ANEXO TÉCNICO

Deberán cumplir mínimo las siguientes características técnicas:

Partida A **Suministro de Sistema de Alimentación Interrumpida** **Cantidad: 6**
Se requiere que se proporcione una solución de alimentación ininterrumpida que cumpla con las siguientes características técnicas mínimas: • Deberá soporta topología línea interactiva • Deberá soportar voltaje de entrada de 90Vac a 140Vac • Deberá soportar frecuencia de 57Hz a 63Hz • Deberá tener plug de conexión tipo NEMA 5-15P • El cable de poder deberá ser de al menos 3 metros. • Deberá soportar voltaje de salida de al menos 1000VA. • Deberá soportar al menos 600 Watts de salida. • Deberá soportar el tipo de onda simulada. • La batería deberá soportar voltajes de 120Vac con variación del diez por ciento hacia arriba y hacia abajo. • Deberá soportar frecuencias de más y menos del uno por ciento de 60Hz. • Deberá soportar al menos 6 salidas tipo NEMA 5-15R • Deberá soportar al menos 4 salidas con respaldo y protección contra sobretensiones. • Deberá soportar al menos 2 salidas solo con protección de sobretensiones. • Deberá soportar al menos 4ms en tiempo de transferencia. • Deberá proporcionar 13 minutos de respaldo a media carga y 3 minutos con carga completa. • Deberá soportar la administración remota. • Deberá de soportar la protección de picos de al menos 1030 Joules • Deberá tener la protección de datos para teléfono RJ11 • Deberá de tener indicadores de pantalla LCD de lectura. • Deberá ser de no más de una unidad de rack. • Deberá incluir 3 años de garantía tanto en equipo como en baterías. • Deberá ser equipo nuevo, no remanufacturado. **SERVICIO DE INSTALACIÓN** Se deberá incluir todo lo necesario para la correcta instalación y operación de la solución de sistema de alimentación ininterrumpida,

ANEXO TÉCNICO

- Se deberá incluir el suministro, instalación, puesta en marcha del equipo solicitado.
- Se deberá de considerar los servicios profesionales para la instalación, configuración y puesta en funcionamiento de la solución del sistema de alimentación ininterrumpida.
- Se deberá incluir como parte de los servicios la entrega de una memoria técnica al finalizar los servicios.
- Se deberá entregar las garantías/pólizas de soporte técnico del fabricante.
- Se deberá considerar que el o los equipos serán instalados en edificio dentro de la ciudad de Mérida, y como parte de su propuesta deberá considerar todos los gastos necesarios para la correcta implementación en sitio. La información y ubicación de dicho edificio será acordado con el Licitante ganador.
- Se deberá considerar que la convocante cuenta con una infraestructura de centro de datos la cual el Licitante dispondrá de unidades en rack de comunicaciones para poder realizar correctamente la instalación de los nuevos equipos.
- Se deberá considerar el correcto aterrizaje a tierra en el rack disponible de la convocante.

Partida B
Switch de acceso de 24 puertos POE
Cantidad: 6

Se requiere de una solución de conectividad tipo switch de acceso a nivel LAN que incluya lo siguiente:

- Se debe incluir todos los elementos necesarios para su correcta operación.
- Los equipos deberán ser capaces de soportar las nuevas tecnologías de seguridad, internet de las cosas, movilidad y nube.
- El equipo a ofertar deberá ser equipo nuevo de fábrica.

Características:

- Switch de Acceso de 24 puertos 10/100/1000 RJ-45 con PoE+ otorgando 30w por puerto
- El equipo deberá contar con 4 puertos 10 Gigabit SFP +
- El switch de acceso deberá de soportar un ancho de banda de reenvío de datos de 28 Gbps y un ancho de banda de conmutación de 56 Gbps.
- Deberá soportar una tasa de transferencia de 40 Mpps.
- El equipo deberá contar con una la capacidad de ser administrado con las siguientes opciones:
- El equipo deberá contar con los puertos de consola para la gestión de comandos CLI: RJ45, puerto USB mini-B y USB tipo A.
- Soportar una interfaz web amigable en la cual permita tener la posibilidad de configurar, gestionar, administrar el equipo. Esto ayudara al administrador a monitorear y diagnosticar problemas mucho más eficientes.
- El equipo deberá soportar nuevas tecnologías tales como en su hardware contar con Bluetooth de administración, el cual estará listo para poder administrar el equipo de forma

ANEXO TÉCNICO

inalámbrica. Este puerto Bluetooth deberá tener la dualidad de habilitar la administración vía web o por CLI.

- Deberá incluir la versión más reciente liberada, estable y libre de errores del sistema operativo con el que cuente el fabricante.
- Deberá soportar configuración vía línea de comando y conexión SSH v2
- Deberá soportar el protocolo SNMP v3.
- Deberá poder ser administrado vía puerto de consola
- Deberá soportar los siguientes grupos de RMON: históricos, estadísticas, alarmas y eventos
- El equipo deberá ser capaz de configurar puertos de monitoreo para análisis de tráfico por puerto o por vlan en el switch local o en cualquier otro switch dentro de la misma red.
- Deberá tener capacidad de implementar Syslog
- Proveer los beneficios de balanceo de carga de Layer 2.
- Deberá permitir Rapid Spanning Tree (rstp), Multiple Spanning Tree (MSTP), Per-VLAN Rapid Spanning Tree (PVRS+)
- Deberá tener la capacidad de mantener el PoE+ durante el reinicio del switch.

Estándares

- El equipo deberá de soportar los siguientes protocolos
- IEEE 802.1D STP
- IEEE 802.1p CoS Prioritization
- IEEE 802.1Q VLAN
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab LLDP
- IEEE 802.3ad
- IEEE 802.3ah
- IEEE 802.3x full duplex con puertos 10BASE-T, 100BASE-TX, and 1000BASE-T
- IEEE 802.3 10BASE-T
- IEEE 802.3u 100IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-X
- RMON I and II
- SNMP v1, v2c, y v3

ANEXO TÉCNICO

- IEEE 802.3az
- IEEE 802.3ae 10 Gigabit Ethernet
- IEEE 802.1ax
- IEEE 802.3af, IEEE 802.3at

Rendimiento del equipo.

- Deberá soportar 16,000 direcciones MAC en unicast
- Deberá soportar 542 rutas directas en unicast
- Deberá soportar hasta 1000 rutas multicast IPv4
- Deberá soportar hasta 256 VLAN activas.
- Deberá soportar 10,00 tramas Jumbo Ethernet
- Deberá soportar 4,000 VLAN IDs
- Deberá soportar la agregación de múltiples enlaces físicos para formar un solo enlace lógico de acuerdo al estándar IEEE 802.3ad.
- Deberá manejar 8 colas de prioridad por puerto.

Seguridad

- Deberá soportar RADIUS y TACACS.
- Deberá soportar DHCP server y DHCP snooping
- El equipo deberá de contar con mecanismos que eviten la ejecución de código en operación que sea apócrifo o modificado, que pueda generar vulnerabilidades como el filtrado de información, la modificación de la misma, o su pérdida total.
- Deberá contar con un mecanismo de arranque seguro
- Deberá manejar mecanismos de protección a las vulnerabilidades del protocolo ARP.
- El equipo deberá de ser capaz de prevenir que un usuario malicioso utilice la dirección IP válida de otro dispositivo de red.
- Deberá soportar IGMP snooping e IGMPv3.
- IGMP para IPv4 y para IPv6

Calidad de Servicio

- El equipo deberá de ser capaz asignar configuraciones de calidad de servicio de manera automática a los puertos conectados a dispositivos de Telefonía IP.
- El equipo deberá de soportar el protocolo 802.1p
- El equipo deberá soportar el protocolo DSCP.
- Deberá soportar hasta 8 colas de entrada, soportando el control de ancho de banda de salida

Regulaciones

ANEXO TÉCNICO

- El equipo deberá cumplir con las siguientes regulaciones de seguridad:
  - UL 60950-1 Segunda edición ó CAN/CSA-C22.2 No. 60950-1
  - 47CFR Part 15 Class A
  - EN55024
  - Reduction of Hazardous Substances (RoHS)

Licenciamiento

- El fabricante del switch deberá ofrecer un licenciamiento que tenga cobertura de soporte por parte del fabricante del equipo.

Garantía

Se deberá otorgar una garantía de 3 años con reemplazo de refacciones al siguiente día hábil.

Accesorios

Se deberá integrar los siguientes accesorios:

2 Modulos de fibra 10GBASE SR SFP por equipo

Credenciales del Partner:

Deberá demostrar con una carta emitida por el fabricante, el contar con un nivel de certificación de socio de al menos tipo GOLD.

En efectos de garantizar el correcto suministro, instalación y configuración de los equipos, el licitante deberá anexar 2 certificados ingenieros en la tecnología hardware de redes de nivel asociado, 2 certificados de ingenieros en la tecnología de hardware de redes de nivel profesional y al menos 4 certificados de ingenieros nivel experto en la marca y tecnología ofertada.

Servicio De Instalación

Se deberá incluir todo lo necesario para la correcta instalación y operación de los switches de acceso.

- Se deberá incluir el suministro, instalación, puesta en marcha del equipo solicitado y los accesorios solicitados.
- Se deberá de considerar los servicios profesionales para la instalación, configuración y puesta en funcionamiento de los switches de acceso.
- Se deberá incluir como parte de los servicios la entrega de una memoria técnica al finalizar los servicios.
- Se deberá entregar las garantías/pólizas de soporte técnico del fabricante.
- Se deberá considerar que el o los equipos serán instalados en edificio dentro de la ciudad de Mérida, y como parte de su propuesta deberá considerar todos los gastos necesarios para la correcta implementación en sitio. La información y ubicación de dicho edificio será acordado con el Licitante ganador.
- Se deberá considerar que la Convocante cuenta con una infraestructura de centro de datos la cual el Licitante dispondrá de unidades en rack de comunicaciones para poder

ANEXO TÉCNICO

realizar correctamente la instalación de los nuevos equipos.

- Se deberá considerar el correcto aterrizaje a tierra en el rack disponible de la Convocante.

Con el fin de garantizar la correcta ejecución de los servicios, se deberá incluir como parte de su propuesta técnica el certificado que avale a la persona que realizará funciones de Administrador de Proyectos con las capacidades de Project Management Professional (PMP).

Partida C
Suministro de Licencias EndPoint
Cantidad: 50

SUMINISTRO DE LICENCIAS ENDPOINT

Se requiere que el Licitante proporcione una solución de protección de punto final que cumpla con las siguientes características técnicas mínimas:

ADMINISTRACIÓN

Operacional

- La política deberá poder definir listas blancas para implementar excepciones a la política base.
- La solución deberá ser compatible con clientes locales y remotos independientemente de la red.
- La solución deberá tener una API profundamente funcional y documentada para admitir la integración y la automatización en toda la plataforma y con otras plataformas.
- La solución deberá tener una consola central para definir políticas, crear grupos de sistemas/usuarios, iniciar sesión, implementar actualizaciones, generar informes.
- La solución deberá tener soporte.
- Deberá proporcionar acceso basado en roles a la consola.
- Capacidad para excluir archivos y carpetas de los análisis. (Ejemplo: Exenciones para carpetas de bases de datos específicas).
- Capacidad para detener completamente el antivirus/EPP durante la instalación de la aplicación.
- Control granular de la funcionalidad.
- La solución deberá ser capaz de realizar operaciones de inserción en los clientes finales.
- La solución debería poder proporcionar una recopilación remota de registros de resolución de problemas.
- La solución debería permitir ejecutar un script de PowerShell remoto en el cliente.
- La solución deberá ser "Network Aware" y tener la capacidad de cambiar la política del cliente según su ubicación de red.

ANEXO TÉCNICO

- La solución deberá tener soporte para importar y prevenir IOC personalizados.
- El acceso a la consola deberá ser compatible con el uso de autenticación de sistemas de terceros.

Despliegue

- La solución deberá proporcionar métodos modernos y sencillos de implementación/instalación/desinstalación remota (incluida la compatibilidad con secuencias de comandos).
- La solución deberá tener la capacidad para la instalación remota nativa y la implementación del cliente sin el uso de herramientas de terceros.
- La solución deberá utilizar un "token de autenticación" para registrar de forma segura una nueva instalación de cliente en el servidor de gestión.
- La solución deberá permitir gestionar la versión del agente y los componentes desde la interfaz de gestión.

Nube

- La solución deberá proporcionar gestión como un servicio.
- La solución permite la selección de la región de la nube.
- La solución deberá tener copias de seguridad proporcionadas como parte del servicio.
- La solución deberá cumplir con el RGPD.
- La solución deberá tener una separación total de datos entre clientes.
- La solución de gestión deberá ser compatible con un cliente completo o un cliente ligero basado en web.
- La solución deberá tener autenticación de dos factores para el inicio de sesión del administrador.
- La autenticación web deberá admitir la autenticación SAML.
- La Convocante cuenta con una sola consola de gestión en la nube, por lo que el licitante deberá realizar el suministro sobre la base instalada actual.

Registro e informes

- La solución deberá poder proporcionar alertas de correo electrónico en tiempo real.

CLIENTE

Soporte de SO y VDI

- SO compatibles: Clientes Windows a partir del Windows 7 SP1 Pro +; Servidores Windows a partir del Windows 2008 R2 + Mac OS: 10.15 + (compatible con M1 completamente nativo) Linux: Debian v10, Ubuntu 18.04, CentOS 8, Red Hat Enterprise Linux 8.1
- La solución admite entornos VDI, tanto persistentes (flotantes) como no persistentes (dedicados). Los proveedores de Microsoft Terminal Server, Vmware Horizon y Citrix PVS/MCS son totalmente compatibles.

ANEXO TÉCNICO

- La solución deberá estar alineada y ser compatible con las últimas versiones del sistema operativo.
- Esta solución permitirá implementar el cliente y proteger las máquinas que se ejecutan en servidores de terminales y cajeros automáticos.
- Esta solución permite ejecutar funciones de protección de dispositivos habilitadas: HVCI, Credentials Guard y Windows Defender App Control.

Características del cliente

- El agente deberá ser liviano.
- La solución es configurable para una utilización mínima de los recursos del sistema.
- La solución deberá proporcionar la capacidad de ejecutarse en un hipervisor.
- La solución no afecta ni entra en conflicto con los controles de seguridad nativos integrados del sistema operativo u otras herramientas de seguridad empresarial actualmente integradas con Gold Load o las versiones estándar del servidor.
- La solución deberá proporcionar métodos modernos y sencillos de implementación/instalación/desinstalación remota (incluida la compatibilidad con secuencias de comandos).
- La solución permite actualizar a versiones más nuevas sin realizar un reinicio.
- El tamaño del paquete de la solución incluirá solo los componentes relevantes para implementar en un solo instalador.
- La solución deberá proporcionar capacidades de proxy para clientes que están fuera de línea y para limitar el uso del ancho de banda.
- La solución debería poder recuperar actualizaciones de firmas para Internet mediante un proxy NTLM autenticado con las credenciales de un usuario conectado.
- Al realizar actualizaciones, la solución descargará solo los cambios acumulados de la versión instalada.

Detección

- La solución deberá recopilar continuamente los eventos del sistema necesarios para la detección y el análisis. El proveedor deberá enumerar elementos específicos que se recopilan en tiempo real. (Los datos recopilados a través de secuencias de comandos posteriores al evento o la interacción en vivo con el host se tratan en un requisito separado). Los ejemplos deberán incluir, entre otros, eventos de proceso, modificaciones de archivos y registros, conexiones de red, actividad entre procesos, argumentos de línea de comando, eventos de Windows, consultas y respuestas de DNS.
- La solución deberá monitorear continuamente e informar los hallazgos lo más rápido posible. Si un endpoint no puede informar inmediatamente sobre los resultados, los resultados deberán almacenarse localmente hasta que puedan cargarse en el sistema de gestión central de la solución.
- La solución deberá permitir alertas en tiempo real o registro de eventos notables basados en contenido personalizado (comportamientos) o indicadores atómicos de compromiso

ANEXO TÉCNICO

basados en tipos de datos identificados por la solución.

- La solución deberá proporcionar una forma de garantizar que la información del proceso, los metadatos, las solicitudes de dns, las conexiones de red, los archivos binarios o cualquier otra información recopilada no se comparta con el proveedor o un tercero (por ejemplo, VirusTotal) sin una suscripción explícita.
- La solución deberá poder demostrar gráficamente la actividad del sistema (árboles de procesos u otro tipo de interfaz de mapeo) para ayudar en las investigaciones.
- La solución deberá capturar metadatos detallados sobre archivos binarios y procesos que se ejecutan en puntos finales. Los detalles deberán incluir, entre otros, el hash del binario (MD5, SHA-256), la información del editor, los detalles de la firma del código, la frecuencia observada en nuestro entorno, la información de la versión y el propietario del sistema de archivos.
- La solución deberá tener la capacidad de cambiar la marca de las notificaciones de los usuarios.
- La solución deberá tener la capacidad de controlar el nivel de mensajes para mostrar a los usuarios.

Respuesta

- La solución deberá proporcionar una forma de aislar un sistema que asegure que los controles preventivos se mantengan durante los reinicios. La configuración de aislamiento deberá estar preestablecida para permitir que el punto final se aísle de las amenazas pero pueda conectarse a los sistemas de investigación/remediación.
- La solución deberá ser capaz de aplicar inmediatamente controles preventivos (bloquear actividad específica o maliciosa conocida, etc.).
- La solución deberá tener una capacidad de respuesta en vivo que permita la capacidad de interactuar de forma remota con el sistema.
- La solución deberá proporcionar la capacidad de escribir una respuesta en vivo de forma condicional (es decir, si sucede X, entonces sucede Y).
- La solución deberá tener una sólida comunidad de intercambio de socios.
- La solución deberá permitir a los analistas la capacidad de alternar rápidamente entre diferentes actividades observadas en un punto final y proporcionar información contextual si está disponible.
- La solución deberá tener la capacidad de buscar en todos los puntos finales los IOC u otros atributos del sistema que no se capturan en los datos de telemetría en tiempo real.

Informes

- La solución no deberá exponer la actividad de un usuario a otro usuario que esté usando la misma máquina.

PROTECCIÓN DE DATOS Y DISPOSITIVOS

Protección de puertos

ANEXO TÉCNICO

- La solución deberá brindar administración de todos los puertos de punto final, con registro centralizado de la actividad del puerto para auditoría y cumplimiento.
- La solución permitirá notificaciones de mensajes de usuario personalizados al conectar un dispositivo según el escenario.

Cumplimiento

- La solución obligará a los terminales a cumplir con las reglas de seguridad definidas para la organización. Los equipos que no cumplan se mostrarán como no conformes y se les pueden aplicar políticas restrictivas.
- La solución hará cumplir las aplicaciones y los archivos requeridos en función de la configuración de cumplimiento al monitorear la presencia de archivos específicos, valores de registro y procesos que deberán estar ejecutándose o presentes en las computadoras finales.
- La solución hará cumplir las aplicaciones y los archivos prohibidos en función de la configuración de cumplimiento mediante la supervisión de la presencia de archivos específicos, valores de registro y procesos cuya ejecución o presencia está prohibida en los equipos terminales.
- La solución aplicará una verificación Anti-Malware para verificar que las computadoras tengan un programa anti-malware instalado y actualizado.
- La solución deberá admitir la integración con Windows Server Update Services (WSUS).

Cortafuegos

- La solución hará cumplir las reglas del cortafuegos para permitir o bloquear el tráfico de red a las computadoras finales en función de la información de conexión, como direcciones IP, puertos y protocolos.
- La solución se utilizará para determinar si los usuarios pueden conectarse a redes inalámbricas mientras se encuentran en la LAN de su organización para proteger la red de las amenazas asociadas con las redes inalámbricas.
- La solución definirá si los usuarios pueden conectarse a la red de la organización desde puntos de acceso en lugares públicos, como hoteles o aeropuertos.
- La solución se utilizará para restringir o permitir el tráfico de red IPV6.
- El Firewall del cliente de la solución deberá permanecer activo durante la actualización del cliente.
- La solución deberá incluir una opción para que Aislamiento de host aísle o permita un host específico (acceso a la red) que está bajo ataque de malware y presenta un riesgo de propagación.

Control de aplicaciones

- La solución se utilizará para restringir el acceso a la red para aplicaciones específicas. El administrador de Endpoint Security define políticas y reglas que permiten, bloquean o cancelan aplicaciones y procesos.
- La solución podrá incluir aplicaciones en la lista blanca o en la lista negra.

ANEXO TÉCNICO

- La solución deberá admitir la habilitación/deshabilitación del tráfico originado por los procesos WSL ("Subsistema de Windows para Linux").
- La solución se utilizará para restringir el acceso a la red para aplicaciones específicas. El administrador de Endpoint Security define políticas y reglas que permiten, bloquean o cancelan aplicaciones y procesos.
- La solución podrá incluir aplicaciones en la lista blanca o en la lista negra.
- La solución deberá admitir la habilitación/deshabilitación del tráfico originado por los procesos WSL ("Subsistema de Windows para Linux").

AntiMalware

- La solución deberá ser capaz de identificar la similitud de un archivo malicioso con una familia de malware conocida.
- La solución permitirá el escaneo programado de unidades locales, mensajes de correo. Unidades ópticas y dispositivos extraíbles.
- En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos.
- La solución deberá proporcionar una interfaz de línea de comandos para iniciar el análisis de malware.
- La solución deberá proporcionar una interfaz de línea de comandos para actualizar la base de datos de firmas antimalware.
- La solución deberá ser compatible con un Anti-malware compatible con DHS.
- La solución AV deberá ser capaz de proporcionar pruebas de que el escaneo se ha realizado en la mayoría de los archivos .DAT actuales o proporcionar un método de prueba igualmente eficaz que satisfaga los requisitos de auditoría para las soluciones AV sin DAT.
- La solución protegerá la computadora de todo tipo de amenazas de malware, desde gusanos y troyanos hasta adware y registradores de pulsaciones de teclas. La solución gestionará de forma centralizada la detección y el tratamiento de malware en los equipos finales.
- La solución permitirá el escaneo programado de unidades locales, mensajes de correo. Unidades ópticas y dispositivos extraíbles.
- Las soluciones deberán descargar firmas de un proxy NTLM autenticado con las credenciales de un usuario conectado.
- La solución debería poder usar un cliente dedicado como proxy para actualizaciones de firmas antimalware para clientes que están fuera de línea y no tienen una conexión directa a Internet o para limitar el uso de ancho de banda.
- En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos.

ANEXO TÉCNICO

Protección contra ransomware

- La solución protegerá contra ransomware existente y de día cero sin requerir actualizaciones de firmas.
- La solución reparará y restaurará los archivos que se cifraron durante un ataque de ransomware.
- La solución anti-ransomware tiene validación de terceros.

Protección conductual

- La solución aprovechará múltiples sensores para identificar de manera efectiva y única los comportamientos de malware genérico, así como los comportamientos específicos de la familia de malware.
- La solución prevendrá o detectará inmediatamente comportamientos maliciosos sin importar si la máquina está en línea o fuera de línea.
- La solución detectará y evitará ataques sin archivos utilizando únicamente procesos de Windows.
- La solución detectará y evitará ataques sin archivos basados en secuencias de comandos.
- La solución deberá proteger contra la técnica "Pass The Hash" para el robo de credenciales.
- La solución debería detectar archivos LNK (acceso directo de Windows) maliciosos.
- La solución deberá detectar la escalada de privilegios locales (LPE) de día cero.
- La solución se integrará con la interfaz de análisis antimalware (AMSI) de Microsoft para recibir y analizar scripts decodificados.

Modelos ML para análisis estático

- La solución deberá ser capaz de identificar archivos de día cero incluso si no están familiarizados con ningún servicio de reputación.
- Cualquier modelo de ML utilizado por el endpoint deberá actualizarse con frecuencia para protegerlo contra nuevos ataques de día cero.
- La solución deberá impedir que el usuario use archivos hasta que se verifiquen y se determine que son benignos.
- El Motor de Detección Estática de la solución deberá monitorear el acceso a los archivos.
- La solución deberá comprobar la reputación de los archivos en función del hash ssdeep/Fuzzy.

Anti-robot

- La solución identificará y bloqueará la comunicación saliente a sitios C&C maliciosos.
- Los recursos de inteligencia de amenazas en la nube se utilizarán para actualizaciones e identificación de ataques C&C de día cero.
- Tras un ataque de bot identificado, la solución remediará completamente el ataque

ANEXO TÉCNICO

dejando el punto final limpio e ileso.

Protección de navegación web

- Navegadores compatibles, al menos, Windows: Chrome, Edge (cromo), FireFox. Sistema operativo Mac: Safari, Chrome, FireFox.
- La solución deberá tener capacidades de limpieza sin hardware adicional. Los archivos entrantes se extraerán de todo el contenido malicioso potencial, como secuencias de comandos, macros y contenido activo.
- Al realizar la limpieza, el usuario final deberá poder acceder al archivo original si el sandbox lo considera benigno.
- Los archivos entrantes se emularán mediante sandboxing para contenido potencialmente malicioso.
- La solución detectará sitios de phishing de día cero que solicitan credenciales de usuario, incluso si los motores de reputación no los conocen.
- La solución deberá impedir que el usuario explore direcciones URL o dominios maliciosos conocidos.
- La solución deberá impedir que el usuario utilice sus credenciales corporativas en un sitio que no pertenezca al dominio corporativo.
- La solución deberá proporcionar filtrado de URL basado en categorías con una lista adicional en blanco y negro.
- La solución deberá aplicar la función "Búsqueda segura" cuando emplean los motores de búsqueda de Google, Bing y Yahoo.
- El usuario no deberá poder eliminar la protección de navegación de ninguna manera.

Sandboxing

- Todos los archivos escritos en el sistema de archivos serán monitoreados y analizados estáticamente. Si se encuentran como potencialmente maliciosos, los archivos serán emulados por sandboxing y puestos en cuarentena si se encuentran como maliciosos.
- La solución deberá ser capaz de limpiar completamente el endpoint de cualquier resto del ataque en caso de que el sandbox encontrara que el archivo es malicioso.

Prevención de exploits

- La solución detectará y evitará técnicas de explotación de software confiable.
- La solución tiene la capacidad de bloquear los nuevos ataques RDP RCE como BlueKeep en sistemas sin parches.

EDR

Análisis forense

- La solución creará automáticamente un análisis de incidentes para cada detección/prevención que ocurra. Este análisis deberá incluir árboles de ejecución de procesos incluso entre arranques si es relevante.

ANEXO TÉCNICO

- El informe forense identificará automáticamente el punto de entrada de la actividad maliciosa y resaltará el daño potencial, la acción de remediación y toda la cadena de ataque.
- La solución mejorará las detecciones de seguridad o antimalware de terceros mediante la creación y visualización automáticas de un informe de incidentes.
- El informe forense registrará, presentará y quitará la ofuscación de los scripts de PowerShell utilizados durante un ataque.
- La solución enumerará el análisis de reputación de los archivos, las URL y las IP utilizadas durante un ataque. La solución mostrará la geolocalización de IP como parte de la información de reputación.
- La solución podrá seguir métodos indirectos de ejecución utilizados por malware como llamadas WMI e inyecciones para poder rastrear la actividad de malware más avanzado.
- La solución deberá incluir los siguientes sensores: Servicio de ejecución remota Descubrimiento del proceso de creación Descubrimiento de la ventana de la aplicación Tarea programada Captura de pantalla Captura de entrada DDE (intercambio dinámico de datos).
- La solución creará un informe de incidentes que mostrará el incidente en términos de Mitre ATT&CK Matrix.
- La solución permitirá la búsqueda de múltiples tipos de datos de sensores no detectados, incluidos datos de archivo, proceso, red, registro, inyección y usuario.
- La solución permitirá la remediación de cualquier archivo o proceso que se encuentre a través de la plataforma EDR.
- La solución permitirá el análisis forense y el informe de cualquier indicador encontrado a través de la plataforma EDR.
- La solución proporcionará múltiples opciones de remediación manual, como Cuarentena, Proceso de eliminación y Análisis forense con remediación.
- La solución proporcionará una capacidad de gestión central para aislar las máquinas de forma remota.
- La solución permitirá la búsqueda de incidencias mediante técnicas de Mitre Att&ck.
- La solución deberá tener la capacidad de ver las direcciones MAC de cada computadora que envíe datos.
- La solución EDR deberá proporcionar datos relacionados con periféricos y dispositivos de almacenamiento externo.
- La solución enriquecerá automáticamente los resultados de búsqueda con reputación.

REGISTRO E INFORMES

Informes

- La solución debería generar informes periódicos sobre tipos de malware, tipos de vulnerabilidades explotadas, etc.

ANEXO TÉCNICO

- La solución deberá tener la capacidad de generar informes visuales.
- La solución deberá proporcionar el estado de salud del agente.

Registros

- La solución deberá mostrar el proceso afectado, las claves de registro afectadas y los archivos afectados en el entorno del sistema operativo.
- La solución mostrará capturas de pantalla y videos de emulación de archivos maliciosos en el entorno Sandbox.
- La solución debería poder registrar la comunicación de C&C desde el archivo BOT emulado.

CUMPLIMIENTO DE LA NORMATIVA

La solución deberá cumplir con al menos:

- Reglamento Internacional de Tráfico de Armas (ITAR).
- Ley Federal de Gestión de la Seguridad de la Información (FISMA).
- Marco de gestión de riesgos del Departamento de Defensa (RMF).
- Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).
- Normas de seguridad de la industria de tarjetas de pago (PCI).
- Directiva de la comunidad de inteligencia (ICD) 503.
- La solución deberá cumplir con las regulaciones de GDPR.

Inteligencia de amenazas

Nube

- La solución deberá actualizarse dinámicamente en función de una red global de sensores de amenazas mediante el intercambio de datos de amenazas.

VIGENCIA

Deberá considerar una vigencia de Licenciamiento y Soporte directo por parte del fabricante de al menos 24 meses.

La solución de seguridad deberá contar con un soporte de fabricante con al menos los siguientes alcances:

- Soporte de fabricante 24x7, con opción de que la Convocante puede solicitar soporte de manera directa.
- Soporte telefónico y por correo electrónico
- Solicitudes de soporte ilimitado
- Acceso a la base de datos de conocimientos
- Acceso a actualizaciones mayores y mejoras

ANEXO TÉCNICO

- Acceso a Hot Fixes y paquetes de servicio

Carta por parte del fabricante.

- El Licitante deberá demostrar ser un socio autorizado (al menos socio nivel 4 o su equivalente) en la marca ofertada, mediante carta expedida directamente por el fabricante, dicha carta deberá ser firmada por el representante legal del fabricante en México.

- El licitante deberá demostrar los siguientes certificaciones: 2 certificados nivel experto en resolución de problemas de la marca ofertada y 1 certificado de nivel experto en seguridad de la marca ofertada, dichas certificaciones deberán de estar vigentes.

SOPORTE TÉCNICO PARA LICENCIAS ENDPOINTS

El Licitante deberá brindar soporte técnico a solución de protección de puntos finales por al menos 2 años, los alcances del soporte técnico cumplir con:

- Deberá contar con una mesa de ayuda para la recepción de solicitudes de atención con un esquema de atención 24x7.

- Deberá contar con soporte técnico durante la vigencia del servicio con atención en un esquema de tipo 5x8.

- Deberá incluir soporte técnico por medio telefónico, remoto y email.

- Deberá incluir soporte técnico en las configuraciones y resolución de dudas sobre la administración de la solución de seguridad.

- Deberá incluir acciones correctivas y resolución de problemas para incidencias.

- Apertura de casos y seguimiento puntual con fabricante para incidencias.

- El licitante deberá mantener actualizada la solución de seguridad durante la vigencia del servicio.

- El licitante deberá proporcionar soporte técnico a través de un centro SOC (Security Operation Center) propietario.

- Deberá alinear todos sus procesos a las mejores prácticas ITIL, ISO27001:2022, 20000-1:2018, ISO 37001:2016 y 9001:2015. El Licitante deberá proporcionar como parte de su propuesta técnica los certificados que demuestran el cumplimiento de dichos estándares.

- El SOC deberá pertenecer al grupo de respuesta de incidencias FIRST.

- Deberá alinear todos sus procesos a las mejores prácticas ITIL, deberá incluir como parte de su propuesta los certificados de al menos 3 personas que cuenten con certificación ITIL Foundation e ITIL OSA.

ANEXO TÉCNICO

Partida D
Switch de Acceso de 48 Puertos
Cantidad: 2

SWITCH DE ACCESO de 48 PUERTOS

Se requiere de una solución de conectividad tipo switch de acceso a nivel LAN que incluya lo siguiente:

- Se debe incluir todos los elementos necesarios para su correcta operación.
- Los equipos deberán ser capaces de soportar las nuevas tecnologías de seguridad, internet de las cosas, movilidad y nube.
- Deberán ser equipos nuevos, no remanufacturados.

Características:

- Switch de Acceso de 48 puertos 10/100/1000 Ethernet
- El equipo deberá contar con 4 puertos 10 Gigabit SFP+
- El switch de acceso deberá de soportar un ancho de banda de reenvío de datos de 52 Gbps y un ancho de banda de conmutación de 100 Gbps.
- Deberá soportar una tasa de transferencia de 77 Mpps.
- El equipo deberá contar con una la capacidad de ser administrado con las siguientes opciones:
- El equipo deberá contar con los puertos de consola para la gestión de comandos CLI: RJ45, puerto USB mini-B y USB tipo A.
- Soportar una interfaz web amigable en la cual permita tener la posibilidad de configurar, gestionar, administrar el equipo. Esto ayudara al administrador a monitorear y diagnosticar problemas mucho más eficientes.
- El equipo deberá soportar nuevas tecnologías tales como en su hardware contar con Bluetooth de administración, el cual estará listo para poder administrar el equipo de forma inalámbrica. Este puerto Bluetooth deberá tener la dualidad de habilitar la administración vía web o por CLI.
- Deberá incluir la versión más reciente liberada, estable y libre de errores del sistema operativo con el que cuente el fabricante.
- Deberá soportar configuración vía línea de comando y conexión SSH v2
- Deberá soportar el protocolo SNMP v3.
- Deberá poder ser administrado vía puerto de consola
- Deberá soportar los siguientes grupos de RMON: históricos, estadísticas, alarmas y eventos
- El equipo deberá ser capaz de configurar puertos de monitoreo para análisis de tráfico por

ANEXO TÉCNICO

puerto o por vlan en el switch local o en cualquier otro switch dentro de la misma red.

- Deberá tener capacidad de implementar Syslog
- Proveer los beneficios de balanceo de carga de Layer 2.
- Deberá permitir Rapid Spanning Tree (rstp), Multiple Spanning Tree (MSTP), Per-VLAN Rapid Spanning Tree (PVRS+)

Estándares

- El equipo deberá de soportar los siguientes protocolos
- IEEE 802.1D STP
- IEEE 802.1p CoS Prioritization
- IEEE 802.1Q VLAN
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab LLDP
- IEEE 802.3ad
- IEEE 802.3ah
- IEEE 802.3x full duplex con puertos 10BASE-T, 100BASE-TX, and 1000BASE-T
- IEEE 802.3 10BASE-T
- IEEE 802.3u 100IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-X
- RMON I and II
- SNMP v1, v2c, y v3
- IEEE 802.3az
- IEEE 802.3ae 10 Gigabit Ethernet
- IEEE 802.1ax

Rendimiento del equipo.

- Deberá soportar 16,000 direcciones MAC en unicast
- Deberá soportar 542 rutas directas en unicast
- Deberá soportar hasta 1000 rutas multicast IPv4
- Deberá soportar hasta 256 VLAN activas.
- Deberá soportar 10,00 tramas Jumbo Ethernet
- Deberá soportar 4,000 VLAN IDs

ANEXO TÉCNICO

- Deberá soportar la agregación de múltiples enlaces físicos para formar un solo enlace lógico de acuerdo al estándar IEEE 802.3ad.
- Deberá manejar 8 colas de prioridad por puerto.

Seguridad

- Deberá soportar RADIUS y TACACS.
- Deberá soportar DHCP server y DHCP snooping
- El equipo deberá de contar con mecanismos que eviten la ejecución de código en operación que sea apócrifo o modificado, que pueda generar vulnerabilidades como el filtrado de información, la modificación de la misma, o su pérdida total.
- Deberá contar con un mecanismo de arranque seguro
- Deberá manejar mecanismos de protección a las vulnerabilidades del protocolo ARP.
- El equipo deberá de ser capaz de prevenir que un usuario malicioso utilice la dirección IP válida de otro dispositivo de red.
- Deberá soportar IGMP snooping e IGMPv3.
- IGMP para IPv4 y para IPv6

Calidad de Servicio

- El equipo deberá de ser capaz asignar configuraciones de calidad de servicio de manera automática a los puertos conectados a dispositivos de Telefonía IP.
- El equipo deberá de soportar el protocolo 802.1p
- El equipo deberá soportar el protocolo DSCP.
- Deberá soportar hasta 8 colas de entrada, soportando el control de ancho de banda de salida

Regulaciones

- El equipo deberá cumplir con las siguientes regulaciones de seguridad:

o UL 60950-1 Segunda edición ó CAN/CSA-C22.2 No. 60950-1

o 47CFR Part 15 Class A

o EN55024

o Reduction of Hazardous Substances (RoHS)

Licenciamiento

- El fabricante del switch deberá ofrecer un licenciamiento que tenga cobertura de soporte por parte del fabricante del equipo.

Garantía

Se deberá otorgar una garantía de 3 años con reemplazo de refacciones al siguiente día hábil.

Accesorios

ANEXO TÉCNICO

Se deberá integrar los siguientes accesorios:

2 Modulos de fibra 10GBASE SR SFP por equipo

Credenciales del Partner:

Deberá demostrar con una carta emitida por el fabricante, el contar con un nivel de certificación de socio de al menos tipo GOLD.

En efectos de garantizar el correcto suministro, instalación y configuración de los equipos, el licitante deberá anexar 2 certificados ingenieros en la tecnología hardware de redes de nivel asociado, 2 certificados de ingenieros en la tecnología de hardware de redes de nivel profesional y al menos 4 certificados de ingenieros nivel experto en la marca y tecnología ofertada.

Servicio De Instalación

Se deberá incluir todo lo necesario para la correcta instalación y configuración de los switches de acceso.

- Se deberá incluir el suministro, instalación, puesta en marcha del equipo solicitado.
- El Licitante deberá de considerar los servicios profesionales para la instalación, configuración y puesta en funcionamiento de los switches de acceso.
- El Licitante deberá incluir como parte de los servicios la entrega de una memoria técnica al finalizar los servicios.
- El Licitante deberá entregar las garantías/pólizas de soporte técnico del fabricante.
- El Licitante deberá considerar que el o los equipos serán instalados en edificio dentro de la ciudad de Mérida, y como parte de su propuesta deberá considerar todos los gastos necesarios para la correcta implementación en sitio. La información y ubicación de dicho edificio será acordado con el Licitante ganador.
- El licitante deberá considerar que la Convocante cuenta con una infraestructura de centro de datos la cual el Licitante dispondrá de unidades en rack de comunicaciones para poder realizar correctamente la instalación de los nuevos equipos.
- El licitante deberá considerar el correcto aterrizaje a tierra en el rack disponible de la Convocante.

Con el fin de garantizar la correcta ejecución de los servicios, el Licitante deberá incluir como parte de su propuesta técnica el certificado que avale a la persona que realizará funciones de Administrador de Proyectos con las capacidades de Project Management Professional (PMP).

Partida E
Punto de Acceso Wifi para Interior
Cantidad: 15

PUNTO DE ACCESO WI-FI PARA INTERIOR

Se requiere que el Licitante proporcione una solución punto de acceso para interior que cumpla con las siguientes características técnicas mínimas:

- Deberá soportar Wi-Fi 802.11 a/b/g/n/ac Wave 2

ANEXO TÉCNICO

- Deberá soportar transmisiones de 5 GHz y 2.4GHz.
- Deberá poder soportar la administración mediante la nube, de manera local en las premisas de la Convocante o de manera independiente.
- Deberá estar equipado con 2 radios: Un radio de 5GHz (802.11 a/n/ac Wave 2), 4x4 y otro de 2.4 GHz (802.11 b/g/n), 2x2.
- Deberá soportar SU-MIMO / MU-MIMO: 4 transmisiones.
- Deberá soportar seguridad en los nombres de red Wi-Fi: WPA2 (802.11i), WPA2 Enterprise (802.1x/EAP), WPA PSK, Abierto.
- Deberá soportar tasa de transferencia física máxima de: 400Mbps en radio de 2.4 GHz y 1700Mbps en radio de 5.2GHz.
- Soporte de Antena tipo omnidireccional interna
- Deberá de proveer una máxima ganancia de: 27.5 dBm y de 27.25 dBm en 2.4 GHz y 5.2 GHz respectivamente.
- Máximo de clientes: 512
- Máximo de SSID: 32
- Deberá soportar en WLAN: WPA-TKIP, WPA2 AES, 802.1x, 802.11w PMF
- Deberá soportar carga de alimentación típica 12 W
- Deberá soportar carga de alimentación máxima: 22W
- Deberá soportar alimentación vía Ethernet: 802.3af o 802.3at
- Deberá poder ser montado en escritorio, en pared y techo
- Deberá incluir los accesorios necesarios para su correcta instalación física.
- Deberá soportar temperaturas de operación de cero grados centígrados a cincuenta grados centígrados.
- Deberá contar con las siguientes certificaciones: Wi-Fi Alliance 802.11 a/b/g/n/ac, Passpoint 2.0 FCC, ETSI, CE, EN 60601-1-2, IEC60950 Ul2043
- Deberán ser equipos nuevos, no remanufacturados.

Garantía

- Deberá incluir garantía de fabricante por 5 años.

Sistema de Gestión

Se deberá proveer un sistema de administración en la nube para todos los puntos de acceso requeridos en las presentes bases.

Deberá contar con las siguientes características mínimas:

- Deberá soportar interfaces:
    - HTTP / HTTPS web interface, SSL, Telnet

ANEXO TÉCNICO

- SNMP V1, V2, V3
- Syslog, SNMP traps, NTP

- Deberá soportar la implementación:
  - Nube pública
  - Nube privada
  - Local.
- Deberá soportar la visualización de:
  - Dispositivos inalámbricos
  - Dispositivos cableados.
- Deberá soportar el aprovisionamiento sin intervención
- Se deberá poder crear, aprovisionar y supervisar desde un único panel.
- Deberá poder desplegar métricas clave de rendimiento, alarmas y alertas.
- Deberá estar diseñada para brindar escala y seguridad en todos los niveles.
- La conexión de los dispositivos a ser administrados por la herramienta de administración en la nube deberá ser vía SSL.
- Deberá soportar hasta un máximo de 10,000 dispositivos administrados.
- Deberá incluir herramientas de resolución de problemas como ping, traceroute, rendimiento y captura de paquetes.
- Deberá admitir jerarquías de red personalizada.
- Deberá soportar el proporcionar una vista empresarial y una vista de proveedor de servicios.
- Deberá soportar el monitoreo:
  - Paneles de dispositivos dedicados
  - Estadísticas y tendencias
  - Alertas de correo, Syslog, Webhooks
- Administración:
  - Basado en roles
  - RADIO, TACACS+, LDAP y AD LOGIN
- Gestión:
  - Vista simplificada Wireless LAN
  - Grupos de AP y Configuración WLAN
- Seguridad:

ANEXO TÉCNICO

- Comunicación a través SSL.
- Sin acceso entrante a internet.
- Recuperación ante desastres.

Accesorios

Deberá suministrar una fuente de alimentación tipo PoE, con las características técnicas mínimas siguientes:

- Que soporte voltaje salida: 56 Vdc +/-5%
- Que soporte voltaje de entrada de: 90-264 Vac
- Soportar la frecuencia de entrada de 47 a 63 Hz
- Deberá soportar una eficiencia igual o mayor al 85%
- Deberá soportar en operación, temperaturas de 0 a 40 grados centígrados
- Deberá ser de la misma marca de los puntos de acceso.
- Deberá ser equipo nuevo, no remanufacturados.

Servicio De Instalación

Se deberá incluir todo lo necesario para la correcta instalación y configuración de los puntos de acceso Wi-Fi.

- Se deberá incluir el suministro, instalación, puesta en marcha del equipo solicitado.
- El Licitante deberá de considerar los servicios profesionales para la instalación, configuración y puesta en funcionamiento de los puntos de acceso Wi-Fi.
- El Licitante deberá incluir como parte de los servicios la entrega de una memoria técnica al finalizar los servicios.
- El Licitante deberá entregar las garantías/pólizas de soporte técnico del fabricante.
- El Licitante deberá considerar que el o los equipos serán instalados en edificio dentro de la ciudad de Mérida, y como parte de su propuesta deberá considerar todos los gastos necesarios para la correcta implementación en sitio. La información y ubicación de dicho edificio será acordado con el Licitante ganador.
- El Licitante deberá considerar todos los trabajos necesarios para instalar físicamente los equipos en las ubicaciones designadas por la convocante. Las ubicaciones, condiciones de acceso y distribución serán acordadas con el licitante ganador previo a la ejecución de dichos servicios.

Con el fin de garantizar la correcta ejecución de los servicios, el Licitante deberá incluir como parte de su propuesta técnica el certificado que avale a la persona que realizará funciones de Administrador de Proyectos con las capacidades de Project Management Professional (PMP).

ANEXO TÉCNICO

Partida F
Suministro de toma corriente
Cantidad: 4

SUMINISTRO DE TOMACORRIENTE

Se requiere que el Licitante suministre tomacorriente con supresor de picos que cumpla con las siguientes características técnicas mínimas:

- Que soporte voltaje de operación: 120Vca@60Hz.
- Deberá contar con fusible térmico: 15A.
- Deberá contar cable de alimentación de 1.8m de largo con terminal de clavija polarizada IEC tipo C13.
- Deberá soportar filtro EMI/RFI (100KHz - 10MHz) - 70dB.
- Deberá soportar Protección: 150V CA y 200V CD continuo
- Deberá soportar tecnología MOV (Metal Oxide Varistor) con fusible térmico de alta precisión.
- Deberá soportar al menos protección transitoria por modo: 20kA.
- Deberá soportar protección transitoria de línea: 40kA.
- Deberá contar con protección de línea: 480J.
- Deberá contar con indicadores visuales.
- Deberá tener tres modos de protección L-N, L-G y N-G.
- Deberá tener led´s indicadores de protección activa en tiempo real en los modos de protección L-N y L-G.
- Deberá proveer 10 contactos perfectamente polarizados NEMA 5-15R, 8 en la parte trasera y 2 en la parte frontal del supresor.
- Deberá soportar la instalación en gabinete de acero (montable en rack de 19”)
- Deberá soportar temperatura de operación: -10°C ~ 60°C.
- Deberá soportar humedad relativa: 0% ~ 95%.
- Deberá contar con garantía de fabricante por 1 año.

ANEXO TÉCNICO

Partida G **Suministro de charola de estante de dos piezas** **Cantidad: 25**
SUMINISTRO DE CHAROLA DE ESTANTE DE DOS PIEZAS. Se requiere que el Licitante suministre charola de estante de dos piezas para instalar en los rieles trasero y delantero de los racks de 2 postes que cumpla con las siguientes características técnicas mínimas: o Deberá contar con tipo de producto estante de rack o Deberá ser de material aluminio o Deberá poder instalarse en rack de 19 pulgadas o Deberá de tener una altura extendida de 4.58 in o Deberá de tener anchura total de 19.24 o Deberá de tener una profundidad extendida de 12.45 in o Deberá ser de 3 unidades de rack o Deberá poder soportar carga estática de hasta 90.72 Kg. o Deberá ser de color negro o Deberá cumplir con las siguientes normas: Cumple con la directiva RoHS o Deberá incluir con 2 medios estantes y material de montaje

Partida H **Plataforma de gestión CICERO para salas orales** **Cantidad: 4 salas**	
Funcionalidades de la solución	● La solución a proveer deberá permitir implementar una solución completa de Videograbación de audiencias en las Sala de oralidad, con los siguientes requisitos mínimos: ✓El sistema de grabación de audio y video debe ser en español, así como sus manuales técnicos y de uso, y el servicio de soporte. ✓Debe ser capaz de incluir en las bases de datos tanto locales como centrales la información de los procedimientos laborales vigentes en el estado de Yucatán. ✓Debe ser capaz de incluir en las bases de datos tanto locales como centrales, la información de los diferentes órganos judiciales, existentes en las leyes vigentes

ANEXO TÉCNICO

	● El software deberá tener los niveles de calidad adecuados. Deberán acreditarse por certificaciones ISO/IEC 33000 e ISO/IEC 12207 de Nivel de Madurez Procesos del ciclo de vida software, presentándose dichos certificados en el anexo técnico. No se aceptará a los licitantes ninguna otra certificación por parte de otras entidades. ● La grabación deberá permitir en forma manual y automática la generación de marcas adicionales a la grabación que permitan poder ser localizadas en el archivo digital, a fin de poder reproducir a partir de dichas marcas. Se deberá proveer la documentación sobre el formato del archivo de dichas marcas a fin de poder ser utilizado el mismo ● El formato de registro de audio y video deberá ser un formato digital estándar Windows Media. ● Deberá de estar desarrollado e implantado sobre plataformas abiertas Windows: ✓Windows 10pro o superior, para el servidor de Sala de oralidad. ● El sistema de sala deberá poseer mecanismos de respaldo de la información tanto manual como automática. En particular será posible para las salas autónomas, (i) un mecanismo de backup a pen-drive o disco duro de videos, pruebas y metadatos, reingestable tanto de forma local como a servidores. ● Los sistemas de sala y los servidores sincronizarán sus contenidos en las dos direcciones, ascendente y descendente, independientemente del punto donde el usuario final haya introducido los datos. ● Deberá disponer de un módulo de preparación del Juicio previo a la celebración de la audiencia, con los datos del expediente judicial, intervinientes, jueces… ● Deberá generar un acta, oficio u escrito de la sesión durante el proceso de grabación, tanto manual como automática, desde la misma herramienta de grabación. En particular, el acta automática podrá incorporar sin intervención humana adicional los comentarios introducidos durante la grabación del juicio oral ● Dispondrá de un Módulo de Pruebas con capacidad para adjuntar documentación electrónica (documentos de texto, hojas de cálculo, imágenes, archivos escaneados, audio y/o video adicionales a la grabación), de todas aquellas pruebas que se aporten durante la celebración del Juicio Oral. La prueban podrán incorporarse en

ANEXO TÉCNICO

	cualquier momento del acto del juicio oral, sin interrumpir la grabación del mismo. ● El sistema debe tener la capacidad de generar copias restringidas de las grabaciones para distribución a las partes, con el mismo visor de la Sala, videos y etiquetas, además de una herramienta integrada y de fácil uso, para la grabación en CD/DVD/USB. ● El sistema permitirá que el secretario judicial o un funcionario habilitado para ello, bloquee la generación de copias hasta que el video y audio sean revisados y autorizados por dicha autoridad. Dicha autorización podrá llevarse a cabo tanto en el momento del juicio oral, como posteriormente, para lo cual el funcionario habilitado podrá visualizar la grabación, comentarios y pruebas del juicio previamente a su autorización desde la interfaz del navegador web. ● El sistema debe permitir establecer filtros de audio y video para distorsionar la voz y ocultar la imagen, para toma de declaración de testigos protegidos, menores… ● El tramo de video ya grabado podrá visualizarse durante la realización del propio juicio sin necesidad de interrumpir la grabación del mismo. ● El sistema deberá tener la capacidad de gestión de los recursos de Sala de oralidad del edificio judicial (sistema de reserva de salas), incluyendo fecha y hora. La reserva estará asociada a un órgano judicial y a un procedimiento y requerirá la autorización por parte de un funcionario habilitado para ello (secretario judicial, etc…). Soportará identificación mediante certificado electrónico a estos efectos. ● Deberá tener la capacidad de integrar los sistemas de videoconferencia más extendidos en el mercado, indexando las intervenciones a través de la videoconferencia, de la misma forma en que se realiza con los intervinientes presentes en la Sala de oralidad. ● El módulo de consulta de los videos debe integrar los datos asociados (documentos adjuntos, datos del expediente…), así como presentar de manera unificada todas las actuaciones judiciales relacionadas con el proceso seleccionado. ● El módulo de consulta permitirá también la búsqueda y acceso a la información dentro del audio y el video, a través de los tags o etiquetas agregadas antes, durante o después de la actividad, sean

ANEXO TÉCNICO

	juicios o audiencias. ● Deberá disponer en el Sistema Central, de un módulo de consulta con interfaz web para la búsqueda y acceso a la información desde cualquier punto de la intranet judicial ● La calidad y tasa de almacenamiento de la grabación de vídeo debe ser configurable. ● El sistema dispondrá de un módulo de administración tanto a nivel de sala, como a nivel de servidores centrales. ● El sistema controlará el acceso de usuarios y bitácora de acciones realizadas en el sistema. ● El sistema debe permitir la firma digital de los archivos generados con el fin de garantizar la integridad de la información grabada utilizando formatos CAdES, XAdES y con sellado de tiempo. ● El sistema permitirá a usuarios que sean secretarios de un órgano judicial o habilitados, la realización de la firma de distribución para las actuaciones en las que no fue realizada tras su captura mediante un mecanismo de buzón web. ● Deberá integrarse con Active Directory de Windows. ● Deberá tener la capacidad de integrarse con sistemas de información al Público mediante mecanismos de servicios web. ● El sistema permitirá al magistrado, secretario judicial o autoridad habilitada para ello, la eliminación de entradas y colas (partes iniciales y finales) de una grabación de un juicio, forzando en este caso la realización de nuevo de todos los procedimientos de firma digital y garantía de integridad de los contenidos. La eliminación de entradas y colas de video y audio deberá ser parte integral del sistema, no una herramienta externa al mismo. ● Los archivos de las grabaciones deben almacenarse en formato encriptado, con controles de seguridad para impedir la manipulación de su contenido. ● Solución “llave en mano” que incluya todo el software y hardware necesario para la correcta operación de los sistemas de grabación. Deberá dejarse la solución debidamente instalada y funcionando, con los respectivos manuales en español. ● La grabación será realizada completamente en el equipamiento instalado en la sala, el cual deberá permitir la grabación en sonido y audio aun cuando estuviera desconectado o interrumpida su

ANEXO TÉCNICO

	interconexión a la red de datos y/o sistemas anexos a la solución planteada. ● Se deberá permitir realizar la grabación de solo audio en aquellos actos donde se determine que no sea necesario la grabación de video. ● Debe de disponer de un sistema de alertas de fallas para micrófonos, cámaras, corriente eléctrica y espacio en disco, tanto local, como para supervisión remota; siendo su gestión realizada directamente desde la aplicación software. ● El equipamiento de sala que pudiera comprender la solución deberán permitir controlar y supervisar el nivel de grabación de cada sala, así como el funcionamiento de cada micrófono, a fin de comprobar el normal funcionamiento del equipamiento. ● La solución deberá proveer un aplicativo para el resguardo de copias de seguridad de las grabaciones digitales en forma asincrónica con la grabación en servidores centrales. ● La solución no deberá permitir el borrado de los archivos de registros de grabación sin haber realizado su resguardo en forma previa. ● La solución deberá permitir realizar copias de Seguridad en otros dispositivos mediante protocolos FTP, NFS o Similares con acceso restringido a fin de acceder a los archivos digitales para su copia. ● El sistema debe permitir especificar si el acto del juicio oral es público o privado. ● Todos los componentes de la Solución deberán proveer un adecuado nivel de seguridad en su acceso permitiendo definir perfiles y sus permisos de acceso de acuerdo a la función del personal en la administración y operación del sistema en todos sus componentes. ● El sistema deberá poder operar de forma autónoma en caso de no disponibilidad de servicios residentes en infraestructuras externas a la Sala de oralidad ● El sistema podrá incorporar un módulo de procesamiento de audio que permita generar índices de forma automática. ● El sistema permitirá realizar búsqueda por palabras y acceder de forma inmediata a la grabación de audio o audio/video al preciso momento en que se dice esa palabra.

ANEXO TÉCNICO

	● El sistema podrá generar un acta escrita y acceder de forma inmediata a cualquier parte de la grabación a partir de dicha acta ● El sistema dispondrá de un API (Interfaz de Programación de Aplicaciones) que permita su integración con sistemas de terceros. Dicha API estará basada en Servicios Web. ● El sistema deberá incluir, como parte integral de la solución, un sistema de mensajería que permita notificaciones al secretario judicial o fedatario público acerca de incidencias en juicio oral: ✓Anulación de una reserva de sala ✓Inicio de grabación ✓Pausa de una grabación ✓Comentario en vivo ✓Mensaje desde buzón ✓Resultado de tarea de backup ✓Resultado de tarea de restore ✓Anulación de autorización de reserva de sala ✓Reanudación de grabación tras pausa ✓Finalización de actuación ✓Aplazamiento de actuación ✓Fallo en hardware de audio ✓Fallo en hardware de video ✓Autorización de pausa en grabación ● Esta funcionalidad deberá tener dos partes diferenciadas. ● La primera deberá ser un buzón de entrada, en el que el usuario recibe notificaciones ocurridas en actuaciones de las que es secretario, y no estaba presente en la grabación. ● La segunda deberá ser un buzón de salida, que envíe mensajes de las actuaciones en las que el usuario realizó la grabación, siendo otro el secretario asociado a las mismas. ● Deberá permitir la visualización en tiempo real mediante streaming por la red IP, siempre y cuando así lo autorice el Magistrado, del Juicio Oral que se esté celebrando en ese momento. Se utilizará también para monitorizar en remoto lo que ocurre en las

ANEXO TÉCNICO

	Salas de oralidad desde un Centro de Control ● La preparación de Actos (pre-catalogación o catalogación) deberá poder realizarse tanto desde una aplicación de escritorio, como desde un entorno WEB. ● Deberá disponer para cada actuación de los siguientes datos ✓ Procedimiento al que pertenece y su tipo, además de un comentario asociado al mismo. ✓ Tipo de la actuación entre las permitidas para el tipo de procedimiento al que pertenece. ✓Intervinientes a participar en la actuación, indicando los roles que tomará cada uno, a seleccionar entre los permitidos para el tipo de actuación seleccionada. ✓Secretario al cargo de la actuación a seleccionar entre los dados de alta para el órgano. ✓Magistrado que oficia la actuación, a seleccionar entre los dados de alta para el órgano. ✓Fecha y hora prevista de comienzo de la actuación. ✓Comentario global a asociar a la actuación. ✓Emisión en vivo (Pública) o no (Secreta) de la actuación durante su captura. ✓ Autorización de preparación por parte del secretario judicial, necesario para que la actuación pueda grabarse. ● La Grabación deberá disponer de las siguientes funcionalidades: ✓Generación de actos sincronizados con el vídeo: - Intervenciones - Comentarios ✓Inserción de nuevos intervinientes ✓Emisión en vivo, siempre que el Magistrado dé su autorización ✓Control de entrada de vídeo. ✓Control de captura ✓Sobreimpresión del código de tiempo ✓Distorsión del audio ✓Mute Audio/Vídeo: Se permite eliminar la señal de audio o de

ANEXO TÉCNICO

	vídeo en la entrada. ✓Generar logs de acceso y alarmas ✓Permitir generar de manera automática un aplazamiento, es decir, una actuación con los mismos datos de catalogación que la finalizada, pero aplazada para otro día especificado mediante la selección del mismo en un calendario. ● Deberá disponer, tanto en aplicación de escritorio, como en entorno WEB, de dos tipos de consulta: ✓Básica: Permitirá consultar las actuaciones de un procedimiento determinado que fueron capturadas en un intervalo de tiempo determinado. ✓Avanzada: Permitirá seleccionar los parámetros con los que quiere buscar: - Número de procedimiento - interviniente que participó en la actuación - tipo del procedimiento al que pertenece - tipo de actuación - fecha de captura - estado de la actuación ● Una vez se ha seleccionado una actuación en el módulo de consulta (tanto en aplicación de escritorio, como en entorno WEB), y si el usuario dispone de permiso para ello, la aplicación deberá permitir lo siguiente: ✓Generación de copias en soporte óptico ✓Acceso al Acta de la actuación ✓Gestión de archivos adjuntos: Se debe permitir añadir y eliminar archivos adjuntos a la actuación seleccionada. ✓Firmar digitalmente los juicios ya realizados y pendientes de firma, al secretario judicial o fedatario público, tanto en el sistema instalado en la Sala, como desde cualquier punto de la intranet judicial. ✓ Comprobación de la integridad de las firmas realizadas con anterioridad. ● Y sólo para el caso de aplicación de escritorio (para evitar sobrecargar la red): ✓Edición de vídeo: deberá poderse seleccionar la porción del vídeo original que desea conservarse y eliminar el resto si se disponen de

ANEXO TÉCNICO

	los permisos adecuados. El nuevo vídeo pasará a ser el activo para la actuación y el anterior pasará a ser un archivo adjunto. Se realizarán de manera automática las modificaciones en los códigos de tiempo de las intervenciones y comentarios sincronizados para adecuarlos a la nueva duración del vídeo. ● La Gestión de Intervinientes deberá permitir especificar Relaciones de representación (ejemplo: que abogado representa a quien…), detectar la Duplicidad de Intervinientes si se diera el caso y la Búsqueda por interviniente. ● La Gestión de Usuarios tendrá que definir los Perfiles de Usuario, así como los Campos obligatorios para Usuarios y la Autenticación de los mismos. ● La solución deberá disponer de un Buzón de notificaciones de usuario en el que poder recibir mensajes del siguiente tipo: Anular reservas de salas, recibir Actos en grabación, Pausar grabaciones, recibir Mensajes desde la Sala de oralidad. ● En las Búsquedas y en la operación general, deberán poderse realizar: ✓Búsquedas de actuaciones, ✓Reproductor - información estado. ✓Selección de elementos ✓Añadir Adjuntos desde consulta Web ● Deberá tener agenda de señalamientos e insertar la fecha de fin de la grabación de la actuación correspondiente. ● La Gestión del Sistema tendrá que incorporar: ✓Administración Local de Salas, ✓Identificación de sala con su correspondiente sistema de sede o Central, ✓Administración de perfiles de usuarios y perfiles de órganos, ✓Administrar y Configurar la calidad de grabación, ✓Identificación de órgano, ✓Expendedor de copias de usuarios, ✓Permitir Backup/Restore, ✓En la monitorización de las salas permitir la Protección del Flujo de

ANEXO TÉCNICO

	Video, ✓Disponer de un Instalador ✓Periodos de actividad Estructura Procesal ● En los procesos de Firma y Autorización deberá disponer de: ✓Autenticación con tarjeta, ✓Autorización de reserva de sala, ✓Autorización de Pausa, ✓Autorización de Pausa/Reanudación, ✓Filtro buzón de firmas, ✓Mensajes de error de firma, ✓Flujos de Firma, ✓Firma de Máquina, ✓Identificación de quien firma y de quien anula, ✓Firma de Distribución por permisos/tipos, ✓Flujos de Firma, ✓Firma de distribución en consulta, ● Y en el visualizador que se entrega con la copia del juicio a las partes, se deberá Validar sólo firmas ingesta y de distribución, sólo los jueces pueden ver vídeos y documentos sin firma del secretario judicial. La comprobación de la integridad de las firmas digitales se puede realizar en local ● Deberá disponer el sistema de un MODO DE EMERGENCIA, el cual entrará en acción cuando algún elemento Hardware presente en la sala falle, y no se desactivará hasta que dicho fallo no sea subsanado ● El Secretario Judicial o equivalente puede visualizar en remoto, desde la web, el estado de la grabación (parado, grabando…) mientras se realiza el Streaming del Juicio que se está realizando en remoto. ● El Perfil Administrador de Usuarios no podrá crear otros perfiles Administrador de Usuarios ● El sistema borrará automáticamente cada cierto tiempo los ficheros que ya se han catalogado en otros servidores

ANEXO TÉCNICO

	● El sistema borrará bajo demanda y con el perfil de usuario adecuado que lo tenga permitido, la grabación de un juicio en los 3 niveles de su arquitectura ● La aplicación debe disponer de servicios web (publicados y documentados) que permitirán su integración con cualquier servicio de firma electrónica ● El sistema deberá disponer de la agenda judicial de cada Sala, desplegándose un calendario por cada sala, con la capacidad de reservarla. ● Dentro del calendario de una sala en concreto, se mostrarán en un color las audiencias que están señaladas, y en otro color la selección actual, en caso de estar previamente señalada. Se deberán poder escoger franjas horarias de un mínimo de quince minutos, dentro de los horarios definidos para la sala, y a partir del día actual, no en anteriores. ● La información que se mostrará de cada audiencia consistirá en las horas de inicio y fin en la parte superior y el número del procedimiento en la parte inferior de cada recuadro. Una vez una grabación ha sido señalada, un secretario podrá autorizar la misma a través de un proceso de firma digital. ● Deberá disponer también de un Módulo de Información al Público. Este módulo deberá permitir alimentar de manera automatizada los paneles de Información al público ubicados en los edificios judiciales, presentando en tiempo real la información de estado de cada acto judicial y otra información adicional. ● El Módulo de Información al Público debe utilizar también todo tipo de soportes audiovisuales que incorporen un navegador compatible HTML5 (tableta, PC), así como comunicar a los usuarios de la Justicia no sólo información sobre el estado de los juicios en la sala, sino horarios previstos, tipo de juicio, número del procedimiento… ● Deberá poder incorporar otro tipo de mensajes tales como vídeos y mensajes institucionales, información de actos, avisos de emergencia… ● El Módulo de Información al Público deberá permitir: ✓Generación de diferentes canales/layout para su emisión en diferentes zonas del edificio o áreas geográficas. ✓Múltiples diseños de plantillas de presentación, adaptables según

ANEXO TÉCNICO

	dispositivo de presentación seleccionado. ✓Video en tiempo real, web online, imágenes, texto, flash, formatos digitales de vídeo y cualquier otra fuente de información incrustable en contenidos HTML5. ✓Almacenamiento local de los contenidos multimedia presentados, minimizando el ancho de banda requerido para la visualización. ✓Gestión simultánea de múltiples layout para permitir la combinación de diferentes fuentes de información en pantallas de gran formato, proyectores o videowall. ✓La presentación agregada de grandes listados de actos, realizando de forma automática su distribución entre múltiples pantallas. ● El sistema deberá disponer también de Terminales Expendedores al Público, con las siguientes características: ✓Se instalarán en zonas comunes de la Sede Judicial ✓Permitirán a las partes obtener copias de las grabaciones a las que el juzgado autorice. ✓Liberará de trabajo al personal de la oficina judicial ✓Deberá tener un diseño ergonómico que garantice la accesibilidad a personas discapacitadas ✓Permitirá la generación de copias en varios soportes: cd, dvd y/o pendrive. El usuario del mismo lo controlará mediante pulsaciones en la pantalla táctil que debe poseer. ● Deberá disponer también de un SISTEMA DE ESTADÍSTICAS E INTELIGENCIA DE NEGOCIO que permita procesar y presentar de forma inmediata el estado de diversas variables y ratios que informen sobre los niveles de productividad de los órganos judiciales. Las vistas pueden ser de uno o múltiples órganos, dependiendo de los permisos del usuario. Podrán presentarse de forma individual o totalizada para todos los órganos o por jurisdicción (Penal, Civil, Laboral…), proporcionando una información invaluable a los responsables de la gestión judicial. ● La información podrá presentarse como evolución histórica y permitirá evaluar el comportamiento de cada órgano judicial en el tiempo, detectando y alertando de posibles problemas de rendimiento. ● La representación gráfica podrá seleccionarse a conveniencia del

ANEXO TÉCNICO

	usuario (tartas, líneas, barras, etc) ● La información histórica podrá presentarse también agrupada para los órganos judiciales de interés, así como la selección por jurisdicción (civil, penal,…) ● Además de las estadísticas de negocio, el módulo permitirá estadísticas sobre la infraestructura técnica (número de fallos, tasas de fallo), por sala o zona geográfica, ofreciendo a los responsables técnicos de la infraestructura una valiosa herramienta de análisis y predicción ● Deberá soportar en los sistemas de sala: ✓Windows 7/8/10 profesional 32 bits ✓Windows 7/8/10 profesional 64 bits ● Compatibilidad con: ✓MySQL Community Server 5.6.19 ✓MySQL Connector/ODBC 5.3.2 ● Soporte a las Máquinas virtuales JAVA ● Los servidores de aplicaciones podrán ser: ✓JBoss Application Server EAP 6.2.0 GA ● Los Videoserver soportados deberán ser: ✓Windows Server
Requerimiento de equipamiento de sala	● El equipamiento en la Sala deberá operar en forma autónoma aún en situaciones de conexión/desconexión de cualquier sistema central en la grabación. ● Equipamiento necesario para tener una capacidad mínima de 3000 hs. de almacenamiento local (independiente de otros Sistemas o componentes de la solución). ● Si fuera necesaria la adecuación de la infraestructura (iluminación, insonorización, etc.) de cada sala para la normal operación de sistema de videograbación, el oferente se compromete a indicar los cambios necesarios a realizar. ● La solución deberá proveer al menos 5 cámara y 7 micrófonos en cada Sala de oralidad, así como el servidor de Sala necesario para la

ANEXO TÉCNICO

	aplicación. ● La consola o sistema hardware de gestión del audio de sala supervisará el estado de la microfonía para garantizar el buen funcionamiento del mismo ● La consola de audio incluirá capacidad de análisis de presencia y nivel de señal para detección del uso del mismo, con detección de perdida de servicio y generación de alarmas por umbrales de voz, para evitar nulidades de las actuaciones judiciales o repetición de juicios. ● Deberá disponer de un control del nivel de audio por canal. Cuando se supera un umbral prefijado, se indique al sistema de grabación, proporcionando información de presencia de audio en cualquiera de los canales.
Integración Sistemas de Gestión Internos	● Deberá ser compatible con la solución CICERO Server de Sede ● Deberá permitir la integración del audio, el video y las anotaciones realizadas durante la actividad, a otros sistemas informáticos mediante Web Services. ● El Sistema de Grabación de Salas de Oralidad debe tener la capacidad de poder integrarse con el Sistema de Gestión, para lo cual es requisito que con Web Services provea los siguientes servicios mínimos: ✓Identificación univoca de actos y audiencias. ✓Preparación de Actos de forma automática ✓Modificación de actos ✓Elaboración y acceso a Actas ✓Acceso a Grabaciones
Capacitación	El oferente debe contemplar e incluir en su propuesta un plan de Capacitación a usuarios finales que se realizará al término implementación de la Sala, para al menos 10 personas en la ubicación de las. La capacitación deberá contemplar la correcta operación de la sala y el sistema de grabación, así como la detección y diagnósticos de fallas de todo el equipamiento ofertado e instalado.
Requisitos Equipamiento	● Todos los componentes deberán ser de marca reconocida internacionalmente. El equipamiento corresponderá a equipos diseñados para la Solución planteada no admitiéndose equipos

ANEXO TÉCNICO

	modificados o adaptados. ● Se deberá incluir el detalle de los equipamientos (incluyendo el número de parte identificador del producto por el fabricante) ofertados de forma de poder conocer las características técnicas del equipo a entregar. ● Los equipos deberán ser nuevos, Sin uso y en caja original. ● Se podrán ofertar propuestas de Soporte posteriores a la garantía para el mantenimiento de los equipos y asesoramiento del uso y funcionalidad que los mismos brindan.
Equipamiento por plataforma	Equipo Estación de Ingesta para grabación de audiencias con las siguientes especificaciones técnicas: ● Chassis: SFF Small Form Factor, Diseño tipo Tool less. 13th Generation Intel® Core™ i7-13700 16-Core, 24MB Cache, 2.9GHz to 4.8GHz, 65W. BIOS Instalado UEFI BIOS. De la misma marca del fabricante del equipo. Contiene las características principales del sistema del hardware. Pre-cargado el número de serie de la computadora. ● El equipo ofertado debe contar con un diagnóstico mejorado del sistema de pre-arranque, el cual debe permitir ejecutar pruebas de forma automática para reconocer errores de arranque de forma proactiva. ● Motherboard De la misma marca del fabricante del equipo con marca troquelada o grabada en la tarjeta, no deberá presentar alteraciones o correcciones de ingeniería. No se aceptan calcomanías o etiquetas, ni tarjetas con doble logotipo o marca. ● Memoria 16 GB (2 x 8 GB) de DDR4 UDIMM Non-ECC de 2666 MHz con crecimiento hasta 64 GB. Unidad de disco duro SATA de 3.5" 2 TB 7200 RPM; Unidad SSD de 512Gb;. Tarjeta de Video Intel HD Graphics. Tarjeta de Red integrada Ethernet LAN 10/100/1000. Unidad óptica DVD+/-RW. Audio Interno. ● Ranuras de Expansión 1 PCIe x16 Gen3 de altura media, 1 PCIe x4 Gen3 de altura media, 1 M.2 de 22 x 80 mm. - Puertos al menos - 1 puerto USB 3.2 Tipo C - 4 puertos USB 3.2 Tipo A - 2 puertos USB 2.0 Tipo A - 1 RJ45 Conector - 2 PS2 - 1 puerto serial - 2 Display Port 1.4

ANEXO TÉCNICO

	- 1 Universal Audio Jack - 1 Line out ● Fuente de alimentación PSU típica de 200W con 92% de eficiencia (80 PLUS Platinum); cumple con las normas ENERGY STAR. Teclado USB de 105 teclas en español alámbrico. ● Mouse óptico alámbrico, con un botón de clic izquierdo, un botón de clic derecho y una rueda de desplazamiento ● Características de seguridad El equipo ofertado debe proporcionar como mínimo los siguientes puntos en materia de seguridad ● Módulo compatible con TPM v2.0 ● Contraseña de usuario y administrador almacenada en BIOS con opción para requerir una contraseña robusta (Mínimo 8 caracteres, uno en mayúscula y uno en minúscula) ● Habilitación / Des-habilitación de puertos Paralelo, Serial y USB. ● Opción para deshabilitar el arranque (Boot) desde USB. ● Reporte de alertas al usuario y administrador. ● Número de serie grabado en “Setup” no modificable. ● Administración El fabricante del producto ofertado deberá ser miembro del "Distributed Management Task Force" (DMTF) y aparecer en el rubro Board Member, garantizando así que sus productos cuentan con los estándares para la gestión de sistemas en entornos organizacionales. ● Esta participación debe ser verificable a través de la página http://www.dmtf.org/about/list ● El equipo deberá contar con un agente (software) propietario de la marca residente en BIOS el cual debe ser capaz de detectar de forma proactiva el estado del hardware y software, alertar los incidentes en una consola centralizada y crear casos de soporte de manera automática para la resolución de estos ● Certificaciones y Cumplimiento a Regulaciones Configuraciones con calificación ENERGY STAR disponibles ● Configuraciones con registro de EPEAT disponibles ● Configuraciones con certificación TCO 8.0 disponibles CEL WEEE

ANEXO TÉCNICO

	Ley de Energía de Japón E-Standby de Corea del Sur Eco-label de Corea del Sur RoHS de la UE RoHS de China ● Sistema Operativo Windows 10 Pro, 64 bits, inglés, francés, español. ● 3 años de garantía PRO SUPPORT DELL. ● El equipo ofertado deberá cumplir con la completa compatibilidad con Sistemas Operativos Microsoft Windows, por lo cual se solicita que éste aparezca en el listado de productos certificados por el fabricante de Software. https://partner.microsoft.com/en-us/dashboard/hardware/search/cpl 3 años de garantía. ● Monitor de 23.8" Resolución máxima 1920 x 1080 a 60 Hz, Relación de contraste 1000:1, Proporción de Aspecto 16:9, Superficie de la pantalla antirreflejo, 250 cd/m2 de Brillo, 1 puerto DisplayPort versión 1.2, 1 puerto VGA. De la misma marca que el CPU". ● Unidad básica de mezcla y supervisión CICERO CAV UBS-110-8-MC, procesador de audio/video (NTSC) entradas de micrófono: 8, balanceadas, audio analógico XLR, interfaz USB audio multiplexado, detección de audio por canal, detector de presencia de vídeo, configuración y control vía USB. ● La solución completa (4 plataformas) para la microfonía, deberá contar con 28 Micrófonos de cuello de ganso tipo condensador, r de frecuencia 70-16khz, patrón cardioide, cuello de ganso 12", 2 secciones flexibles, XLR, totales incluyendo sus respectivas bases para micrófono. ● 5 Cámaras IP tipo BALA lente motorizado (zomm), infrarrojo 60m, 5mpx (2592x1944px) admite SD de 256G, tarjeta red 100Mbps. ●Unidad profesional de mezcla de sonido portátil con las siguientes características: 6 entradas mic/line como

ANEXO TÉCNICO

	mínimo, efectos internos, Faders, todas las entradas con control de nivel, Audio estéreo USB configurable entrada/salida, 1 pre-fade Aux send mínimo, 1 envío de efecto interno, salidas XLR main stereo con insertos, alimentación 48V para micrófono phantom, Jacks XLRs y de 1/4 pulgada. 2 años de garantía. ●1 Par de bocinas de altavoz compacto (plafón o pared) ●1 Pantalla Smart TV 50 pulgadas para transmisión de video en sala ●Amplificador de sonido medida de rack de 2 espacios (3.5”). 1000w RMS, 2 canales, potencia de 250 W @ 8 Ω, Respuesta en frecuencia de 10 Hz a 22 kHz en -0.1 dBu.,
Accesorios por plataforma	● Convertidor HDMI para distribución de señal de video en pantalla de sala ● Tarjeta capturadora audio/video ● Cámara de evidencias
Licencias por plataforma	● Licencia de Sala Software Cicero ● Licencia a Perpetuidad ● Ilimitados usuarios. ● Módulo VCF Cicero+ Para Videoconferencias ● Mantenimiento y actualización de versiones 3º año, software CICERO sala
Energía por plataforma	Respaldo de energía UPS 850VA/510W para PC de operador de sala. Lote de material de cable de audio, video, poder, extensores de señal incluye conectores.
Debe incluir por plataforma	Servicios profesionales que incluyen: conexión, instalación y configuración de sistema integral de grabación, pruebas de funcionamiento, puesta a punto de sistema de grabación y capacitación para el personal técnico, personal administrativo y/o usuarios, gastos de traslado y estancia de personal técnico.
	● El oferente se compromete a brindar un servicio de soporte en garantía a la finalización del proyecto por un plazo mínimo de 24

ANEXO TÉCNICO

Garantía y soporte por plataforma	meses, ● Dicho soporte podrá ser brindado en forma remota mediante teléfono, correo el electrónico u otros. El horario mínimo para recepción de reclamos será de 9 a 18 horas en días hábiles comprometiéndose a brindar respuestas en un plazo máximo de 24 horas a partir de la recepción de la consulta. ● La propuesta deberá incluir la actualización del Software en todos sus componentes durante el período de garantía sin costo adicional. ● Se podrán ofertar propuestas de soporte posteriores a la garantía para el mantenimiento de los equipos y asesoramiento del uso y funcionalidad que los mismos brindan. ● La solución ofrecida deberá contar con soporte oficial en el País. La responsabilidad por el soporte se extiende a la empresa diseñadora del producto y/o solución ofrecida