar al menos las siguientes velocidades: 1300Mbps en 5ghz y 300 Mbps en 2.4 Ghz.</p> <p>El Ap debe tener Radio 3x3 802.11ac con Multi User Mimo (wave 2) y un Bluetooth Low Energy BLE radio que puede ser usado como beacon integrado para ubicación avanzada de usuarios, push de notificaciones y wayfinding.</p> <p>Un puerto 10/100/1000BASE-T Ethernet. Interface USB 2.0. Interface serial de consola</p> <p>El Ap debe soportar Advanced Cellular Coexistence (ACC) para mitigar interferencia 3G y 4G Externas</p> <p>El Ap debe tener un sistema de firewall embebido para hacer filtrado de contenido web y un motor de reputación web</p> <p>"Operacional: • Operating: - Temperatura: 0° C to +50° C (+32° F to +122° F) - Humedad: 5% to 93% non-condensing"</p> <ul style="list-style-type: none"> • FCC/ISED • CE Marked • RED Directive 2014/53/EU • EMC Directive 2014/30/EU • Low Voltage Directive 2014/35/EU



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- UL/IEC/EN 60950
- EN 60601-1-1, EN60601-1-2"

PoE: 48Vdc (nominal) 802.3af/at PoE

DC power interface"

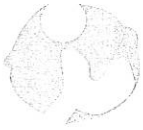
Garantía de por vida limitada

Calidad de servicio, manejo de prioridades y aplicación de políticas para aplicaciones de comunicación unificada incluyendo Skype for Business con video conferencia encriptada y alta experiencia de usuario en features como "desktop sharing" y llamadas de voz

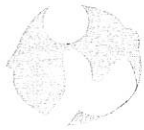
Soporta la tecnología Airmatch que gestiona las bandas de 2.4Ghz y 5ghz y optimiza de manera dinámica el ambiente RF incluyendo el ancho del canal, selección de canal y potencia de transmisión.

Ruckus no soporta in-built BLE beacon

- El Ap debe soportar una tecnología que permita a la wlan tener el control de la conectividad del usuario y del roaming para evitar el fenomeno de "sticky Client"
- Los Aps deben contar con zero touch provisioning para despliegues rápidos.
- Los Aps deben poder reconocer sin software adicional mas de 2000 aplicaciones y ofrecer políticas de control basado en dichas aplicaciones
- El licenciamiento podrá ser manejado de manera Local y no necesariamente bajo esquema de suscripción.
- Trusted Platform Module (TPM) para almacenamiento de llaves y credenciales
- Los Aps no deben depender de la conectividad de la cloud para las funciones del plano de Control.
- Se requiere garantía de por vida
- El fabricante debe estar posicionado como lider en el cuadrante mágico de Gartner.
- El Ap debe tener un sistema de firewall embebido para hacer filtrado de contenido web y un motor de reputación web
- Los Aps deben poder reconocer sin software adicional mas de 2000 aplicaciones y ofrecer políticas de control basado en dichas aplicaciones
- Los modelo de Aps ofertados deben ser capaces de trabajar sin controlador, con Controlador y en la nube .
- El fabricante de los Aps deben estar posicionados como #1 en el reporte de capacidades críticas de Gartner.
- Debe soportar integraciones mejoradas con Skype for Business y poder visualizar mediante software adicional metricas de calidad de llamada y un dashboard de comunicaciones unificadas deicadas.
- El Ap debe soportar una tecnología que permita a la wlan tener el control de la conectividad del usuario y del roaming para evitar el fenomeno de "sticky Client".

**ISSSTELEON**Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León**SERVICIOS PROFESIONALES DE RED WIRELESS**

Etapa	Actividades
Preparación	Creación de diagrama de ubicación y alcance de APs actuales
	Creación de diagrama de ubicación y alcance de APs nuevos
Instalación e interconexión de Infraestructura.	Instalación de controladora en ubicación de rack
	Energización interconexión de controladora
	Instalación y conexión de APs
Preconfiguración	Actualización de Firmware de las Controladora
	Preconfiguración de la controladora
	Configuración de dominio e IP de Administración
	Configuración SSID's
	Configuración Vlan's
	Aprovisionamiento de los Access Point
Configuración de control de acceso a la red	Preparación de controladora para integración con herramienta de control de acceso a la red
	Instalación de infraestructura virtual para la herramienta de control de acceso a la red
	Configuración de métodos de autenticación
	Integración de controladora y dispositivos con la herramienta de control de acceso a la red
Transferencia de conocimiento	Desarrollo y entrega de memoria técnica
Retiro de equipo	Inventario de equipo retirado
	Transportación y almacenamiento de equipo retirado
Soporte y Monitoreo	Soporte y monitoreo de infraestructura



ISSSTELEON

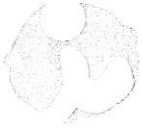
Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

RED ALÁMBRICA

SWITCH CORE

Cantidad	Características
4	<p>Stand-alone / Switch de capa 2, 3 avanzado</p> <p>Debe incluir:</p> <ul style="list-style-type: none"> • 48 puertos 10/100/1000 Base-T, Auto-MDIX , IEEE 802.3at PoE+ • Un módulo de cuatro (4) interfaces adicionales SFP+ • Doble fuente de poder • Módulos y cables para apilamiento <p>Capacidad de conectarse en stack con otros equipos de la misma serie:</p> <ul style="list-style-type: none"> • Los equipos que son parte del stack deberán comportarse como un único dispositivo virtual. • El stack debe ser capaz de crecer al menos hasta 10 equipos de la misma serie en topología ring o chain o 5 equipos full mesh • La conexión del stack debe soportar un BW de hasta 336 Gb/s. • PoE+ 1440W para este propósito <p>Al menos una (1) bahía de expansión para módulo de crecimiento.</p> <p>Modulos soportados:</p> <ul style="list-style-type: none"> • Cuatro (4) interfaces adicionales SFP+ • Dos (2) interfaz de 40G QSFP+ • Cuatro (4) interfaces 10G cobre 802.3bz • un (1) interfaz serial RJ45. • un (1) interfaz Ethernet para administración fuera de banda. • un (1) puertos micro USB." <p>Al menos vía:</p> <ul style="list-style-type: none"> • Línea serial de comandos (CLI) • Telnet • HTTP • SSH v2" <p>Soporte de múltiples configuraciones almacenadas en la memoria flash.</p> <p>Al menos:</p> <ul style="list-style-type: none"> • SNMP v1, v2c, v3





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- RMON
- sFlow (RFC 3176)

Soporte al menos de:

- IPv6 host
- Dual Stack

Soporte de monitoreo de puertos de entrada y salida.

Monitoreo calidad de servicio para trafico VoIP monitoreando parametros UDP jitter monitor quality of voice traffic using the UDP jitter and UDP jitter

64k direcciones MAC

- 4096 VLANs simultáneas.
- GVRP y MVRP."

Al menos:

- Detección de estado de canales.
- MACSEC

Soporte de tramas mayores a 1500 bytes

Al menos:

- MAC address learning limit por puerto."

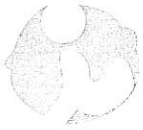
Al menos:

- IEEE 802.1Q.
- IEEE 802.1v.
- IEEE 802.1w.
- IEEE 802.1p.
- IEEE 802.1X.
- IEEE 802.1ad.
- IEEE 802.3u.
- IEEE 802.3x.
- IEEE 802.3ab.
- IEEE 802.3ad."

"Listas de control de acceso (ACL) en todos los puertos:

- ACLs por hardware que operen a la velocidad del cobre.
- Parámetros configurables de Capa 2, Capa 3 y Capa 4.
- ACL para IPv6.
- ACLs basadas en identidad de los usuarios, para facilitar la integración con sistemas de Control de Acceso a la red (NAC)"

LACP IEEE 802.3ad:



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Al menos 144 enlaces agregados.
- Al menos 8 enlaces por enlace agregado."

Soporte de:

- STP
- RSTP
- MSTP
- RPVST+
- STP Root guard
- STP BPDU port protection"

Limitación de tráfico de Broadcast.

Soporte al menos de:

- LLDP
- LLDP-MED"

Manejo de VLAN de voz.

Al menos:

- IPv4
- IPv6"

10000 (IPv4), 5000 (IPv6)

Al menos:

- Enrutamiento: estático.
- Enrutamiento Inter-Vlan.
- RIPv1, RIPv2, OSPF, BGP y PBR

Al menos:

- Enrutamiento: estático, RIPng y OSPFv3"

Soporte de:

- Protección dinámica de ARP."

Al menos:

- IGMP (Internet Group Management Protocol) v2/3
- MLD IPv6 "

Soporte para asignar direccionamiento IP dinámico mediante protocolo DHCP

Al menos 8 colas por puerto.

Soporte de:

- Rate limiting.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Priorización de tráfico.
- Priorización de tráfico en L4, basado en puertos TCP/UDP."

Al menos:

- 802.1p
- DSCP"

Limitación de ancho de banda

Soporte de:

- Autenticación por dirección MAC
- Radius
- Autenticación basada en WEB."

Al menos:

- VLAN privada
- VLAN isolation para tráfico no IP.
- DHCP protection.
- Dynamic ARP protection.
- IP multicast snooping."

Al menos:

Detección de fallas en el cable entre dos equipos (describir implementación).

Soporte al menos OpenFlow

Soporte para Aprovisionamiento desde la nube o on premises

Tunelización de tráfico hacia un Controlador Wireless para aplicar las mismas políticas de autenticación, acceso y seguridad que en la red inalámbrica

Integración con Sistema de Control de Acceso a la red para asignar políticas de autenticación, seguridad y QoS basada en el rol del usuario que se conecta

Debe traer todos los accesorios para montaje y operación en rack estándar de 19".

Soporte:

100 VAC a 240 VAC

50 Hz a 60 Hz."

Cumplir al menos:

EEE con IEEE 802.3az."

Al menos:

Rendimiento: 190,5 Mpps

Capacidad de conmutación: 320 Gbps.

 Matamoros 319 Pte.
Monterrey, N.L. México

 isssteleon.gob.mx

 81.2020.9400 / 81.2033.9000



**Gobierno de
Nuevo León**



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

En 1 Gbps menor a 2,8 us.
En 10 Gbps menor a 1,8 us.
En 40 Gbps menor a 1,5 us."
Al menos:

RAM: 2 GB

Buffer compartido: 13,5 MB.

El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.

Garantía de por vida válida durante el tiempo que el usuario final original sea propietario del producto. Debe incluir cobertura de los ventiladores y las fuentes de alimentación integrados para el periodo de garantía completo. Debe incluir soporte telefónico en horario laboral, reemplazo de hardware y actualizaciones de software para el periodo de garantía completo.



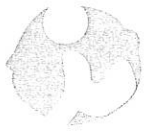
ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

SWITCH DE ACCESO TIPO 1

Cantidad	Características
4	<p>De configuración fija de 1 RU</p> <p>Debe incluir mínimo:</p> <ul style="list-style-type: none"> - 20 puertos 10/100/1000Base-T PoE+, Auto-MDIX - 4 puertos combo 10/100/1000Base-T PoE+ o 4 puertos 100/1000 SFP - Un (1) puerto consola de personalidad dual (RJ-45 o USB micro-B) - Un (1) puerto USB B para la carga y descarga de archivos - Un (1) puerto 100Base-T para la gestión fuera de banda <ul style="list-style-type: none"> • Considerar redundancia en fuentes y que tenga una capacidad exclusiva para PoE+ de 740 watts <p>Al menos una (1) bahía de expansión para crecimiento modular en interfaces de red. Los módulos deben permitir agregar por lo menos los siguientes tipos de puertos:</p> <ul style="list-style-type: none"> - Interfaces 10GE SFP+, mínimo cuatro (4); ó, - Interfaces 10GE Base-T 1/2.5/5/10 GbE, con soporte de 802.3bz, mínimo cuatro (4); ó, - Interfaces 40G QSFP+, mínimo una (1)." <p>"Capacidad de conectarse en stack con otros equipos de la misma familia:</p> <ul style="list-style-type: none"> - Los equipos que son parte del stack deberán comportarse como un único dispositivo virtual. - El stack debe ser capaz de crecer al menos hasta diez (10) equipos de la misma serie. - El stack es configurado utilizando un módulo dedicado para este propósito. - La conexión del stack debe tener un rendimiento de al menos 100Gbps utilizando puertos dedicados." <p>Al menos:</p> <ul style="list-style-type: none"> - Rendimiento: 95.2 Mpps - Capacidad de conmutación: 128 Gbps (228 Gbps incluyendo stacking). <p>Latencia:</p> <ul style="list-style-type: none"> - < 3.1 μs (64-byte packets) en 1000 Mb - < 3.4 μs (64-byte packets) en 10Gb" <p>Al menos:</p> <ul style="list-style-type: none"> - RAM: 1 GB - FLASH: 4 GB - Buffer compartido: 12.38 MB. <p>El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.</p> <ul style="list-style-type: none"> - Al menos 8 colas por puerto - Priorización de tráfico (IEEE 802.1p) - Priorización de tráfico en L4, basado en puertos TCP/UDP - CoS (Class of Service) en base a la dirección IP, al ToS (Type of Service) IP, al protocolo Layer 3, al





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

número de puerto TCP/UDP, al puerto de origen y a DiffServ

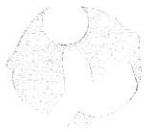
- Función rate limiting que permita establecer máximos obligados de ingreso por puerto y mínimos por puerto, por cola
- DSCP"
- " - Auto-MDIX en todos los puertos 10/100/1000
- Soporte de IEEE 802.3at y 802.3af
- LLDP-MED (Media Endpoint Discovery)
- IEEE 802.1AB LLDP (Link Layer Discovery Protocol)
- IPv6 host permite que los switches se administren en una red IPv6
- Dual stack (IPv4 y IPv6) transiciona de IPv4 a IPv6, soportando conectividad para ambos protocolos
- MLD snooping reenvía tráfico multicast IPv6 a la interface apropiada
- IPv6 ACL/QoS soporta ACL y QoS para tráfico de red IPv6
- El enrutamiento IPv6 soporta los protocolos estático y RIPng
- La seguridad proporciona RA guard, protección DHCPv6, dynamic IPv6 lockdown y ND snooping"
- " - Fuente de alimentación certificada en 80 PLUS Silver (aumenta la eficiencia y el ahorro de energía).
- Soporte para EEE (Energy-efficient Ethernet) reduce el consumo de potencia de conformidad con IEEE 802.3az"
- " - IGMP (Internet Group Management Protocol) v1, v2 y v3
- IGMP Snooping
- IGMP MLD
- IP Multicast routing: PIM Sparse y Dense (hasta 16 interfaces)"
- " - STP
- RSTP
- MSTP
- RPVST+
- STP Root guard
- STP BPDU port protection
- VRRP (Virtual Router Redundancy Protocol) para redes IPv4 y IPv6 (limitado a 128 VRs).
- LACP (IEEE 802.3ad link aggregation control protocol). Soporta hasta 128 troncales estáticas, dinámicas, o distribuidas activas (por stack) y cada uno de estas troncales hasta 8 puertos."
- " - SNMPv1, v2 y v3
- Manejo de al menos dos (2) imágenes de sistema operativo en modo primario y secundario.
- Se permite almacenar múltiples archivos de configuración en la memoria flash
- RMON, XRMON y sFlow
- UDLD (unidirectional link detection) "
- " - IEEE 802.1Q, Soporte de 4,094 VLAN Ids (2000 vlans en simultáneo)
- Paquetes jumbo de hasta 9,220 bytes
- IEEE 802.1v
- GVRP y MVRP
- Protocolo de encapsulación VxLAN (tunelización)
- MAC Address table: 32,678"



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- " - Enrutamiento estático
- ECMP
- RIP (Routing Information Protocol) proporciona enrutamiento RIPv1, RIPv2 y RIPv3
- OSPF v2 y v3 (solo acceso): Soporta un área OSPF y hasta 8 interfaces.
- PBR (Policy Based Routing) hasta 16 rutas de siguiente salto
- 2,000 rutas IPv4, 1,000 rutas IPv6 en hardware, 200 rutas OSPF, 256 estáticas y 10,000 rutas RIP "
- " - Configuración de políticas de plano de control que establecen rate limits que protegen a la sobrecarga del CPU originada por ataques DOS.
- Múltiples métodos de autenticación de usuarios:
 - IEEE 802.1X utiliza un supplicant IEEE 802.1X en el cliente, en conjunto con un servidor RADIUS para autenticar de conformidad con las normas de la industria.
 - La autenticación basada en Web proporciona un ambiente basado en navegador, similar a IEEE 802.1X, para autenticar clientes que no soportan el supplicant IEEE 802.1X.
 - Autenticación basada en MAC autentica al cliente con el servidor RADIUS basado en la dirección MAC del cliente.
- Flexibilidad de autenticación
 - Multiple IEEE 802.1X users per port proporciona autenticación de múltiples usuarios IEEE 802.1X por puerto y; evita que un usuario utilice la autenticación IEEE 802.1X de otro usuario.
 - Esquemas de autenticación concurrentes IEEE 802.1X, Web y MAC por cada switchport aceptarán hasta 32 sesiones de autenticaciones IEEE 802.1X, Web y MAC.
- Las ACLs, listas de control de acceso, proporcionan filtrado IP de Capa 3 basado en dirección IP/subred de origen/destino y número de puerto TCP/UDP de origen/destino.
- El filtrado de puertos de origen permite que únicamente puertos especificados se comuniquen entre sí.
- RADIUS/TACACS+ facilita la administración de seguridad de cada switch, utilizando un servidor de autenticación de contraseñas.
- Secure shell cifra todos los datos transmitidos para acceso remoto seguro a la CLI sobre redes IP.
- SSL (Secure Sockets Layer) cifra todo el tráfico HTTP, permitiendo acceso seguro al GUI de administración basada en navegador del switch.
- Port security permite acceso solamente a direcciones MAC especificadas, las cuales se pueden aprender o ser especificadas por el administrador.
- MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red.
- Secure FTP permite la transferencia segura de archivos hacia y desde el switch; protege contra descargas de archivos no deseadas o copiado no autorizado del archivo de configuración de un switch.
- Switch management logon security ayuda a asegurar el inicio de sesión de la CLI de un switch, requiriendo opcionalmente autenticación de RADIUS o TACACS+.
- Custom banner muestra la política de seguridad con los usuarios inician una sesión en el switch.
- STP BPDU port protection bloquea BPDUs (Bridge Protocol Data Units) en puertos que no requieren BPDUs, evitando ataques de BPDUs falsificadas.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- DHCP protection bloquea paquetes DHCP desde servidores DHCP no autorizados, evitando ataques denial-of-service.
- Dynamic ARP protection bloquea broadcasts ARP desde hosts no autorizados, evitando espionaje o robo de los datos de la red.
- STP root guard protege al puente raíz de ataques maliciosos o de errores de configuración.
- Identity-driven ACL permite la implementación de una política de seguridad de acceso altamente granular y flexible y asignación de VLANs específicas a cada usuario autenticado en la red.
- Per-port broadcast throttling configura el control de broadcasts selectivamente en puertos uplink con tráfico pesado.
- Private VLAN proporciona seguridad de la red restringiendo comunicaciones peer-to-peer para evitar una variedad de ataques maliciosos; típicamente, un switch port solo se puede comunicar con otros puertos en la misma comunidad y/o con un puerto uplink, sin importar la ID de la VLAN o de la dirección MAC de destino "

Soporte OpenFlow v1.3

Debe traer todos los accesorios para montaje y operación en rack estándar de 19".

Soporte:

- 100 VAC a 240 VAC
- 50 Hz a 60 Hz.

Debe incluir la capacidad de fuentes hot-swap redundantes, al menos dos (2)

El switch debe incluir dos (2) fuentes de poder.

Cumplir al menos:

- RoHS
- EEE con IEEE 802.3az.

Temperatura de operación:

- 0°C a 55°C (1500 m.s.n.m.)

Humedad relativa de operación:

- 15% a 95%"

- Soporta políticas unificadas, alámbricas e inalámbricas, a través del sistema de control de acceso a redes

- Configura el switch automáticamente para diferentes valores, como VLAN, CoS, potencia máxima PoE y prioridad PoE cuando se detecta un punto de acceso

- Define un conjunto de políticas basadas en switch en áreas como seguridad, autenticación y QoS.

- Proporciona un túnel asegurado para transportar tráfico de red en base a cada puerto a un Controlador. Las políticas de autenticación y de la red se aplicarán y se hará cumplir en el controlador.

- Aprovisionamiento sin intervención humana para simplificar la instalación de la infraestructura del switch o un proceso basado en DHCP con el software de administración.

Garantía limitada de por vida válida durante el tiempo que el usuario final original sea propietario del producto. Debe incluir cobertura de los ventiladores y las fuentes de alimentación integrados para el periodo de garantía completo. Debe incluir soporte telefónico en horario laboral, reemplazo de hardware y actualizaciones de software para el periodo de garantía completo.



SWITCH DE ACCESO TIPO 2

Cantidad	Características
2	<p>De configuración fija de 1 RU</p> <p>Debe incluir mínimo:</p> <ul style="list-style-type: none"> - 44 puertos 10/100/1000Base-T PoE+, Auto-MDIX - 4 puertos combo 10/100/1000Base-T PoE+ o 4 puertos 100/1000 SFP - Un (1) puerto consola de personalidad dual (RJ-45 o USB micro-B) - Un (1) puerto USB B para la carga y descarga de archivos - Un (1) puerto 100Base-T para la gestión fuera de banda <ul style="list-style-type: none"> • Considerar redundancia en fuentes y que tenga una capacidad exclusiva para PoE+ de 1440 watts <p>Al menos una (1) bahía de expansión para crecimiento modular en interfaces de red. Los módulos deben permitir agregar por lo menos los siguientes tipos de puertos:</p> <ul style="list-style-type: none"> - Interfaces 10GE SFP+, mínimo cuatro (4); ó, - Interfaces 10GE Base-T 1/2.5/5/10 GbE, con soporte de 802.3bz, mínimo cuatro (4); ó, - Interfaces 40G QSFP+, mínimo una (1)." <p>"Capacidad de conectarse en stack con otros equipos de la misma familia:</p> <ul style="list-style-type: none"> - Los equipos que son parte del stack deberán comportarse como un único dispositivo virtual. - El stack debe ser capaz de crecer al menos hasta diez (10) equipos de la misma serie. - El stack es configurado utilizando un módulo dedicado para este propósito. - La conexión del stack debe tener un rendimiento de al menos 100Gbps utilizando puertos dedicados." <p>Al menos:</p> <ul style="list-style-type: none"> - Rendimiento: 112 Mpps - Capacidad de conmutación: 176 Gbps (276 Gbps incluyendo stacking). <p>Latencia:</p> <ul style="list-style-type: none"> - < 3.1 μs (64-byte packets) en 1000 Mb - < 3.4 μs (64-byte packets) en 10Gb" <p>Al menos:</p> <ul style="list-style-type: none"> - RAM: 1 GB - FLASH: 4 GB - Buffer compartido: 12.38 MB. <p>El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.</p> <ul style="list-style-type: none"> - Al menos 8 colas por puerto - Priorización de tráfico (IEEE 802.1p) - Priorización de tráfico en L4, basado en puertos TCP/UDP - CoS (Class of Service) en base a la dirección IP, al ToS (Type of Service) IP, al protocolo Layer 3, al



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

número de puerto TCP/UDP, al puerto de origen y a DiffServ

- Función rate limiting que permita establecer máximos obligados de ingreso por puerto y mínimos por puerto, por cola
- DSCP"
- " - Auto-MDIX en todos los puertos 10/100/1000
- Soporte de IEEE 802.3at y 802.3af
- LLDP-MED (Media Endpoint Discovery)
- IEEE 802.1AB LLDP (Link Layer Discovery Protocol)
- IPv6 host permite que los switches se administren en una red IPv6
- Dual stack (IPv4 y IPv6) transiciona de IPv4 a IPv6, soportando conectividad para ambos protocolos
- MLD snooping reenvía tráfico multicast IPv6 a la interface apropiada
- IPv6 ACL/QoS soporta ACL y QoS para tráfico de red IPv6
- El enrutamiento IPv6 soporta los protocolos estático y RIPng
- La seguridad proporciona RA guard, protección DHCPv6, dynamic IPv6 lockdown y ND snooping"
- " - Fuente de alimentación certificada en 80 PLUS Silver (aumenta la eficiencia y el ahorro de energía).
- Soporte para EEE (Energy-efficient Ethernet) reduce el consumo de potencia de conformidad con IEEE 802.3az"
- " - IGMP (Internet Group Management Protocol) v1, v2 y v3
- IGMP Snooping
- IGMP MLD
- IP Multicast routing: PIM Sparse y Dense (hasta 16 interfaces)"
- " - STP
- RSTP
- MSTP
- RPVST+
- STP Root guard
- STP BPDU port protection
- VRRP (Virtual Router Redundancy Protocol) para redes IPv4 y IPv6 (limitado a 128 VRs).
- LACP (IEEE 802.3ad link aggregation control protocol). Soporta hasta 128 troncales estáticas, dinámicas, o distribuidas activas (por stack) y cada una de estas troncales hasta 8 puertos."
- " - SNMPv1, v2 y v3
- Manejo de al menos dos (2) imágenes de sistema operativo en modo primario y secundario.
- Se permite almacenar múltiples archivos de configuración en la memoria flash
- RMON, XRMON y sFlow
- UDLD (unidirectional link detection) "
- " - IEEE 802.1Q, Soporte de 4,094 VLAN Ids (2000 vlans en simultáneo)
- Paquetes jumbo de hasta 9,220 bytes
- IEEE 802.1v
- GVRP y MVRP
- Protocolo de encapsulación VxLAN (tunelización)
- MAC Address table: 32,678"



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- " - Enrutamiento estático
- ECMP
- RIP (Routing Information Protocol) proporciona enrutamiento RIPv1, RIPv2 y RIPng
- OSPF v2 y v3 (solo acceso): Soporta un área OSPF y hasta 8 interfaces.
- PBR (Policy Based Routing) hasta 16 rutas de siguiente salto
- 2,000 rutas IPv4, 1,000 rutas IPv6 en hardware, 200 rutas OSPF, 256 estáticas y 10,000 rutas RIP "
- " - Configuración de políticas de plano de control que establecen rate limits que protegen a la sobrecarga del CPU originada por ataques DOS.
- Múltiples métodos de autenticación de usuarios:
 - IEEE 802.1X utiliza un supplicant IEEE 802.1X en el cliente, en conjunto con un servidor RADIUS para autenticar de conformidad con las normas de la industria.
 - La autenticación basada en Web proporciona un ambiente basado en navegador, similar a IEEE 802.1X, para autenticar clientes que no soportan el supplicant IEEE 802.1X.
 - Autenticación basada en MAC autentica al cliente con el servidor RADIUS basado en la dirección MAC del cliente.
- Flexibilidad de autenticación
 - Multiple IEEE 802.1X users per port proporciona autenticación de múltiples usuarios IEEE 802.1X por puerto y; evita que un usuario utilice la autenticación IEEE 802.1X de otro usuario.
 - Esquemas de autenticación concurrentes IEEE 802.1X, Web y MAC por cada switchport aceptarán hasta 32 sesiones de autenticaciones IEEE 802.1X, Web y MAC.
- Las ACLs, listas de control de acceso, proporcionan filtrado IP de Capa 3 basado en dirección IP/subred de origen/destino y número de puerto TCP/UDP de origen/destino.
- El filtrado de puertos de origen permite que únicamente puertos especificados se comuniquen entre sí.
- RADIUS/TACACS+ facilita la administración de seguridad de cada switch, utilizando un servidor de autenticación de contraseñas.
- Secure shell cifra todos los datos transmitidos para acceso remoto seguro a la CLI sobre redes IP.
- SSL (Secure Sockets Layer) cifra todo el tráfico HTTP, permitiendo acceso seguro al GUI de administración basada en navegador del switch.
- Port security permite acceso solamente a direcciones MAC especificadas, las cuales se pueden aprender o ser especificadas por el administrador.
- MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red.
- Secure FTP permite la transferencia segura de archivos hacia y desde el switch; protege contra descargas de archivos no deseadas o copiado no autorizado del archivo de configuración de un switch.
- Switch management logon security ayuda a asegurar el inicio de sesión de la CLI de un switch, requiriendo opcionalmente autenticación de RADIUS o TACACS+.
- Custom banner muestra la política de seguridad con los usuarios inician una sesión en el switch.
- STP BPDU port protection bloquea BPDUs (Bridge Protocol Data Units) en puertos que no requieren BPDUs, evitando ataques de BPDUs falsificadas.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- DHCP protection bloquea paquetes DHCP desde servidores DHCP no autorizados, evitando ataques denial-of-service.
- Dynamic ARP protection bloquea broadcasts ARP desde hosts no autorizados, evitando espionaje o robo de los datos de la red.
- STP root guard protege al puente raíz de ataques maliciosos o de errores de configuración.
- Identity-driven ACL permite la implementación de una política de seguridad de acceso altamente granular y flexible y asignación de VLANs específicas a cada usuario autenticado en la red.
- Per-port broadcast throttling configura el control de broadcasts selectivamente en puertos uplink con tráfico pesado.
- Private VLAN proporciona seguridad de la red restringiendo comunicaciones peer- to-peer para evitar una variedad de ataques maliciosos; típicamente, un switch port solo se puede comunicar con otros puertos en la misma comunidad y/o con un puerto uplink, sin importar la ID de la VLAN o de la dirección MAC de destino "

Soporte OpenFlow v1.3

Debe traer todos los accesorios para montaje y operación en rack estándar de 19".

Soporte:

- 100 VAC a 240 VAC
- 50 Hz a 60 Hz.

Debe incluir la capacidad de fuentes hot-swap redundantes, al menos dos (2)

El switch debe incluir dos (2) fuentes de poder.

Cumplir al menos:

- RoHS
- EEE con IEEE 802.3az.

Temperatura de operación:

- 0°C a 55°C (1500 m.s.n.m.)

Humedad relativa de operación:

- 15% a 95%"

- Soporta políticas unificadas, alámbricas e inalámbricas, a través del sistema de control de acceso a redes


- Configura el switch automáticamente para diferentes valores, como VLAN, CoS, potencia máxima PoE y prioridad PoE cuando se detecta un punto de acceso

- Define un conjunto de políticas basadas en switch en áreas como seguridad, autenticación y QoS.

- Proporciona un túnel asegurado para transportar tráfico de red en base a cada puerto a un Controlador. Las políticas de autenticación y de la red se aplicarán y se hará cumplir en el controlador.

- Aprovisionamiento sin intervención humana para simplificar la instalación de la infraestructura del switch o un proceso basado en DHCP con el software de administración.

Garantía limitada de por vida válida durante el tiempo que el usuario final original sea propietario del producto. Debe incluir cobertura de los ventiladores y las fuentes de alimentación integrados para el periodo de garantía completo. Debe incluir soporte telefónico en horario laboral, reemplazo de hardware y actualizaciones de software para el periodo de garantía completo.

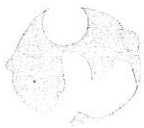
 Matamoros 319 Pte.
Monterrey, N.L. México

 isssteleon.gob.mx

 81.2020.9400 / 81.2033.9000



Gobierno de
Nuevo León

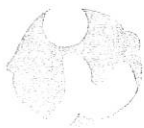


ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Servicios profesionales de red alámbrica

Etapa	Descripción
Configuración Switch Acceso	Solicitar "Show run config" de los switches actuales
	Realizar Script para switch nuevos
	Cargar configuración a los nuevos switch
	Actualiza Firmware
Configuración adicional	Revisión de la configuración
	Pruebas de funcionalidad en conjunto con el instituto
Instalación	Conexión y energización de equipos
	Pruebas de funcionalidad y comunicación
Transferencia de conocimiento	Desarrollo y entrega de memoria técnica
	Transferencia de conocimiento al instituto para 6 personas
	Transferencia oficial al área de soporte
Retiro de equipo	Inventario de equipo retirado
	Transportación y almacenamiento de equipo retirado
Soporte y Monitoreo	Soporte y monitoreo a infraestructura

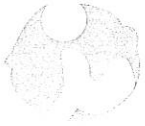
**ISSSTELEON**Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

TELEFONÍA

Telefonía para usuario

Cantidad	Características
115	<p>SOPORTE DE PROTOCOLO DE SEÑALIZACIÓN: Protocolo de inicio de sesión (SIP) COMPATIBLE CON LÍNEAS COMPLETAS: 2 líneas (registros SIP) LENGUAJE SOPORTADO: búlgaro, catalán, chino (simplificado y tradicional), croata, checo, danés, holandés, inglés americano, inglés, finlandés, francés, griego, español (España y Colombia), alemán, húngaro, italiano, japonés, coreano, noruego, polaco, portugués, ruso, eslovaco, sueco, esloveno y turco.</p> <p>MÚLTIPLES TONOS DE LLAMADA: Los teléfonos admiten tonos de llamada ajustables por el usuario</p> <p>OPCIONES DE CALIDAD DE SERVICIO (QOS): El teléfono es compatible con el Protocolo de descubrimiento de Cisco y los estándares 802.1Q / p, y se puede configurar con un encabezado VLAN 801.1Q que contiene las anulaciones de ID de VLAN configuradas por el ID de VLAN de administrador.</p> <p>SEGURIDAD:</p> <ul style="list-style-type: none"> • Autenticación 802.1X • Autenticación de dispositivo • Archivos de configuración encriptados • Autenticación de archivos • Autenticación de imágenes • Certificados instalados en fábrica • Cifrado de medios mediante SRTP con estándar de cifrado avanzado AES-128 o AES-256 • Cifrado de señalización mediante TLS con AES-128 o AES-256 <p>OPCIONES DE CONFIGURACIÓN: El usuario puede configurar la asignación de la dirección IP de forma estática o mediante el cliente DHCP</p> <p>DIMENSIONES: 8.2 x 6.7 x 1.5 pulgadas</p> <p>PESO: 456 g- excluyendo el pedestal, el auricular y el paquete</p> <p>DISPLAY: 6,4 cm, 240 x 120 píxeles</p> <p>INTERRUPTOR DE ETHERNET: Conexión Ethernet a través de dos puertos RJ-45; uno para la conexión LAN y el otro para una conexión de dispositivo Ethernet descendente, como una PC.</p> <p>COMPOSICIÓN DE LA CARCASA DEL TELÉFONO Y KEM: Plástico texturizado policarbonato acrilonitrilo butadieno estireno (ABS)</p>





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

REQUERIMIENTOS DE ENERGÍA: Dispositivos IEEE 802.3af PoE (clase 2) interoperables. Se requieren 5 V CC; se pueden suministrar localmente en el escritorio utilizando una de las fuentes de alimentación opcionales de CA a CC específicas del país.

CERTIFICACIONES Y CUMPLIMIENTO

CUMPLIMIENTO NORMATIVO:

- Marcas CE según las directivas 2014/30 / EU y 2014/35 / EU

SEGURIDAD

- UL 60950 segunda edición
- CAN/CSA-C22.2 No. 60950 segunda edición
- EN 60950 Segunda edición (incluidos A11 y A12)
- IEC 60950 Segunda edición (incluidos A11 y A12)
- AS / NZS 60950

EMC-EMISIONES

- 47CFR Parte 15 (CFR 47) Clase B
- AS/NZS CISPR32:2015 Clase B
- CISPR 32: 2015_COR1:2016 Clase B
- EN55032: 2015+AC:2016
- EN61000-3-2:2014 e IEC 61000-3-2:2014
- EN61000-3-3:2013 and IEC61000-3-3:2013
- VCCI Class B

EMC-INMUNIDAD

- EN55024
- CISPR24
- Armadillo Light

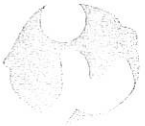
TELECOM

- FCC Part 68 HAC
- CS-03-HAC
- AS/ACIF S004
- AS/ACIF S040
- NZ PTC 220
- Estándares de la industria: TIA 810
- Estándares de la industria: IEEE 802.3 Ethernet, IEEE 802.3af

GARANTÍA: Garantía de hardware limitada de un año.

**Telefonía para ejecutivos**

Cantidad	Características
30	<p>Diseño ergonómico</p> <ul style="list-style-type: none"> El teléfono ofrece una interfaz fácil de usar y proporciona una experiencia de usuario similar a la telefonía tradicional. <p>Pantalla gráfica</p> <ul style="list-style-type: none"> El 800 × 480, color de 24 bits, 5 pulgadas. La pantalla WVGA proporciona acceso desplazable a funciones de llamada y aplicaciones XML basadas en texto. <p>Auricular</p> <ul style="list-style-type: none"> El teléfono es un teléfono de audio estándar con capacidad de banda ancha (se conecta a través de un puerto RJ-9). El cable en espiral estándar tiene un extremo personalizado para enrutar el cable oculto debajo del teléfono (la longitud del cable es de aproximadamente 55 cm [21 pulgadas] enrollado y hasta 183 cm extendido). El teléfono es compatible con audífonos (HAC) y cumple con los requisitos de volumen de la Comisión Federal de Comunicaciones (FCC) de la Ley de Estadounidenses con Discapacidades (ADA). Puede lograr los requisitos de sonoridad de la Sección 508 utilizando amplificadores de auricular en línea estándar de la industria, como los amplificadores Walker Equipment W-10 o CE-100. El teclado de marcación también cumple con la ADA. <p>Altavoz</p> <ul style="list-style-type: none"> Un altavoz de dúplex completo le brinda flexibilidad para realizar y recibir llamadas con manos libres. Para mayor seguridad, los tonos audibles de multifrecuencia de tono dual (DTMF) están enmascarados cuando se usa el modo de altavoz. <p>Auriculares analógicos</p> <ul style="list-style-type: none"> El conector para auriculares analógicos es un puerto de audio RJ-9 estándar con capacidad de banda ancha. <p>Puerto auxiliar</p> <ul style="list-style-type: none"> Puede utilizar un puerto auxiliar para admitir el control del conmutador de gancho electrónico con un auricular de otro fabricante conectado a él. <p>USB</p> <ul style="list-style-type: none"> Un puerto USB lateral mejora la facilidad de uso de la gestión de llamadas al habilitar auriculares con cable o inalámbricos, además de proporcionar una salida de potencia de hasta 500 mA a 5 V o 2,5 W para la carga de teléfonos inteligentes. <p>Interruptor de Eternet</p> <ul style="list-style-type: none"> Un conmutador Cisco Ethernet interno de 2 puertos permite una conexión directa a una red Ethernet 10/100 / 1000BASE-T (IEEE 802.3i / 802.3u / 802.3ab) a través de una interfaz RJ-45 con conectividad LAN única para ambos teléfonos. y una PC coubicada.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- El administrador del sistema puede designar VLAN independientes (IEEE 802.1Q) para la PC y el teléfono, lo que proporciona una mayor seguridad y confiabilidad del tráfico de voz y datos.

Bluetooth

- Se admite la tecnología Bluetooth 3.0 Enhanced Data Rate (EDR) Clase 1 (alcance de hasta 66 pies [20 m]).
- El perfil de manos libres (HFP) es compatible con conexiones de auriculares sin ataduras y comunicaciones de voz.
- El perfil de acceso a la agenda telefónica (PBAP) es compatible con el intercambio de objetos de la agenda telefónica entre dispositivos.

Teclas

El teléfono tiene las siguientes teclas:

- Teclas de línea
- Teclas suaves
- Teclas de retroceso y liberación
- Navegación de cuatro direcciones y teclas de selección
- Teclas Retener / Reanudar, Transferir y Conferencia
- Teclas de mensajería, aplicación y directorio
- Teclado estándar
- Tecla de alternancia de control de volumen
- Altavoz, auriculares y teclas de silencio

Indicador retroiluminado

- El teléfono admite indicadores retroiluminados para las teclas de ruta de audio (auricular, auricular y altavoz), tecla de selección, teclas de línea y mensaje en espera.

Bisel reemplazable

- El teléfono incluye un bisel negro; un bisel plateado opcional también se puede pedir por separado.

Pedestal de dos posiciones

- La pantalla es fácil de ver y los botones y teclas son fáciles de usar. El pedestal de dos posiciones admite ángulos de visión de 35 y 50 grados; Puede quitar el pedestal para montarlo en la pared, con los orificios de montaje ubicados en la base del teléfono.

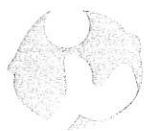
De pared

- Puede instalar el teléfono en una pared con un kit de montaje en pared opcional.

Módulo de expansión clave (KEM)

- El teléfono admite hasta dos KEM para expandirse desde botones de 5 o 10 líneas a botones de 61 o 66 líneas. Tiene la conveniencia de muchas marcaciones rápidas o funciones programables, o la necesidad de seguir la actividad de muchas líneas.

Seguridad física



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- El teléfono es compatible con el sistema antirrobo Kensington Security Slot (K-Slot).

Funciones de potencia

Alimentación por Ethernet (PoE) IEEE

- IEEE Power over Ethernet clase 3 para la versión de hardware anterior a V08, clase 4 para la versión de hardware V08 y superior. En el caso de PoE clase 3, un KEM se puede conectar y encender a través de PoE junto con el teléfono host 8851, en el caso de PoE clase 4, se pueden conectar y encender dos KEM a través de PoE junto con el teléfono host 8851.
- El teléfono es compatible con los conmutadores blades IEEE 802.3af y 802.3at y es compatible con el protocolo de descubrimiento de Cisco y el protocolo de descubrimiento de capa de enlace: alimentación por Ethernet (LLDP-PoE).
- Power Cube 4 del teléfono IP de Cisco
- Este cubo de energía opcional se utiliza como una fuente de alimentación de CA a CC (48 V) para implementaciones sin PoE. El uso del power cube 4 también requiere el uso de uno de los cables de CA correspondientes del país.

Soporte de control de llamadas

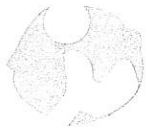
Gestor de Comunicaciones Unificadas

Agente de comunicaciones unificadas

Servicios profesionales de telefonía

Etapa	Descripción
Preparación de equipo	Documentar ubicación actual de los equipos de telefonía
	Crear diagrama de ubicación y detalles de telefonía
Envío	Traslado de equipos de telefonía a sitio
Instalación de equipos	Instalación de equipo de telefonía
	Configuración a red en equipos de telefonía
	Agregar equipos a servidor de telefonía
Retiro de equipos	Inventario de equipo retirado
	Transportación y almacenamiento de equipo retirado

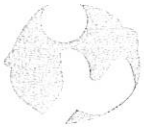




SEGURIDAD

Control de Acceso Firewall, VPN y Prevención de Intrusos

Cantidad	Características
1	<p>Equipo requerido</p> <p>La solución de Control de Acceso Firewall, VPN y Prevención de Intrusos deberá considerar 2 Equipos Firewall de siguiente generación modo alta disponibilidad (HA) activo/pasivo o activo/activo, los cuales deberán cumplir con al menos las siguientes características:</p> <ul style="list-style-type: none"> • El equipo deberá proveer los servicios de: Firewall, VPN y Prevención de Amenazas • Ser una solución en hardware (dispositivo o appliance). • Contar con la consola de administración integrada • Desempeño de firewall con control de aplicaciones: mínimo 5 Gbps • Desempeño de Prevención de Amenazas (IPS , Antivirus, Antispyware, Protección de Malware día cero habilitados simultáneamente): 2.4 Gbps • Desempeño de VPN: mínimo 2.7 Gbps • Sesiones soportadas al menos : 1,000,000 • Túneles IPSec VPN Soportados: 3,000 • Ruteadores virtuales soportados: 10 • Zonas de seguridad soportadas: 60 • Puertos de Red: mínimos: 10 x 10/100/1000, 4 x 1 GbE y 4 x 10 GbE en SFP+ • Capacidad de VPN client to site para 600 usuarios móviles con soporte de Windows 10, Windows 8, MacOS 10 en adelante, Android 4.0.3 en adelante y IOS 6.0 en adelante. • Capacidad de generar al menos 100 VPN Site to Site. • Interfaz de administración fuera de línea adicionales a las solicitadas a la inspección. • Al menos dos interfaces predefinidas para la funcionalidad de alta disponibilidad adicionales a las solicitadas a la inspección. • La solución deberá contar con certificación ICSA Labs y Nist USG v6 tipo NPD para modulo Firewall e IPS. <p>Funcionalidades de sensor para análisis de amenazas y protección tipo Firewall de siguiente generación integrado</p> <ul style="list-style-type: none"> • Capacidad de identificar y controlar aplicaciones independientemente del puerto, protocolo, cifrado SSL o SSH, o táctica evasiva. • Deberá permitir políticas de uso positivo de aplicaciones, es decir, permitir, negar, habilitar políticas por horario. • Deberá incluir la capacidad de actualización para identificar nuevas aplicaciones. • Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación,



por categoría de aplicación, subcategoría de aplicación, tecnología y factor de riesgo.

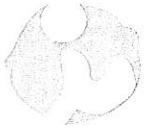
- Deberá incluir la capacidad de creación de políticas basadas en nombre de usuario, grupo de usuario o dirección IP.
- Deberá permitir definir instancias virtuales dentro del firewall físico (firewalls virtuales).
- La tecnología de identificación de aplicaciones deberá estar habilitada por default (motor de inspección base) sin necesidad de habilitar funcionalidades adicionales.
- Deberá incluir herramientas gráficas que permitan tener la vista de aplicaciones que fluyen a través del firewall.
- Deberá identificar usuarios a través de integración con Active Directory, LDAP, eDirectory, Syslog Listener y XML-API.
- Deberá realizar políticas que permitan el control de aplicaciones, usuarios y contenido mediante una sola política.
- Deberá incluir mecanismos de protección contra paquetes fragmentados.
- Deberá incluir mecanismos de protección contra ataques de reconocimiento (escaneo).
- La identificación de aplicaciones deberá realizarse tan pronto la información llegue al Firewall, sin depender de tecnología de Firewall de estado.
- Deberá permitir el manejo de aplicaciones no identificadas, ya sea creando políticas para su inspección y control, además de permitir, desarrollar firmas para la identificación de aplicaciones desconocidas.
- Para garantizar el acceso de la plataforma de seguridad, incluso en períodos de alta cantidad de tráfico, la solución deberá contar con procesadores y memorias dedicados a un plano de control (administración del equipo) y deberá integrar procesadores y memorias separados y dedicados específicamente al plano de datos (inspección de usuarios) dentro del mismo dispositivo.
- Para aquellos usuarios que no estén integrados al directorio activo de IsssteLeon, por ejemplo, red invitados, deberá permitir la integración con soluciones de autenticación a través de un XML-API configurable. Para esto, deberá incluir el soporte de identificación de usuarios que utilicen direcciones IPv4 e IPv6.

Deberá incluir, sin costo ni hardware adicional, tecnología que permita descifrar el tráfico SSL y SSH

En relación a este punto, deberá permitir

- a) Bloqueo de sesiones SSL con certificados expirados.
- b) Bloqueo de sesiones SSL con certificados no confiables
- c) Bloqueo de sesiones SSL y SSH para mecanismos de cifrado no soportados

- Deberá incluir la capacidad de limitar la transferencia de archivos no autorizados.
- Deberá permitir el control de transferencia de archivos por aplicación, identificando más de 30 tipos de archivos (DLL, ZIP, EXE, etc.)
- Deberá incluir sin costo y en el mismo equipo tecnología de identificación de malware moderno contando con la detección de comportamientos maliciosos, detección de tácticas



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

de evasión y aprendizaje de máquina (machine learning).

- Deberá incluir la capacidad de análisis malware día cero de archivos ejecutando archivos desconocidos en un SandBox virtualizado.
- Deberá incluir la inspección de malware en día cero para documentos del tipo: Ejecutables (EXE), DLL, Office (Word, Excel, Powerpoint), PDF, APK, JAR (Java); MacOS y Adobe Flash.

Deberá incluir mecanismos para establecer redes privadas virtuales (VPN) IPsec Site to Site con las siguientes características:

- Cifrado 3DES, AES 128, 192 y 256 bits.
- Autenticación MD5, SHA1, SHA256, SHA384, SHA512.
- El firewall debe tener la capacidad de operar en los siguientes modos de manera simultánea mediante el uso de sus interfaces físicas modo sniffer (monitoreo y análisis del tráfico de la red), capa 2 (L2) y Capa 3 (L3)

a) Modo sniffer: Para inspección vía un puerto espejo del tráfico de datos de la red.

b) Modo Capa-2 (L2): Para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación.

c) Modo Capa-3 (L3): Para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación. Con capacidad de generar ruteo virtual para al menos 10 ruteadores virtuales y manejo de tráfico entre diferentes zonas de seguridad y sub-redes, soportando al menos 60 zonas de seguridad.

El equipo deberá contar con soporte para los siguientes servicios:

- Soporte de 4,000 redes virtuales VLANs 802.1q,
- Traducción de direcciones de red (NAT) por fuente y destino, por direcciones IP dinámicas y pool de puertos.
- Traducción de direcciones IPv6 NAT64
- Al menos 10,000 direcciones en tabla de ruteo en IPv4
- Al menos 10,000 direcciones en tabla de ruteo en IPv6
- PPPoE

- Enrutamiento BGP, OSPFv3 y RIP2
- Soporte de enrutamiento con base en políticas
- Soporte de enrutamiento multicast
- PIM-SM o PIM-SSM
- IGMP v1, v2, v3
- BDF (Bidirectional Forwarding Detection)
- DHCP server y DHCP Relay
- El equipo deberá incluir fuentes de poder redundante.
- El equipo deberá incluir fuentes de poder redundante.

Matamoros 319 Pte.
Monterrey, N.L. México

isssteleon.gob.mx

81.2020.9400 / 81.2033.9000



Gobierno de
Nuevo León



- En caso de aplicaciones desconocidas, deberá contar con un editor de firmas.
- Deberá incluir control de tráfico IPv4 e IPv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido IPv6, debe ser soportado en interfaces trabajando en Capa 2 (L2) y Capa 3 (L3).
- Deberá soportar SLAAC en interfaces de IPv6.
- Deberá soportar alta disponibilidad en esquemas activo-activo y activo-pasivo.
- Activar alta disponibilidad con base en el estado de interfaz o Monitoreo de conectividad para activar alta disponibilidad. Deberá soportar geo localización para la creación de políticas con base en la región/país o zona geográfica.

Deberá incluir características para la definición de criterios y complejidad mínima para contraseña y soportar al menos los siguientes criterios:

- Longitud mínima de contraseña
- Número mínimo de mayúsculas
- Número mínimo de minúsculas
- Número mínimo de caracteres numéricos
- Número mínimo de caracteres no alfanuméricos
- Prevenir el uso de contraseñas previas
- Prevenir el uso de nombre de usuario como contraseña
- Advertencia de expiración de contraseña
- Forzar el cambio de contraseña en un periodo específico

Deberá crear listas dinámicas a partir del registro de algún evento en el log de seguridad, obteniendo leer de forma dinámica el origen y/o destino IP para asociarlo a una etiqueta dinámica, por ejemplo, a partir del registro de un evento tipo malware asociará a la dirección IP víctima de forma automática a una etiqueta dinámica de direcciones IPs, donde se asociaran a una política restrictiva de seguridad para impedir conexiones subsecuentes a dicho evento.

Soporte a la creación de políticas de autenticación cuando el destino sea de altamente restringido sin la necesidad de instalar algún cliente en el endpoint, es decir de forma transparente, solicitará automáticamente al usuario final autenticación tipo Multifactor (MFA), evitando el acceso a servidores únicamente por usuario y contraseña. Este módulo deberá ser compatible al menos con PingID, Duo y Okta.

Administración del equipo y reporte

La administración de políticas y objetos deberá realizarse a través de interface gráfica embebida en el equipo Firewall basada en Web y Administración del equipo a través de CLI (ssh y puerto consola) y adicionalmente vía una consola de administración centralizada basada en un appliance con capacidad de almacenamiento de al menos 4 TB en disco en RAID1



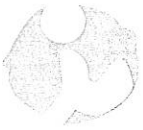
- Deberá soportar Syslog y SNMPv3.
- Deberá desplegar un resumen gráfico de aplicaciones y amenazas.
- Deberá desplegar las aplicaciones con el mayor número de sesiones o Deberá desplegar las aplicaciones con el mayor factor de riesgo.
- Deberá permitir crear de manera automática búsquedas a la base de datos de registros a partir de la navegación de uso principal de aplicaciones.

Deberá permitir la generación de reportes de actividad de usuarios, con base en el tiempo, los cuales deberán incluir:

- Listado de aplicaciones utilizadas.
- Categoría y subcategoría de aplicaciones utilizadas.
- Envío de reportes por correo de manera automática.
- Generación de reportes personalizados permitiendo seleccionar la base de datos de registro a utilizar, así como el periodo de tiempo a emplear en el reporte incluyendo la capacidad de proporcionar un resumen gráfico.
- Deberá contar con la funcionalidad para exportar logs de tráfico y amenazas.
- Deberá permitir la creación de reportes personalizados.
- Deberá contar con herramientas para crear filtros de monitoreo de las sesiones en el Firewall, por aplicación y por origen y/o destino.
- Deberá desplegar un resumen gráfico de aplicaciones y amenazas.
- Deberá desplegar las aplicaciones con el mayor número de sesiones o Deberá desplegar las aplicaciones con el mayor factor de riesgo.
- Deberá permitir crear de manera automática búsquedas a la base de datos de registros a partir de la navegación de uso principal de aplicaciones.
- Deberá permitir la generación de reportes de actividad de usuarios, con base en el tiempo, los cuales deberán incluir:
 - Listado de aplicaciones utilizadas.
 - Categoría y subcategoría de aplicaciones utilizadas.
 - Envío de reportes por correo de manera automática.
 - Generación de reportes personalizados permitiendo seleccionar la base de datos de registro a utilizar, así como el periodo de tiempo a emplear en el reporte incluyendo la capacidad de proporcionar un resumen gráfico.
 - Deberá contar con la funcionalidad para exportar logs de tráfico y amenazas.
 - Deberá permitir la creación de reportes personalizados.
 - Deberá contar con herramientas para crear filtros de monitoreo de las sesiones en el Firewall, por aplicación y por origen y/o destino.

Deberá proporcionar como mínimo los siguientes tipos de reportes:

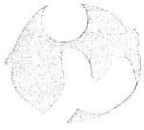
- Utilización en bytes por aplicación.
- Número de sesiones por aplicación.
- Comparativo de utilización de aplicaciones (por consumo o por sesiones) con respecto a periodos anteriores, considerando al menos 24 horas antes y hasta 30 días.



- Principales aplicaciones circulando a través del Firewall.
- Principales direcciones IP (origen o destino) por aplicación.
- Reporte de actividades específicas por usuario.
- Origen o destino del tráfico por aplicación-usuario.
- Deberá permitir la creación de expresiones regulares para hacer búsquedas o queries.
- Deberá permitir la muestra de los registros del Firewall y amenazas del IPS con base en la información de contexto que se esté mostrando en ese momento en la herramienta de monitoreo.
- Deberá permitir generar reportes de aplicaciones tipo SaaS.
- Deberá incluir funcionalidades de prevención de robo de credenciales, detectando el momento en que los usuarios envían credenciales corporativas válidas a un sitio. Este procedimiento puede realizarse de acuerdo a un grupo de usuarios de LDAP e identificación de usuarios activos en la red.

Funcionalidades de prevención de amenazas

- El equipamiento deberá tener un rendimiento mínimo de 2.4 Gbps en modo de Threat Prevention - con funciones de IPS encendido.
- La licencia de IPS deberá permitir la protección contra amenazas de virus, spyware y otras clases de malware sin costo adicional.
- Deberá incluir también, dentro del mismo equipo, el control de transferencia de archivos y bloqueo de archivos por tipo.
- Deberá incluir la capacidad de creación de políticas de inspección basadas en nombre de aplicación, categoría de aplicación y tipo de tecnología.
- Deberá incluir la capacidad de creación de políticas de inspección basadas en nombre de usuario, grupos de usuarios o Dirección IP.
- Deberá permitir crear firmas para identificar las aplicaciones desarrolladas por la entidad.
- Deberá permitir la personalización de firmas "phone home" de spyware.
- La solución deberá permitir el diseño de firmas de vulnerabilidades.
- La solución deberá permitir la detección y bloqueo de amenazas sobre puertos no estándares, tomando como criterio la política de seguridad definida con base en aplicaciones.
- Deberá realizar análisis bidireccionales de paquetes SSL/TLS/SSH e identificación de aplicaciones que viajen en el túnel SSL para detener el empleo de aplicaciones que utilizan tácticas evasivas para viajar de modo cifrado, tales como: PROXIES-SSL, ULTRASURF, SKYPE, y ataques mediante el puerto 443. Este análisis deberá poderse realizar, aunque la sesión SSL no utilice el puerto 443.
- Deberá incluir la funcionalidad de protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en Internet y bloqueo de archivos por tipo.
- Deberá permitir la protección contra descargas involuntarias de archivos ejecutables maliciosos al usar el protocolo HTTP.
- Deberá permitir la inspección en archivos comprimidos que usan algoritmo deflate (zip,



gzip, etc.)

- La actualización de firmas de ataques deberá poder realizarse de manera diaria y semanal.

Los dispositivos deberán tener los siguientes mecanismos y realizar la detección y protección de ataques de Red como:

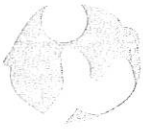
- Análisis basado en protocolo
- Protección contra anomalías basadas en protocolo para detectar uso de protocolos sin cumplimiento de RFC.
- Identificación de patrones que detecte ataques a través de más de un paquete, tomando en cuenta elementos como el orden y secuencia de arribo
- Análisis heurísticos que detecten paquetes anómalos y patrones de tráfico como escaneo de puertos y Host Sweeps.
- Bloqueo de paquetes malformados o inválidos, defragmentación IP, re ensamble TCP para protección contra métodos de ofuscación y evasión.
- Protección contra malformación de paquetes.
- Análisis heurístico.
- Deberá permitir el diseño de firmas de vulnerabilidades.
- Deberá soportar firmas basadas en DNS para detectar búsquedas específicas de DNS hacia nombres de equipo que han sido asociados con malware. La solución deberá permitir habilitar/deshabilitar las firmas de DNS para crear excepciones.

Funcionalidades de filtrado de contenido

- Deberá poder ofrecer la opción de usar ya sea una base de datos de URLs de terceros o la desarrollada por el fabricante.
- La plataforma propuesta deberá soportar la funcionalidad de Filtrado de Contenido sin necesidad de añadir hardware, procesadores ni memoria extra.
- Deberá contar con al menos 60 categorías predefinidas.
- La plataforma propuesta deberá soportar la funcionalidad de descifrado SSL sin necesidad de añadir hardware, procesadores ni memoria extra
- La solución de filtrado de contenido deberá incluir la capacidad de creación de políticas de filtrado en base a nombre de usuario o grupo de usuarios definidos en el directorio de la convocante.

Deberá permitir configurar acciones como:

- Permitir, el acceso a la página web
- Bloquear, el acceso a una página web
- Cuando un usuario accese una página que no cumpla con las políticas definidas, mostrando una página de advertencia y mostrando un botón para continuar.
- Opción de override: para solicitarle al usuario una contraseña que le permita continuar navegando



Deberá bloquear el uso de aplicaciones tipo Proxy, ToR y Ultrasurf

- Además de las funciones de bloqueo, el motor de URL deberá permitir usar las categorías identificadas para definir criterios de descricción de SSL.
- Deberá permitir prevenir la carga/descarga de archivos para categorías que representen alto riesgo.
- Deberá permitir a los administradores del sistema, crear categorías personalizadas
- Deberá permitir obtener reportes de uso de actividad por usuario, que muestren las aplicaciones utilizadas, las categorías URL visitadas, y un reporte detallado de los URLs visitados en un periodo de tiempo específico.
- Deberá contar con una variedad de al menos 30 reportes que desplieguen las categorías URL visitadas, los sitios web visitados, los usuarios que fueron bloqueados, los sitios que fueron bloqueados, etc.
- Deberá permitir la creación de búsquedas en los logs a través de expresiones regulares. El resultado de la búsqueda de registros deberá poder guardarse y exportarse.
- Los registros de los accesos a las páginas deberán poder enviarse a un servidor de logs.

Funcionalidades de VPNs

- La solución deberá contar con capacidades la Red Privada Virtual (por sus siglas en Ingles VPNs) para el envío y recepción de información de forma cifrada, basada en el estándar IPsec.
- Deberá contar con la funcionalidad de establecer túneles seguros sitio a sitio con funcionalidades mínimas de cifrado AES 256, AES 192, AES 128, 3DES y DES.
- Los túneles de VPN deberán contar con soporte de llaves Diffie Hellman mínimos de grupos 1,2,5, 14, 19 y 20. Y métodos de autenticación MD5, SHA1, SHA256, SHA384 y SHA512.
- Soporte de distribución de ruteo dinámico y estático en túneles de VPN, para la conectividad de sitios remotos.
- Soporte de IKEv1 y IKEv2
- Soporte de DPD (Dead Peer Detection)
- Soporte de VPNs en modo Main Mode , aggressive Mode y auto-detección.
- La solución deberá contar con túneles cliente a sitio con funcionalidad de completar la VPN via IPsec en dado caso que no sea posible se auto-conectará vía SSL
- La solución deberá contar al menos con 1,000 túneles simultaneos sitio a sito y al menos 600 túneles cliente a sitio soportando Windows, MacOS, Google ChromeOS, Android y IOS.
- La solución de VPNs cliente a sitio deberá contar con la funcionalidad de revisar el estado del host, es decir, si el Firewall personal se encuentra activo, el estado de la solución de antimalware, parches del sistema operativo y algunas condiciones como entradas en el registry, para permitir no el acceso de uso en políticas de aplicaciones a través del Firewall



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

	de siguiente generación.
--	--------------------------

Prevención y detección de ataques de Endpoint

Cantidad	Características
	<p>Identificación de ataques de exploits:</p> <p>Detección del mecanismo de identificación de propiedades de un sistema por parte de un exploit kit (técnica conocida como exploit kit fingerprinting) sin necesidad de utilizar firmas, patrones o heurísticas.</p> <p>Prevención contra exploits</p> <ul style="list-style-type: none"> • Detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo, para sistemas Microsoft Windows. • Mitigación de vulnerabilidades conocidas, desconocidas y día cero. • Soporta técnicas de explotación de vulnerabilidades distintas, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, etc) • Protección de aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box". • Entre las aplicaciones predeterminadas se encuentran: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, varias versiones de Flash Player, Microsoft Silverlight entre otras. • Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación, incluyendo aquellas desarrolladas internamente. • Capacidad de crear un snapshot de forma automática de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar datos forenses sobre el evento. • Es posible configurar perfiles de protección en modo de prevención o monitoreo. • Terminación del proceso en el cual fue identificado el intento de ejecución de una técnica de explotación. • Prevención de técnicas de explotación que utilizan Dylib-Hijacking para Mac OS.





ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Prevención de técnicas de explotación que utilizan ROP para Mac OS.
- Prevención de técnicas de explotación que utilizan JIT para Mac OS.
- Prevención de técnicas de explotación que buscan secuestrar el flujo de control de un proceso mediante el monitoreo de intentos de enumeración de la distribución de la memoria para sistemas operativos Linux.
- Prevención de técnicas de explotación que buscan redireccionar los flujos de entrada y salida estándares a sockets de red para sistemas operativos Linux.
- Prevención de técnicas de explotación que utilizan return-oriented programming para sistemas operativos Linux.
- Prevención del uso de ciertas áreas de memoria que son usualmente utilizadas para almacenar el payload de un ataque utilizando técnicas de heap spray, para sistemas operativos Linux
- Cuenta con políticas de prevención de técnicas de explotación, así como de compatibilidad, de manera predeterminada, con la finalidad de mejorar la experiencia del usuario final y reducir la creación de falsos positivos.
- Capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.

Identificación de ataques post-explotación.

- Identificación y prevención de intentos de escalación de privilegios a nivel de Kerne. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux.
- Detección y terminación de comportamientos considerados como maliciosos mediante el análisis continuo de los eventos que sucedan en un endpoint. Esta detección debe considerar varios eventos y no sólo un evento para poder proporcionar un veredicto de la actividad. La detección debe utilizar varias reglas preconfiguradas, las cuales deben de tener la capacidad de analizar varios eventos y no sólo un evento.
- La protección no debe de depender de una conexión a la consola de administración.

Prevención contra malware.

- Creación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.
- Envío de ejecutables desconocidos para su análisis en un sandbox ubicado en la nube, con la finalidad de determinar si son maliciosos o benignos. Esta protección debe estar disponible para sistemas operativos Windows, Mac, Linux y Android.
- Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Prevención de malware conocido y desconocido.

- Utiliza un modelo matemático generado a partir de aprendizaje de máquina para comparar aproximadamente 300 características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows y Mac.
- Prevención de ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas.
- Capacidad de identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa.
- Capacidad de proporcionar protección contra malware sin necesidad de tener una conexión a la consola.
- Capacidad de proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas.
- Es posible configurar las políticas en modo de prevención o monitoreo.

Escaneo de archivos ejecutables.

- Permite realizar el escaneo de archivos ejecutables sin la necesidad de firmas.
- Permite programar el escaneo de archivos de manera semanal o mensual.
- Permite definir el día y la hora en la cual se iniciará el escaneo.
- El consumo de recursos al momento de realizar el escaneo no debe de impactar en la experiencia del usuario.
- Permite habilitar el escaneo de dispositivos de almacenamiento removible.
- Permite crear listas blancas de carpetas para que sean excluidas del proceso de escaneo.
- Permite poner en cuarentena los archivos identificados como maliciosos, si es que la política está configurada de esta manera.

Protección contra el robo de contraseñas.

- Proporciona una protección predeterminada en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz.

Restricciones de ejecución.

- Restricciones de ejecución de archivos a partir de cierta carpeta.
- Restricciones de ejecución de archivos a partir de recursos compartidos.



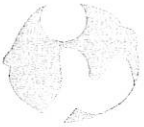
- Restricciones de ejecución de archivos a partir de dispositivos USB o CD/DVD.
- Restricciones granulares de ejecución de procesos hijo definiendo el proceso padre y los procesos hijo a restringir o permitir.
- Restricciones granulares de ejecución de procesos hijo sin necesidad de contar con una conexión a la consola de administración.
- Cuenta con políticas de restricción de creación de procesos hijo configuradas de manera predeterminada.
- Capacidad de crear excepciones para permitir la ejecución de archivos a partir de ciertas carpetas.
- Capacidad de crear excepciones para permitir la creación de procesos hijo.
- Capacidad de crear excepciones para permitir la ejecución de archivos a partir de carpetas dentro de los dispositivos de almacenamiento removibles.
- Es posible configurar perfiles en modo de prevención o monitoreo.

Acciones de respuesta

- La consola permite aislar un endpoint para que sólo exista comunicación con ella.
- La consola permite definir otros dispositivos a los cuales se pueda conectar el endpoint, además de la consola.
- La consola permite poner en cuarentena, bajo demanda, archivos maliciosos que hayan sido detectados o reportados, pero no bloqueados por las políticas de prevención definidas.
- La consola permite terminar bajo demanda los procesos que hayan sido reportados o detectados, pero no bloqueados, por las políticas de prevención definidas.

Administración y revisión de eventos.

- Administración de políticas centralizada, vía una consola web.
- La consola distingue los eventos de prevención y notificación, y para cada uno de estos dos grupos clasifica los eventos en intentos de ejecución de exploits, intentos de ejecución de malware, violaciones a las políticas de restricciones e intentos de violación a las políticas de restricción.
- La consola puede clasificar los eventos en tres niveles de acuerdo a su severidad: bajo, medio y alto.
- La consola de administración identifica claramente los eventos que han sido reportados y/o bloqueados y aquellos que han sido detectados.
- Capacidad para clasificar el estado de las alertas en tres distintas categorías: nuevas, investigando y cerradas.
- La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Permite la actualización y desinstalación del agente a partir de la consola.
- Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
- Cuenta con integración con Active Directory para la gestión de computadoras y configuración de políticas.
- Cuenta con la capacidad de poder crear perfiles granulares.
- Cuenta con la capacidad de poder crear políticas basadas en los perfiles creados.
- Cuenta con la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizaciones de Active Directory
- Cuenta con la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica.
- La alimentación dinámica de los grupos virtuales podrá ser de forma estática y dinámica, siendo posible configurar para la forma dinámica el nombre de la computadora, el dominio o grupo de trabajo y dirección IP
- Cada evento de prevención o notificación cuenta con información básica como tipo de evento, módulo que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención, horario y fecha del evento, información forense (en caso de estar disponible).
- La consola deberá de ser proporcionada bajo un esquema software as a service.
- Cuenta con un dashboard donde se muestran los eventos de seguridad que no han sido atendidos (clasificados de acuerdo a su criticidad en alta, media y baja), la cantidad de endpoints que tienen instalado el agente (clasificados por su plataforma), la cantidad de licencias disponibles y la versión del agente.
- Cuenta con un dashboard donde se describen las características de los eventos de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle el evento de seguridad, incluyendo los reportes generados por el agente.
- Integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas.
- Debe permitir gestionar las excepciones en una pantalla específica, clasificándolas por excepciones de ejecución de archivos, excepciones a ejecución de procesos (exploits y procesos hijo) y excepciones de soporte.

Características del agente



- Agente con un footprint mínimo que no impacte la experiencia de usuario.
- Poco almacenamiento en disco debido a que no utiliza firmas, patrones y/o heurísticas. Soporte para las siguientes versiones de sistemas operativos:
 - Windows XP* (32-bit, SP3 o posterior), Windows Vista (32-bit, 64-bit, SP1 o posterior; FIPS mode), Windows 7 (32-bit, 64-bit, RTM & SP1; excepto Home), Windows Embedded 7 (Standard & POSReady), Windows 8* (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit; FIPS mode), Windows Embedded 8.1 Pro, Windows 10 Pro (32-bit and 64-bit), Windows 10 Enterprise LTSC, Windows 10 Education, Windows 10 Update 1809, Windows Server 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter.
 - OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14.
 - CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16

Soporte para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V.

Capacidad para configurar la captura de datos que serán enviados a la nube para su almacenamiento, procesamiento y análisis en una consola de detección y respuesta a incidentes.

Gestión de usuarios

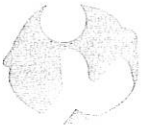
- La consola permite la gestión de usuarios mediante roles.
- La consola cuenta con los siguientes roles preconfigurados: super Admin, viewer, security Admin, IT Admin, No Access, Deployment Admin.
- Los roles preconfigurados tienen las siguientes características:
 - **Super Admin.** Cuenta con todos los permisos, puede cambiar los roles asignados a otros usuarios, pero no puede cambiar su propio rol.
 - **Viewer.** Cuenta con acceso de sólo lectura. Puede exportar datos.
 - **Security Admin.** Cuenta con permisos para gestionar los perfiles, políticas y eventos de seguridad. Tiene acceso de sólo lectura a las tareas de despliegue.
 - **IT Admin.** Cuenta con acceso a las tareas de despliegue. Tiene acceso de sólo lectura a los perfiles, políticas y eventos de seguridad.

**ISSSTELEON**Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

	<ul style="list-style-type: none"> - No Access. Sin acceso. - Deployment Admin. Cuenta con acceso a las tareas de despliegue, pero no tiene acceso a los perfiles, políticas y eventos de seguridad.
--	--

Servicios profesionales de seguridad

Etapa	Descripción
Instalación	Instalar equipo en rack
	Activación de licencias en portal de soporte del fabricante
Preconfiguración	Actualizar de consolas
	Actualizar de las firmas de Apps & Threats.
	Actualizar de las firmas de Antivirus.
	Actualizar de las firmas de amenazas avanzadas
	Actualizar de base de datos de URL filtering.
	Configurar User-ID para la adquisición de usuarios a través de Active Directory - Log monitoring
	Configurar la infraestructura de PKI para la interceptación de SSL
Despliegue	Migración de políticas de seguridad y perfiles de seguridad (As-is)
	Ejecución
	Configurar perfil de Zone Protection por cada zona definida.
	Configurar perfil de Antivirus por cada flujo
	Configurar perfiles de AntiSpyware por cada flujo
	Configurar perfiles de IPS por cada flujo
	Configurar perfil de bloqueo de archivos por cada flujo
	Configurar perfil de ataques desconocidos por cada flujo
	Configurar perfil de URL filtering para la navegación
Ejecución	Realizar ventana de mantenimiento para sustituir los equipos firewall
Post-despliegue	Verificar el CPU, Sesiones, interfaces.
	Verificar que los dynamic updates están trabajando automáticamente.
	Verificar si los archivos pasando por el equipo están siendo inspeccionados por la nube de sandbox.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

	Verificar la generación de alertas de IPS, Antivirus y AntiSpyware.
	Verificar la generación de alertas sobre archivos.
	Realizar documento de Memoria Técnica del proyecto.
	Realizar reporte auditoria de mejores practicas de la plataforma de firewalls de siguiente generacion del sitio principal.
Entrega	Realizar transferencia de conocimiento del proyecto.
	Firma de documento de entrega de servicios y cierre del proyecto
Soporte y Monitoreo	Monitoreo 24/7 de estado de salud de Firewall
	Envío de reportes de ataques por correo electrónico
	Soporte a firewall
Etapa	Descripción
Preconfiguración	Definir método de distribución de agente
Implementación	Instalación y activación de agentes de roteccion y respuesta de amenazas avanzadas para endpoints
Administración	Configuración inicial de consola de administración
	Creación de grupos de Endpoints
	Creación de perfiles de protección de Endpoints
	Crear perfiles de actualización de Endpoint
	Aplicación de perfiles de seguridad
Soporte y Monitoreo	Visualización de dashboards
	Monitoreo de estado de salud de agentes
	Soporte a plataforma de detección y respuesta de amenazas avanzadas para endpoints

UPS

Cantidad	Características
1	Puertos e Interfaz Interfaz: DB-9 RS-232, G35T Puerto serial: 1 Cantidad de salidas AC: 1 salidas AC PESO Y DIMENSIONES Peso: 305.1kg Altura: 1491 mm Ancho: 356mm Profundidad: 838 mm



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

CONTROL DE ENERGÍA

Tiempo de recarga de la batería: 5H
Capacidad de potencia de salida (VA): 10000VA
Voltaje nominal de entrada: 208 V
Eficiencia: 93%
Potencia de salida: 8000w
Corriente de entrada THD: 5%
Salida de Voltaje THD: 5%

EMISION DE SONIDO

Nivel de ruido: 51.3 Db

BATERIA:

Tecnología de la batería: Ácido de plomo sellado (VRLA)

OTRAS CARACTERISTICAS:

Factor de forma: Montaje en rack o Montaje en bastidor
Voltaje nomina de salida: 208 V
Conexiones de salida: 1x hard wire 4-wire (3PH+G)n1x Hard Wire 5-wire (3PH+N+G)

DISEÑO

Seguridad: cUL Listed,CSA,CSA C22.2 No. 107.1,ISO 14001,ISO 9001,UL 1778

Espacio de Trabajo Digital

La solución deberá proveer la infraestructura necesaria así como los componentes de software, hardware, servicios de implementación y adecuaciones para ser implementada en el centro de datos de Isssteleon. Así mismo deberá ser considerado un ambiente productivo con soporte de 24 x 7 los 365 días del año con tiempo de respuesta de 1 hora y tiempo de resolución de 4 horas. Isssteleon solicitará al proveedor un esquema de tercerización que contemple un plazo de (dos) años para la prestación de los servicios de soporte.



1

Capacidad de Computo en infraestructura hiperconvergente para soportar escenarios de aplicaciones y escritorios virtuales

Plataforma de virtualización:

Escalabilidad:

- 1-8 sistemas por grupo de recursos
- Hasta 4 nodos por chassis
- 1-4 sistemas por grupo de recursos
- Sistemas de 3 o 4 nodos

Huella de rack:

- 2U por chasis del sistema

Numero de nodos

- 2, 3 o 4 nodos idénticos por sistema
- 3 o 4 nodos idénticos por sistema

Número de unidades:

- 6 unidades por nodo
- (12 unidades en una configuración de 2 nodos
- 18 unidades para configuración de 3 nodos
- 24 unidades para configuración de 4 nodos)
- 6 unidades por nodo
- (18 unidades para configuración de 3 nodos
- 24 unidades para configuración de 4 nodos)

Capacidad bruta:

- 9,6 TB de almacenamiento todo flash
- 6,4 TB de almacenamiento híbrido por nodo
- 5.6 TB de almacenamiento híbrido por nodo
- 7.2 TB de capacidad de almacenamiento por nodo
- 9,6 TB de almacenamiento todo flash
- 8,8 TB de almacenamiento híbrido por nodo
- 5.6 TB de almacenamiento híbrido por nodo
- 10,8 TB de capacidad de almacenamiento por nodo
- 7.2 TB de capacidad de almacenamiento por nodo

CPU:

- Procesadores Intel Xeon E5-2680v3 o v4 por nodo, o
- Procesador Intel Xeon E5-2660v3 o v4 por nodo, o



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Procesadores Intel Xeon E5-2640v3 o v4 por nodo
- (2) procesadores Intel Xeon E5-2680v3 o v4 por nodo, o
- (2) por nodo de procesadores Intel Xeon E5-2640 v3 o v4

Memoria:

- DIMM DDR4 x4 de doble rango de 128 GB, 256 GB o 512 GB por nodo
- Caché del controlador de almacenamiento
- Caché de escritura respaldada por batería de 4 GB por nodo (una batería compartida por sistema)

Conectividad de red primaria:

- Puertos SFP + de 10 GbE3 por nodo
- Puertos RJ45 de 1 GbE por nodo
- Puertos SFP + de 10 GbE3 por nodo
- Puertos de red secundarios (solo administrador)
- 2x 1 GbE RJ-45 (1000BASE-T) 4 por nodo
- iLO ports
- 1 GbE RJ-45 (100BASE-T) por nodo

Idioma:

- Inglés (EE. UU.)

Fuentes de alimentación:

- 2 fuentes de alimentación Platinum Plus de 1400 W (CA de línea alta solamente, 200-240 V) en el sistema

Garantía:

-

Especificaciones físicas:

- Dimensiones (Al x An x Pr) 2U 8,73 x 44,81 x 82,27 cm (3,44 x 17,64 x 32,4 pulgadas)
- Peso (aproximado) 35,52 kg (78,31 libras)

Especificaciones electricas:

- Fuentes de alimentación de ranura común de conexión en caliente redundantes, ventiladores redundantes Solo CA de línea alta:
- 200-240 V, 50-60 Hz
- 200-240 V / 50 Hz
- 2300 BTU / hora

Especificaciones ambientales:

- Temperatura de funcionamiento 10 ° a 35 ° C (50 ° a 95 ° F)



Matamoros 319 Pte.
Monterrey, N.L. México



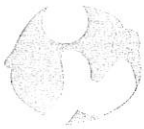
isssteleon.gob.mx



81.2020.9400 / 81.2033.9000



Gobierno de
Nuevo León



- Temperatura no operativa -30 ° a 60 ° C (-22 ° a 140 ° F)
- Humedad relativa de funcionamiento 10% a 90% sin condensación
- Humedad relativa no operativa 5% a 95% sin condensación
- Altitud operativa 3048 m (10,000 pies)
- Altitud no operativa 9144 m (30.000 pies)

Estándares normativos:

- CISPR 22; EN55022; EN55024; FCC CFR 47, Parte 15; ICES-003; CNS13438: GB9254; K22: K24; EN 61000-3-2; EN 61000-3-3; EN 60950-1; IEC 60950-1

Cantidad	Características
1	<p>ESCENARIO 1. SERVICIO DE APLICACIONES Y ESCRITORIOS VIRTUALES</p> <p>Se requiere como minimo 450 posiciones de Aplicaciones y Escritorios Virtuales, para entregar aplicaciones y escritorios virtuales seguros a cualquier dispositivo, en este modelo, la solución se ocupa en mayor parte de la instalación, la configuración, la actualización y la supervisión del producto, permitiendo a Isssteleon mantener control total sobre las aplicaciones, las directivas y los usuarios.</p> <p>COMPONENTES DE LA SOLUCIÓN</p> <p>Capa de control central en una implementación. Los servicios se comunican a través de los conectores de nube en cada ubicación de recurso para:</p> <ol style="list-style-type: none"> 1. Distribuir aplicaciones y escritorios. 2. Autenticar y administrar el acceso de los usuarios. 3. Intervenir como intermediario en conexiones entre los usuarios y sus aplicaciones o escritorios virtuales. 4. Optimizar el uso de las conexiones y equilibrar la carga de estas conexiones. 5. Realizar un seguimiento de los usuarios que han iniciado sesión, dónde lo han hecho, qué recursos tienen, y si necesitan reconectarse a aplicaciones existentes.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

6. Los datos de los servicios del controlador se almacenan en la base de datos del sitio de Microsoft SQL Server. Una implementación usa una base de datos de registros de configuración, además de una base de datos de supervisión.

ADMINISTRACIÓN DEL LICENCIAMIENTO

La función de administración de licencias se comunica con el controlador para administrar las licencias de cada sesión de usuario y para asignar los archivos de licencias. El administrador de Isssteleon no necesita configurar ni administrar el licenciamiento, todo este trabajo se realiza automáticamente en la nube.

CONSOLA DE ADMINISTRACIÓN

Se utiliza para configurar y administrar las conexiones, los catálogos de máquinas y los grupos de entrega. La solución se inicia cuando se selecciona **Administrar** en la consola del fabricante.

CONSOLA DE ADMINISTRACION Y SOLUCION DE PROBLEMAS

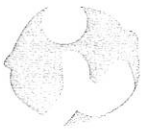
Esta solución permite a los equipos de asistencia técnica y TI supervisar el entorno, solucionar problemas antes de que se agraven, y realizar tareas de asistencia a los usuarios finales. Las pantallas incluyen:

7. Datos de sesión en tiempo real procedentes del gestor de servicio en el controlador, que incluye datos que el gestor de servicio obtiene del agente de gestión en el VDA.
8. Datos históricos de los sitios, procedentes de el monitor de en el controlador.
9. Datos sobre el tráfico conocido como tráfico ICA.

CONFIGURACIÓN DE ESPACIO DE TRABAJO DIGITAL

Desde la configuración de espacio de trabajo en la consola del fabricante, se tendrá:

- Especificar los servicios integrados con la solución de espacios de trabajo digital.
- Personalización de la URL que utilizarán los agentes para acceder a su espacio de trabajo.
- Personalizar la apariencia de los espacios de trabajo para los agentes, con logotipos, colores de Isssteleon.
- Configuración de autenticación por medio de Active Directory y Azure Active Directory.
- Especificar la conectividad externa para las ubicaciones de recursos utilizadas por los agentes.



COMPONENTES EN UBICACIONES DE RECURSOS

Una ubicación de recursos contiene los recursos necesarios para prestar servicios a los suscriptores (usuarios). Estos recursos se administran desde la nube del fabricante. Las ubicaciones de recursos contienen recursos distintos, en función de los servicios de Cloud que esté utilizando y de los servicios que quiera proporcionar a los usuarios.

Para interactuar con el gestor cloud, cada ubicación de recursos necesita conectores de nube y acceso a un dominio de Microsoft Active Directory.

En la implementación de Virtual Apps and Desktops Service, cada ubicación de recursos contendrá elementos de la capa de acceso y de la capa de recursos:

10. Conectores de nube
11. Controlador de dominio de Active Directory
12. Agentes Virtual Delivery Agent
13. Hipervisores que aprovisionan agentes VDA y guardan sus datos, si se utilizan
14. Consola Gateway de ser necesario
15. StoreFront de ser necesario

Cada ubicación de recursos contendrá al menos dos conectores de nube para garantizar alta disponibilidad. Un conector de nube es el canal de comunicación entre los componentes que se encuentran en nube y los componentes que se encuentran en la ubicación de recursos. En la ubicación de recursos, el conector de nube actúa como proxy para el controlador de entrega del ambiente de nube

Los conectores de nube se instalan desde la consola de servicio de nube. Después, la plataforma administra y actualiza automáticamente los conectores de nube

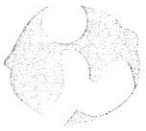
Agentes Virtual Delivery Agent (VDA)

Cada máquina física o virtual que entrega aplicaciones y escritorios debe tener un agente VDA. El VDA se registra en un conector de nube. Después del registro, se utiliza un broker en las conexiones desde esos recursos a los usuarios. Los VDA establecen y administran la conexión entre la máquina y el dispositivo del usuario, y aplican las directivas que se hayan configurado para la sesión.

El VDA comunica la información de la sesión al conector de nube a través del agente de broker incluido en el VDA. El agente de broker aloja varios plugins y recopila datos en tiempo real.

Existen agentes VDA disponibles para sistemas operativos de servidor y de escritorio Windows.

Los VDA para sistemas operativos de servidor Windows permiten que varios usuarios se conecten al servidor al mismo tiempo. Los VDA para SO de escritorio Windows permiten la conexión de un



solo usuario al escritorio en un momento dado. Los agentes VDA para Linux también están disponibles.

En esta documentación, la palabra "VDA" se refiere tanto al agente en sí como a la máquina donde está instalado.

HIPERVISORES Y SERVICIOS EN LA NUBE

Para aprovisionar las máquinas virtuales que entregan las aplicaciones y los escritorios se configuró:

16. Servicio de creación de máquinas virtuales. La tecnología de creación de máquinas virtuales está integrada en la plataforma y se accede automáticamente a ella desde la consola de Cloud. esta tecnología crea copias de una imagen maestra para crear y aprovisionar máquinas virtuales.
17. Acceso con Remote PC para el isssteleon, que permite a los agentes acceder de forma remota a sus PC físicos.

ACTIVE DIRECTORY

Aunque no se trate de un componente nativo en la plataforma de creación de escritorios virtuales, se necesita Microsoft Active Directory para la autenticación y la autorización en cualquier implementación. La infraestructura de Kerberos en Active Directory se usa para garantizar la autenticidad y la confidencialidad de las comunicaciones con el ambiente de Cloud.

ELEMENTOS QUE AYUDAN A ENTREGAR ESCRITORIOS Y APLICACIONES

En el marco de la entrega de escritorios a los usuarios en un entorno de producción, puede configurar los siguientes elementos.

CONEXIÓN DE HOST

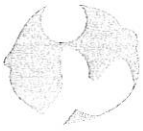
Una conexión de host permite la comunicación entre los componentes del plano de control y los agentes VDA que se encuentran en un hipervisor o servicio de nube. A continuación, se presentan las especificaciones de las conexiones:

18. La dirección y las credenciales para acceder al host
19. La herramienta que se usa para crear las máquinas virtuales
20. El método de almacenamiento a utilizar y las máquinas que se utilizarán para el almacenamiento
21. La red que usarán las máquinas virtuales

CATÁLOGO DE MÁQUINAS

Un catálogo de máquinas es un conjunto de máquinas físicas o virtuales que tienen el mismo tipo de sistema operativo: servidor o escritorio.

Si utiliza máquinas virtuales, puede crear una imagen maestra (también conocida como plantilla) en el hipervisor o el servicio de nube e instalar un VDA en la imagen maestra. También puede instalar aplicaciones en la imagen maestra, si quiere que aparezcan en todas las máquinas que



se creen a partir de esa imagen y no quiere virtualizarlas. A continuación, usted crea un catálogo con la ayuda de una herramienta de servicio para la creación de máquinas virtuales o con sus propias herramientas. Con las herramientas de gestión, el proceso de creación del catálogo aprovisiona máquinas virtuales idénticas a partir de esa imagen.

Si utiliza sus propias herramientas para aprovisionar las VM o si usa máquinas físicas, el proceso de creación del catálogo agrega esas máquinas al catálogo.

GRUPO DE ENTREGA

Un grupo de entrega indica:

22. Una o varias máquinas de un catálogo.
23. También puede indicar a los usuarios autorizados para acceder a esas máquinas. También puede especificar usuarios desde la consola de creación de máquinas virtuales en cloud
24. Opcionalmente, puede indicar las aplicaciones y los escritorios a los que pueden acceder los usuarios. También puede especificar aplicaciones desde la consola de creación de máquinas virtuales en nube

ENTREGA DE APLICACIONES Y ESCRITORIOS

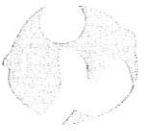
Métodos de entrega describe las opciones disponibles para entregar aplicaciones y escritorios a los usuarios.

ESCENARIO 2. CREACION DE VIRTUAL APPS AND DESKTOPS EN AZURE

La combinación de una plataforma de creación de máquinas virtuales en nube y Microsoft Azure permitirá a isssteleon aumentar los recursos virtuales de con mayor agilidad y elasticidad, ajustando el uso a medida que cambian los requisitos. Las máquinas virtuales en Azure admiten todos los componentes de control y carga de trabajo necesarios para la implementación del servicio de Virtual Apps and Desktops. La plataforma de gestión de nube y Microsoft Azure tienen integraciones comunes de plano de control que establecen identidad, gobernanza y seguridad para operaciones globales.

A continuación se destacan las consideraciones de diseño y e implementación en los siguientes cinco principios arquitectónicos clave:

1. **Operaciones:** Operaciones incluye una amplia variedad de temas como administración de imágenes, supervisión de servicios, continuidad del negocio, soporte y otros. se deberán utilizar herramientas disponibles para ayudar con la automatización de las operaciones, como Azure PowerShell, Azure CLI, ARM Templates y Azure API.
2. **Identidad:** Una de las piedras angulares de toda la imagen de Azure es la identidad de una persona y su acceso basado en roles (RBAC). La identidad de Azure se administra a



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

través de Azure Active Directory (Azure AD) y Servicios de dominio de Azure AD. Isssteleon debe decidir el camino a seguir para su integración de identidad.

- 3. Gobernanza:** La clave del gobierno es establecer las directivas, los procesos y los procedimientos asociados con la planificación, la arquitectura, la adquisición, la implementación y la administración operativa de los recursos de Azure.
- 4. Seguridad:** Azure proporciona una amplia gama de opciones de seguridad configurables y la capacidad de controlarlas para que los clientes puedan personalizar la seguridad para satisfacer los requisitos únicos de las implementaciones de su organización. Esta sección ayuda a comprender cómo las capacidades de seguridad de Azure pueden ayudarle a cumplir estos requisitos.
- 5. Conectividad:** La conexión de redes virtuales de Azure con la red local o en la nube del cliente se denomina red híbrida. En esta sección se explican las opciones de conectividad de red y enrutamiento de servicios de red.

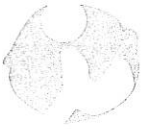
DEFINICION

Se estarán implementando 2 casos para entregar aplicaciones y escritorios a través de Azure:

1. Implementación Greenfield que ofrece ubicaciones de recursos en Azure. Este caso se entrega a través del servicio de Virtual Apps and Desktops y se utiliza cuando para el modelo de suscripción y externalizar la infraestructura del plano de control a un ambiente totalmente independiente.
2. Levanta y cambia. Con este caso, los clientes implementan su infraestructura de administración de escritorios y aplicaciones virtuales en Azure y tratan Azure como un sitio, utilizando una plataforma de entrega adicional para agregar recursos de varios sitios. Este modelo se centra en el modelo de implementación de un ambiente de nube. El Isssteleon podrá planificar y adoptar estos servicios en función de las necesidades de su organización:

DISEÑO DE REDES

La seguridad de red se puede definir cómo el proceso de protección de recursos contra accesos no autorizados o ataques mediante la aplicación de controles al tráfico de red. El objetivo es garantizar que solo se permita el tráfico legítimo. Azure incluye una sólida infraestructura de red para admitir los requisitos de conectividad de aplicaciones y servicios. La conectividad de red es posible entre los recursos ubicados en Azure, entre los recursos locales y hospedados en Azure,



y hacia y desde Internet y Azure.

CONECTIVIDAD

La conexión de redes virtuales de Azure con la red local o en la nube de los clientes se conoce como redes híbridas. En esta sección se detallan las opciones de conectividad de red y enrutamiento de servicios de red. Isssteleon podrá conectar sus equipos y redes locales a una red virtual mediante cualquier combinación de las siguientes opciones:

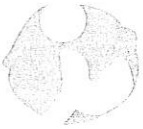
3. VPN de sitio a sitio: establecido entre un dispositivo VPN local y una puerta de enlace VPN de Azure que se implementa en una red virtual. Este tipo de conexión habilita a cualquier recurso local que el cliente autorice para acceder a una red virtual. La comunicación entre el dispositivo VPN local y una Gateway VPN de Azure se envía a través de un túnel cifrado a través de Internet.
4. Azure ExpressRoute: establecido entre la red del cliente y Azure, a través de un socio de ExpressRoute. Esta conexión es privada. El tráfico no pasa por internet.

Las principales consideraciones para la conectividad de Azure a cliente son el ancho de banda, la latencia, la seguridad y el coste. Las VPN de sitio a sitio tienen límites de ancho de banda más bajos que Express Route y dependen del rendimiento del enrutador perimetral utilizado por el cliente. Los SLA están disponibles en los SKU de la puerta de enlace VPN. Las VPN de sitio a sitio utilizan IPSec a través de Internet.

Las rutas Express son conexiones privadas dedicadas y no a través de Internet. Esto da como resultado una menor latencia cuando se usa Express Route. Además, Express Route puede escalar hasta 10 Gbps. Express Route se configura mediante un partner certificado. El tiempo de configuración de estos proveedores debe tenerse en cuenta durante la planificación del proyecto. Los costes de Express Route tienen un componente de Microsoft y un componente de proveedor de Express Route.

Normalmente, estas conexiones se comparten entre varios servicios (replicación de bases de datos, tráfico de dominio, tráfico de aplicaciones, etc.) En una implementación de nube híbrida, puede haber casos en los que los usuarios internos requieran que su tráfico ICA pase por esta conexión para llegar a sus aplicaciones en Azure, por lo que la supervisión de su ancho de banda es fundamental.

Sera necesario considerar cualquier dispositivo adicional para el enrutamiento óptimo de Gateway también se puede utilizar para dirigir la conexión de un usuario a un dispositivo mediante el ISP de una oficina en lugar de Express Route o VPN a Azure.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

SD-WAN

La tecnología WAN definida por software (SD-WAN) permite ofrecer una gran experiencia de usuario, incluso en conexiones difíciles. Es un ajuste natural para la entrega de aplicaciones virtuales y escritorios.

25. Agrega todo el ancho de banda disponible en una conexión activa/activa, proporcionando más ancho de banda.
26. Considerar la tecnología necesaria para garantizar un óptimo rendimiento y ajustar las directivas de red.
27. Garantizar conexiones siempre activas para aplicaciones virtuales y usuarios de escritorio con la experiencia de la más alta calidad posible, incluso para medios enriquecidos y vídeo de alta definición.

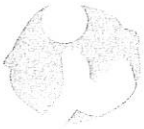
Los clientes que utilizan VPN pueden aprovechar SD-WAN para agregar redundancia a la conectividad del centro de datos de Azure y del cliente o para proporcionar enrutamiento específico de la aplicación. SD-WAN debe redirigir automáticamente el tráfico a través de cualquier conexión disponible. Garantizar una experiencia tan perfecta que los usuarios ni siquiera se darán cuenta de que se ha producido ningún cambio. Su dirección IP de acceso principal permanecerá sin cambios, lo que permitirá a los usuarios acceder a sus aplicaciones y datos utilizando los mismos métodos y dispositivos.

CONTROLADORA PARA LA ENTREGA DE APLICACIONES

Con esta tecnología en Microsoft Azure se pretende garantizar que las Isssteleon tenga acceso a aplicaciones y activos seguros y optimizados implementados en la nube y proporciona la flexibilidad necesaria para establecer una base de red que se ajuste a las necesidades cambiantes de un entorno. En caso de fallo del centro de datos se deberá redirigir automáticamente el tráfico de usuario a un sitio secundario, sin interrupciones para los usuarios. El equilibrio de carga y el equilibrio de carga global de servidores en varios centros de datos garantizan aún más el estado, las capacidades y la utilización óptimas del servidor.

MODELO DE IMPLEMENTACIÓN

Las implementaciones activo-activas aprovechan los nodos independientes que se pueden escalar mediante el equilibrador de carga de Azure. Los pares activo-pasivo facilitan la conmutación por error con estado del tráfico ICA en caso de fallo de nodo, sin embargo, están limitados a la capacidad de un único VPX. Los nodos activo-pasivo también requieren Azure Load Balancer.



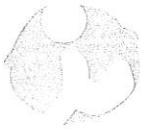
ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Se deberá considerar un máximo de 500 Mbps por NIC de Azure. Se recomiendan varias NIC para aislar el tráfico SNIP, NSIP y VIP para maximizar el rendimiento disponible .

NIVELES DE SOPORTE PARA LA MESA DE AYUDA, PARA LOS RECURSOS EN SITIO Y EL EQUIPO DE CONSULTORES DEL PROVEEDOR

- **Soporte Nivel 1:** Es el soporte más básico, es la mesa de ayuda que recibirá los llamados de los usuarios, aquí ingresarán todos los llamados, no solo los de reporte de inconvenientes sino también consultas y otros. Este nivel de soporte tiene permisos de "Solo ver" la configuración pero no puede tomar acciones.
- **Soporte Nivel 2:** Es el soporte intermedio, idealmente realizado por las personas de el proveedor que administraran la plataforma, solo se les asignó permisos de ver las configuraciones, enviar mensajes a los usuarios, desconectar y terminar sesiones, terminar procesos y tomar control de usuarios. O sea tareas triviales de administración pero no podrán modificar ninguna configuración. Los llamados a este nivel solo deberían llegar escalando los llamados del nivel 1 cuando requieren acciones técnicas.
- **Soporte Nivel 3:** Es el grupo de soporte avanzado, con permisos de cambiar cualquier configuración, además de todas las tareas de los niveles anteriores. Solo un grupo reducido de administradores deberían tener estos permisos. Los llamados a este nivel solo deberían llegar escalando los llamados del nivel 2 cuando requieran cambios en las configuraciones o servidores.
- Se deben revisar y realizar las configuraciones necesarias en Active Directory creando tres Grupos llamados "Soporte_Nivel_1", "Soporte_Nivel_2", "Soporte_Nivel_3". Los usuarios involucrados en cada nivel de soporte solo deberán hacerlos miembros de cada grupo y con eso obtendrán los permisos necesarios en la granja de virtualización.



	<ul style="list-style-type: none"> • Posteriormente se crearan en el ambiente los tres niveles de administración con sus respectivos permisos: • Soporte_Nivel_1: View Only. • Soporte_Nivel_2: Permisos "Custom" • Soporte_Nivel_3: Full Admin • Delegación de permisos de Soporte • Se deben establecer los siguientes permisos personalizados en la consola para los diversos roles de Soporte. Es mejor mantener el nivel de permiso al mínimo necesario para realizar las tareas necesarias.
--	---

Impresión

A) Modelo de impresora 1

Cantidad	Características
5	<ul style="list-style-type: none"> • La impresora comprueba su código de funcionamiento y se repara a sí misma de los ataques. • Las conexiones de red salientes de la impresora se inspeccionan para detener solicitudes sospechosas e impedir el malware. La actividad de la memoria se supervisa para detectar y detener de forma continua los ataques. • El firmware se comprueba automáticamente durante el inicio para determinar si el código es auténtico: firmado digitalmente por el fabricante. • Bolsillo de integración de hardware de 2.ª generación • Puerto USB de fácil acceso • Botón de liberación de la cubierta superior • La bandeja 1 multiuso de 100 hojas admite soportes de hasta 216 x 356 mm • Pantalla táctil en color de 10,9 cm • Bandeja de salida de 250 hojas • Cubierta superior • Impresión automática a doble cara • La bandeja 2 de entrada de 550 hojas admite soportes de hasta 216 x 356 mm • Ranura para bloqueo de seguridad de cable • Gigabit Ethernet, puerto host USB • Puerto impresión USB 2.0 alta velocidad • Puerto USB para conectar los dispositivos USB externos • Tecnología de impresión: Láser



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Velocidad de impresión: Negro (A4, normal) Hasta 43 ppm; Negro (A4, a doble cara) hasta 34 ipm.
- Impresión de primera página Negro (A4, listo): En sólo 5,9 segundos; Negro (A4, suspensión): En sólo 10 segundos
- Resolución de impresión Negro (óptimo): Hasta 1200 x 1200 ppp; Tecnología: 300 ppp, 600 ppp
- Ciclo mensual de trabajo Hasta 150.000 páginas A4
- Volumen de páginas mensual recomendado: De 2.000 a 15.000
- Funciones del software inteligente de la impresora: Vista previa de impresión, impresión a doble cara, impresión de múltiples páginas por hoja (2, 4, 6, 9, 16), ordenación, filigranas, almacenamiento de trabajos de impresión, USB de fácil acceso
- Fuentes y tipos de letra: 105 fuentes internas TrueType escalables, 92 fuentes internas escalables; 1 fuente Unicode interna (Andale Mono World Type); 2 fuentes Windows Vista 8 internas (Calibri y Cambria); Existen soluciones disponibles con fuentes adicionales mediante tarjetas de memoria flash de terceros.
- Área de impresión: Márgenes de impresión Márgenes de impresión Superior: 4,3 mm, Inferior: 4,3 mm, Izquierdo: 4,3 mm, Derecho: 4,3 mm; Área de impresión máxima : 212 x 352 mm
- Impresión a doble cara: Automática (estándar)
- Velocidad de procesador: 1,2 GHz

Conectividad

- Estándar: 2 USB 2.0 de alta velocidad integrados; 1 Dispositivo USB 2.0 de alta velocidad; 1 Red 10/100/1000T Ethernet Gigabit
- Protocolos de red admitidos: Mediante una solución de red integrada: TCP/IP , IPv4, IPv6; Impresión: modo directo TCP-IP puerto 9100, LPD (solo compatible con la cola de impresión sin formato), impresión de servicios web, IPP 2.0, Apple AirPrint™, HP ePrint, impresión FTP , Google Cloud Print; Detección: SLP , Bonjour , detección de servicios web; Configuración IP: IPv4 (BootP , DHCP , AutoIP , Manual, Configuración TFTP , ARP-Ping), IPv6 (enlace local sin estado y a través del enrutador , con estado completo a través de DHCPv6); Gestión: SNMPv2/v3, HTTP/HTTPs, Telnet, Configuración TFTP , Registro del sistema; Seguridad: SNMPv3, gestión de certificados SSL, IPSec/cortafuegos, ACL, 802.1x
- Disco Duro: Unidad de Disco Duro Cifrado Opcional de 500GB mínimo
- Memoria Estándar: 512 MB; Máximo: 1,5 GB, memoria MÁX., cuando el accesorio de 1 GB DIMM está instalado



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Gestión de Soportes:

- Número de bandejas de papel: Estándar: 2 Máximo: 5
- Tipos de soportes: Papel (bond, en color, normal, preimpreso, preperforado, reciclado, rugoso); Sobres; Etiquetas; Cartulina; Transparencias; Definido por el usuario
- Tamaño de soporte: Personalizado (métrica): Bandeja 1: de 76,2 x 127 a 215,9 x 355,6 mm; Bandeja 2: de 105 x 148 a 215,9 x 355,6 mm; Bandeja de 550 hojas opcional: De 105 x 148 a 215,9 x 355,6 mm. Compatible (métrica): Bandeja 1: A4, A5, A6, RA4, B5 (JIS), B6 (JIS), 10 x 15 cm, Oficio (216 x 340 mm), 16K, postales (JIS único y doble), sobres (B5, C5, C6, DL); Bandeja 2: A4, A5, A6, RA4, B5 (JIS), B6 (JIS), Oficio (216 x 340 mm), 16K, postales (JIS doble); Bandeja de 550 hojas opcional: A4, A5, A6, RA4, B5 (JIS), B6 (JIS), Oficio (216 x 340 mm), 16K, postales (JIS doble); Duplexor automático opcional: A4, RA4, Oficio (216 x 340 mm)
- Gramaje de soportes: Bandeja 1: de 60 a 199 g/m²; bandejas 2 y 3: de 60 a 120 g/m²
- Capacidad de entrada: Bandeja 1: Hojas: 100; Transparencias: 50; Sobres: 10 Bandeja 2: Hojas: 550 Bandeja 3: Hojas: 550 Máximo: Hasta 2.300 hojas
- Sistemas operativos compatibles: Windows Server 2008 de 32 bits, Windows Server 2008 de 64 bits, Windows Server 2008 R2 de 64 bits, Windows Server 2012 de 64 bits, Windows Server 2012 R2 de 64 bits, Windows Server 2016 de 64 bits, Windows Server 2019, Citrix con Microsoft Windows Server 2012, 2012 R2 y Microsoft Server 2016, Citrix XenApp y XenDesktop 7.x, Citrix con Microsoft Windows Server 2008 R2 SP1, Citrix XenApp 6.0, Citrix XenApp 6.5, Citrix XenApp y XenDesktop 7.5 (compatible con el sistema operativo Windows Server 2008 R2 SP1), Citrix XenServer 6.x+, Windows 7 SPI (32/64 bits) iPrint Client v5.99+ recomendado, Windows 8 (32/64 bits) iPrint Client v5.99+ recomendado, Windows 8.1 (32/64 bits) iPrint Client v5.99+ recomendado, Novell/Micro Focus (Novell iPrint ahora es Micro Focus) <https://www.novell.com/products/iprint/>, plataformas de servidor Novell iPrint Appliance compatibles, Novell iPrint Appliance v1.1, clientes Novell iPrint compatibles (iPrint v5.94 o posterior recomendados para plataformas Windows), Novell Open Enterprise Server 11/SP1, Services Terminal Server Cluster Server, VMware ESX 4.x+ Workstation 9.x+, XEN en SUSE Linux Enterprise Server (SLES) 11/SP3.
- Gestión de seguridad: Gestión de identidad: Autenticación Kerberos; Autenticación LDAP; Códigos PIN para 1000 usuarios; Soluciones opcionales de autenticación avanzada de HP y de otros fabricantes (p. ej., lectores de credenciales); Red: IPsec/cortafuegos con certificado; Clave previamente compartida y autenticación Kerberos; Admite el complemento de configuración WJA-10 IPsec; Autenticación 802.1X (EAP-PEAP; EAP-TLS); SNMPv3; HTTPS; Certificados; Lista de control de acceso; Datos: Cifrado de almacenamiento; Cifrado de PDF y correo electrónico (utiliza bibliotecas criptográficas validadas FIPS 140 de Microsoft); Borrado seguro; SSL/TLS (HTTPS);

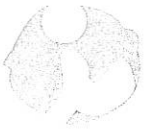
Matamoros 319 Pte.
Monterrey, N.L. México

isssteleon.gob.mx

81.2020.9400 / 81.2033.9000



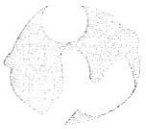
Gobierno de
Nuevo León



	<p>Credenciales cifradas; Dispositivo: Ranura de bloqueo de seguridad; Desactivación del puerto USB; Bolsillo de integración de hardware para soluciones de seguridad; Detección de intrusiones con tecnología de seguridad Red Balloon: supervisión continua de ataques en el dispositivo; Arranque seguro SureStart: comprobación de la integridad de la BIOS con función de recuperación automática; Listas blancas: solo carga el código bueno conocido (archivos DLL y EXE, etc.); Connection Inspector: garantiza que las conexiones de red al dispositivo sean seguras; Gestión de seguridad: Mensajes del registro del sistema de seguridad del dispositivo procesados y accesibles en los SIEM ArcSight, Splunk y McAfee (ESM)</p> <ul style="list-style-type: none"> • Dimensiones de la impresora: Mínimos 418 x 376 x 326 mm; Máximo: 418 x 639 x 326 mm; • Peso de la impresora: 11,48 kg • Alimentación: Requisitos: Voltaje de entrada: de 220 V a 240 V nominal (+/- 10 %), 50-60 Hz nominal (+/-), 4 A; Consumo: 601 vatios (impresión activa), 7,60 vatios (listo), 2,61 vatios (suspensión), 0,06 vatios (apagado automático), 0,06 vatios (apagado), apagado automático/despertar en LAN 0,73 vatios; Consumo eléctrico típico (TEC): Blue Angel: 1,257 kWh/semana; Energy Star: 1,310 kWh/semana; Tipo de fuente de alimentación: Fuente de alimentación de 115V o 220V integrada. • Certificaciones: CISPR 22:2008 (Internacional) - Clase A, CISPR32:2012 (Internacional) - Clase A, EN 55032:2012 (UE) - Clase A, EN 61000-3-2:2014, EN 61000-3-3:2013, EN 55024:2010, Directiva EMC 2014/30/UE, Número 6 Clase A, otras certificaciones EMC impuestas por cada país. Blue Angel; EPEAT® Silver; CECP; Certificación ENERGY STAR® Certificado para Blue Angel: Blue Angel DE-UZ 205. • Garantía: Un año de garantía in situ al siguiente día laborable.
--	--

B) Modelo de impresora 2

Cantidad	Características
31	<ul style="list-style-type: none"> • Bandeja de salida de 150 hojas • Puerta frontal, acceso a los cartuchos de tóner originales HP con JetIntelligence • Impresión automática a doble cara (predeterminada)16 • Pantalla gráfica en colores de 6,9 cm (2,7") • Puerta derecha, acceso a la ruta de impresión Bandeja multipropósito 1 de 100 hojas Bandeja de entrada 2 de 250 hojas • Práctico interruptor de encendido en la parte frontal • Puerto de red Gigabit Ethernet • Puerto de impresión USB 2.0 de alta velocidad



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Puerto USB 2.0 de alta velocidad para dispositivos de terceros
- Velocidad de impresión (carta/A4)12 Hasta 40/38 ppm (predeterminado); 42/40 ppm (HP High Speed)
- Salida de la primera página (carta/A4)10 En tan solo 6,3/6,5 segundos
- Panel de control Pantalla gráfica en colores de 6,9 cm (2,7")
- Memoria 1 GB
- Almacenamiento eMMC de 4 GB
- Impresión automática a doble cara (predeterminada)16
- Capacidad de entrada (estándar/máxima) Hasta 350/900 hojas
- Bandeja de entrada 1 de 100 hojas
- Bandeja de entrada 2 de 250 hojas
- Bandeja de entrada 3 de 550 hojas Opcional
- Volumen mensual de páginas recomendado (RMPV)32 1500 a 7500 páginas
- Ciclo de trabajo Hasta 120 000 páginas
- Rendimiento del cartucho administrado 11 500 páginas Wi-Fi de banda doble con Bluetooth® Low Energy, Wi-Fi Direct® 33 Opcional

Especificaciones de los sustratos

- Capacidad de entrada Hasta 350 hojas estándar (bandeja multipropósito de 100 hojas, bandeja de entrada de 250 hojas) Hasta 900 hojas como máximo (con la tercera bandeja opcional de 550 hojas)
- Capacidad de salida Hasta 150 hojas
- Impresión a doble cara Automática (predeterminado)
- Tamaños de los sustratos

Bandeja 1: carta, legal, oficio, ejecutivo, declaración, 4 x 6, 3 x 5, 5 x 7, 5 x 8, postal (JIS), postal doble (JIS), 8,5 x 13, sobre (comercial N° 9, N° 10, Monarch); A4, RA4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K, sobres (B5, C5 ISO, C6, DL ISO); personalizado: 76 x 127 a 216 x 356 mm (3 x 5 a 8,5 x 14")

Bandeja 2: carta, ejecutivo, declaración, 5 x 7, 5 x 8, postal doble (JIS); A4, RA4, A5, B5 (JIS), A6, 16K; personalizado: 105 x 148 a 216 x 356 mm (4,1 x 5,8 a 8,5 x 14") • **Bandeja 3 (opcional):** carta, ejecutivo, declaración, 5 x 7, 5 x 8, postal doble (JIS); A4, RA4, A5, B5 (JIS), B6 (JIS), A6, 16K; personalizado: 105 x 148 a 216 x 356 mm (4,1 x 5,8 a 8,5 x 14")

Peso de los sustratos

- Bandeja 1: 60 a 175 g/m² (16 a 46,6 lb)
- Bandeja 2: 60 a 120 g/m² (16 a 32 lb)
- Bandeja 3 (opcional): 60 a 120 g/m² (16 a 32 lb)

Matamoros 319 Pte.
Monterrey, N.L. México

isssteleon.gob.mx

81.2020.9400 / 81.2033.9000



Gobierno de
Nuevo León



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Fuentes:

105 fuentes TrueType internas escalables en PCL, 92 fuentes internas escalables en la emulación PostScript Nivel 3 (símbolo de Euro incorporado); 1 fuente interna Unicode (Andale Mono World Type); 2 fuentes internas de Windows Vista 8 (Calibri, Cambria); soluciones de fuentes adicionales disponibles a través de tarjetas de memoria flash de terceros; fuentes LaserJet y emulación IPDS

Conectividad:

1 host USB 2.0 de alta velocidad; 1 dispositivo USB 2.0 de alta velocidad; 1 red Gigabit Ethernet 10/100/1000T

Protocolos de Red:

A través de solución de red integrada: TCP/IP, IPv4, IPv6; Impresión: Modo directo TCP-IP puerto 9100, LPD, impresión de servicios web, IPP 2.0, Apple AirPrint™, HP ePrint; Descubrimiento: SLP, Bonjour, Web Services Discovery; Config. IP: IPv4 (BootP, DHCP, AutoIP, Manual), IPv6 (sin estado para enlace local y a través de enrutador, con estado a través de DHCPv6), Administración: SNMPv2 / v3, HTTP / HTTPS, Syslog; Seguridad: SNMPv3, gestión de certificados SSL, IPsec (IKEv1 e IKEv2), Firewall, 802.1x.

Administración de la seguridad:


Administración de identidad: Autenticación Kerberos, autenticación de Protocolo de Acceso a Directorio Ligero (LDAP), códigos PIN de 1000 usuarios, soluciones opcionales de el fabricante y de terceros de autenticación avanzada (p. ej., lectores de tarjetas magnéticas)

Red: IPsec/firewall con certificado, clave compartida previamente y autenticación Kerberos, compatible con el complemento de configuración WJA-10 IPsec, autenticación 802.1X (EAP-PEAP, EAP-TLS), SNMPv3, HTTPS, certificados, lista de control de acceso

Datos: Cifrado de almacenamiento, PDF y correo electrónico cifrados (usa bibliotecas de cifrado FIPS 140 validadas de Microsoft), SSL/ TLS (HTTPS), credenciales cifradas

Dispositivo: Arranque seguro (comprobación de la integridad del BIOS con capacidad de recuperación automática), detección de intrusiones (supervisión constante de ataques en el dispositivo), listas blancas (carga solo el código correcto conocido), módulo de plataforma segura integrado Inspector de conexión, ranura para traba de seguridad, desactivación de puerto USB

Gestión de la seguridad: Mensajes syslog de seguridad del dispositivo procesados y accesibles en

 Matamoros 319 Pte.
Monterrey, N.L. México

 isssteleon.gob.mx

 81.2020.9400 / 81.2033.9000



Gobierno de
Nuevo León



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

SIEM Arcsight y Splunk.

Sistemas operativos compatibles:

- OS cliente Windows (32 y 64 bits): Windows 10, Windows 8.1, Windows 7 Ultimate
- SO para dispositivos móviles: iOS, Android Mac: Apple® MacOS High Sierra v10.13
- Apple® MacOS Mojave v10.14, Apple® MacOS Catalina v10.15

Sistemas operativos de red compatibles:

- Windows Server 2008 R2 de 64 bits, Windows Server 2008 R2 de 64 bits (SP1), Windows Server 2012 de 64 bits, Windows Server 2012 R2 de 64 bits, Windows Server 2016 de 64 bits, Windows Server 2019 de 64 bits, Citrix Server 6.5, Citrix XenApp & XenDesktop 7.6, servidor Novell iPrint, Citrix Ready Kit Certification hasta Citrix Server 7.18
- Citrix
- Unix

Requisitos del sistema, PC

2 GB de espacio disponible en el disco duro, conexión a internet o puerto USB y navegador de Internet

Dimensiones:

- Mínimo (todas las bandejas cerradas): 381 x 357 x 220 mm (15 x 14 x 8,7")
- Máximo (impresora totalmente abierta): 381 x 781 x 241 mm (15 x 30,8 x 9,5")

Peso:

- 8,5 kg (18,7 lb)

Garantía: al menos de 2 años, reparación en el sitio; soporte técnico telefónico 24/7

C) Modelo de impresora 3

Cantidad	Características
20	<ul style="list-style-type: none"> • Funciones Imprima, copie, escanee y envíe por fax • Panel de control Pantalla táctil IR, pantalla de gráficos en color (CGD) de 10,92 cm (4,3 pulg.) • Velocidad de impresión



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Negro (A4, normal) Negro (A4, normal) Hasta 50 ppm; Color (A4, normal) Color (A4, normal): Hasta 50 ppm; Negro (A4, a doble cara) Negro (A4, a doble cara): Hasta 25 ppm; Color (A4, a doble cara) Color (A4, a doble cara): Hasta 25 ppm; Negro (general de oficina) Negro (general de oficina): Hasta 75 ppm; Color (general de oficina) Color (general de oficina): Hasta 75 ppm;
- Impresión de primera página Negro (A4, listo) Negro (A4, listo): En solo 6 segundos; Color (A4, listo) Color (A4, listo): En sólo 6,5 segundos; Resolución de impresión Negro (óptimo) Negro (óptimo): Hasta 1200 x 1200 ppp optimizados a partir de 600 x 600 ppp de entrada (en papel normal sin especificar , papel mate para presentaciones Premium y papel mate para folletos); Color (óptimo) Color (óptimo): Hasta 2400 x 1200 ppp optimizados a partir de 600 x 600 ppp de entrada (en papel fotográfico Advanced);
- Ciclo mensual de trabajo Hasta 80 000 páginas A4; Volumen de páginas mensual recomendado Volumen de páginas mensual recomendado : 1.000 a 6.000
- Funciones del software inteligente de la impresora

ePrint; Aplicaciones móviles ; Google Cloud Print v2; Apple AirPrint™; EasyColor; Vista previa de impresión; Impresión automática a dos caras; Impresión de varias páginas por hoja (2, 4, 6, 9, 16); Intercalado; Impresión de folletos; Portadas; Selección de bandejas; Ajuste de escala; Orientaciones vertical y horizontal; Solo escala de grises de alta calidad y tinta negra; Modos de impresión de oficina general/profesional/presentación/máximo de ppp; Puerto USB frontal; Copia/Escaneado/Fax; Accesos directos al panel de control; Impresión de PIN UPD ; Control de acceso a color ; Opcional: soluciones de extensibilidad del fabricante y de otros fabricantes; Inalámbrico

- Lenguajes de impresión estándar
- Velocidad de copiado Negro (A4, ISO) Negro (A4, ISO): Hasta 50 cpm; Color (A4, ISO) Color (A4, ISO): Hasta 50 cpm

Especificaciones de la copiadora

- Copia de ID; Cambiar tamaño; Calidad; Más claro/más oscuro; Copia a doble cara; Selección de bandejas; Intercalar; Márgenes de encuadernación; Vista previa de copia con recorte y ajuste de tamaño; Mejoras; Activar/desactivar copia; Activar/desactivar copia en color; Control de acceso a color; Autenticación y autorización nativas; Establecer como nuevos valores predeterminados; Número máximo de copias Número máximo de copias: Hasta 99 copias; Resolución de copia Resolución de copia: Hasta 600 ppp; Reducir/Ampliar Reducir/Ampliar: De 25 a 400%;

Funciones del software inteligente de la copiadora

- Reducción/ampliación desde el cristal del escáner (de 25 a 400 %); Intercalar; Copia a doble cara; Ajustes de imagen (oscuridad, nitidez)

Velocidad de escaneado



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Normal (A4) Normal (A4): Hasta 25 ipm (monocromo y color); A doble cara (A4) A doble cara (A4): Hasta 26 ipm (monocromo y color)

Formato de archivo de escaneado

- Mapa de bits (.bmp), JPEG (.jpg), PDF (.pdf), PNG (.png), texto enriquecido (.rtf), PDF con búsqueda (.pdf), texto (.txt), TIFF (.tif)

Especificaciones del escáner

- Tipo de escáner De superficie plana, alimentador automático de documentos (ADF); Tecnología de escaneado: Contact Image Sensor (CIS); Modos de entrada de escaneado Modos de entrada de escaneado: Aplicaciones del panel frontal: copia, escaneado a correo electrónico con búsqueda de dirección de correo electrónico LDAP , escaneado a carpeta de red, escaneado a USB, escaneado a SharePoint, escaneado a ordenador con software; Aplicaciones del cliente: EWS, aplicación Scan, compatible con Capture and Router; Versión Twain Versión Twain: Versión 1.9; Escaneado de AAD a doble cara: Sí; Tamaño máximo de escaneado (superficie plana, AAD): 216 x 356 mm; Resolución óptica de escaneado: Hasta 1200 ppp

Funciones avanzadas del escáner

- Ajustes de imagen; Ajuste de calidad de salida; Resolución de escaneado seleccionable de 75 a 1200 ppp; Notificación de trabajos; Escanear y guardar en destinos: carpeta de red, ordenador , SharePoint, unidad flash USB, correo electrónico; OCR

Área escaneable

- Tamaño máximo de soportes (superficie plana) Tamaño máximo de soportes (superficie plana): 216 x 356 mm; Tamaño máximo de soportes (AAD) Tamaño máximo de soportes (AAD): 216 x 356 mm

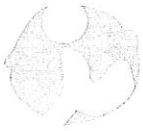
Profundidad de bits/niveles de escala de grises

- color de 24 bits; gris de 8 bits / 256

Envío digital

- Estándar: Escaneado a correo electrónico con búsqueda de direcciones de correo electrónico LDAP; Escaneado a carpeta de red; Escaneado a USB; Escaneado a SharePoint; Escaneado a ordenador con software; Archivo de fax a carpeta de red; Archivo de fax a correo electrónico; Fax a ordenador; Activar/desactivar fax; Activar/desactivar fax en color , control de acceso a color; Autenticación y autorización nativas.

Conectividad



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- 2 hosts USB 2.0 de alta velocidad; 1 dispositivo USB 2.0 de alta velocidad; 1 red Ethernet 10/100 Base-TX; 2 puertos de módem RJ-11/línea telefónica; Estación 802.11 b/g/n; Punto de acceso 802.11 b/g

Protocolos de red admitidos

- Configuraciones de protocolos de red admitidos (IPv4, IPv6); BOOTP; Cliente SMTP; LLMNR; Bonjour; LP/APIPA (IP automática); NetBIOS/WINS; LPD; Puerto sin procesar personalizado/Puerto 9100; DNS Resolver; DNS de multidifusión; SNMPv1/v2; SNMPv3; Detección de servicios web; Impresión de servicios web; Opciones DHCP: 81/RFC4702/RFC4704, 12-Nombre de host; 44; Syslog; Firewall; SSL/TLS (HTTPS); Servidor web integrado de red protegido por contraseña; Activar/desactivar puertos de red y funciones del dispositivo; Autenticación 802.1x con cables; Autenticación inalámbrica 802.1x (EAP-TLS y PEAP)

Capacidades de Red

- Estándar (Ethernet y Wi-Fi 802.11b/g/n integrados)

Manejo de papel

- Papel normal (ligero, intermedio, gramaje medio, gramaje alto, gramaje extra alto, perforado previamente, reciclado, grueso, otro papel normal de inyección de tinta), fotográfico (satinado, brillante, satinado suave, satinado, mate, otro papel fotográfico de inyección de tinta), sobres, etiquetas, tarjetas, papeles especiales (satinado y mate para folletos, tríptico para folletos, Hagaki, tarjetas de felicitación, otros papeles especiales de inyección de tinta)

Tamaño de soporte

- Personalizado (métrica) Personalizado (métrica): Bandeja 1: de 76 x 127 a 216 x 356 mm; Bandeja 2: de 102 x 210 a 216 x 297 mm; Bandeja 3 de 500 hojas opcional: De 102 x 210 a 216 x 356 mm Compatible (métrica) Compatible (métrica): Bandeja 1: Oficio, A4, A5, A6, B5 (JIS), B6 (JIS), 10 x 15 cm, sobres (B5, C5, C6, DL); Bandeja 2: A4, A5, B5 (JIS), sobres (DL, B5, C5); Bandeja 3: A4, A5, B5 (JIS)

Gestión de soportes

- Entrada estándar Entrada estándar: Bandeja de entrada de 500 hojas, bandeja multiuso de 50 hojas Salida estándar Salida estándar: Bandeja de salida de 300 hojas (boca abajo) Entrada opcional Entrada opcional: Bandeja opcional de 500 hojas, soporte y 2 bandejas de papel de 500 hojas AAD AAD: Estándar , 50 hojas

Gramaje de soportes

- Bandeja 1: de 60 a 120 g/m² (papel normal), de 125 a 300 g/m² (papel fotográfico), de 75 a 90 g/m² (sobre), de 120 a 180 g/m² (folleto), de 163 a 200 g/m² (tarjeta); Bandeja 2: de 60 a 120 g/m² (papel normal), de 125 a 250 g/m² (papel fotográfico), de 75 a 90 g/m²

Matamoros 319 Pte.
Monterrey, N.L. México

isssteleon.gob.mx

81.2020.9400 / 81.2033.9000



Gobierno de
Nuevo León



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

(sobre), de 120 a 180 g/m² (folleto), de 163 a 200 g/m² (tarjeta); Bandeja 3, 4: de 60 a 120 g/m² (papel normal), de 125 a 250 g/m² (papel fotográfico), de 120 a 180 g/m² (folleto), de 163 a 200 g/m² (tarjeta) Capacidad de entrada Máximo Máximo: Hasta 1550 hojas AAD AAD: Estándar , 50 hojas

Capacidad de salida

- Estándar Estándar: Hasta 300 hojas Sobres: Hasta 35 sobres Etiquetas: Hasta 100 hojas Tarjetas: Hasta 100 tarjetas Máximo Máximo: Hasta 300 hojas

Sistemas operativos Sistemas operativos compatibles compatibles

- Windows 10, Windows 8, Windows 7; OS X v10.11 El Capitan, OS X v10.10 Yosemite y OS X v10.9 Mavericks Lion; Linux (<http://www.hplip.net>)

Sistemas operativos de red Sistemas operativos de red compatibles compatibles

- Windows 10, Windows 8, Windows 7; Mac OS X v10.11 El Capitan, OS X v10.10 Yosemite y OS X v10.9 Mavericks; Windows Small Business Server 2011, Windows Small Business Server 2008 (64 bits), Windows Small Business Server 2003 (32/64 bits); Windows Server 2012, Windows Server 2008 (Standard Edition, Enterprise Edition, 32/64 bits), Windows Server 2008 R2 (Standard Edition, Enterprise Edition, 64 bits); Windows Server 2003 (Standard Edition, Enterprise Edition, 32/64 bits), Windows Server 2003 R2 (Standard Edition, Enterprise Edition, 32/64 bits); Windows Cluster (Windows Server 2008 R2), Windows Terminal Services (Windows Server 2008 R2), Windows 2003 Server Terminal Services con Citrix Metaframe XP de la versión 3, Windows Server 2003 Terminal Services con Citrix Presentation Server 4.0/4.5, Windows Server 2008 Terminal Services, Windows Server 2008 Terminal Services con Citrix XenApp, Citrix (impresión): Xen Server 5.6, Xen Desktop 5.5, Citrix XenApps 6.0, Citrix XenApp 6.5, Novell Netware 6/6.5/Open Enterprise Server 6.5 (solo se admite Novell iPrint); Linux

Gestión de seguridad Gestión de seguridad

- SSL/TLS (HTTPS), autenticación LDAP; Soluciones de autenticación de el fabricante y de otros fabricantes opcionales (p. ej., lectores de distintivos), IPP sobre TLS; WPA2-Enterprise con cables; Autenticación inalámbrica 802.1x (EAP-TLS, LEAP y PEAP); autenticación de clave previamente compartida para conexión inalámbrica (PSK); Firewall, configuración certificada; Bloqueo del panel de control; EWS protegido con contraseña; Desactivación de protocolos y servicios inactivos; Syslog; Firmware firmado; configuración de administrador; Control de acceso de autenticación y autorización nativos, control de acceso a color nativo; Desconexión de autenticación configurable; Impresión de PIN UPD; Modo Mopy a través de impresión de PIN.

Dimensiones y peso

- Mínimos 530 x 407 x 467 mm



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

- Máximo: 802 X 694 x 467 mm (con bandeja multiuso hacia abajo con extensión hacia afuera, bandeja principal extendida, extensión de la bandeja de salida en posición para papel legal)
- Peso: 22,15 kg

Alimentación

- Requisitos: Tensión de entrada: de 100 a 240 VCA (+/- 10%), 50/60 Hz (+/- 3 Hz)
- Consumo: 104 vatios (máximo), 46,8 vatios de media (impresión), 11,2 vatios (listo), 3,1 vatios (suspensión), 0,2 vatios (apagado manual)
- Consumo eléctrico típico (TEC): 0,994 kWh/semana
- Tipo de fuente de alimentación Tipo de fuente de alimentación: Fuente de alimentación incorporada.

Cerificaciones

- CISPR 22:2008-09/EN 55022:2010 (Clase B); CISPR 24:2010/EN 55024:2010; EN 61000-3-2:2006 +A1:2009 +A2:2009; EN 61000-3-3:2008; Directiva EMC 2004/108/EC con marca CE (Europa) EPEAT® Silver; CECP

Garantía

- Al menos de 2 años garantía, servicio y soporte in situ; soporte técnico por teléfono, chat y correo electrónico.



ISSSTELEON

Instituto de Seguridad y Servicios Sociales
de los Trabajadores del Estado de Nuevo León

Tiempo de Entrega

- 8 Semanas

Requisitos para el proveedor

- Carta de Distribuidor Autorizado de Computo
- Carta de Distribuidor Autorizado de Data Center
- Carta de Distribuidor Autorizado de Redes
- Carta de distribuidor Autorizado de Ciberseguridad
- Carta de Distribuidor Autorizado de Impresión

Monterrey, N.L. a 15 de abril de 2021

C.P. Dory Sislay Aldaco Nava
Encargada de la Dirección de Administración
Finanzas del ISSSTELEON

Cesar Alfredo Montfort Martínez
Administrador de Sistemas del ISSSTELEON