HOSPITAL NACIONAL EL SALVADOR

GOBIERNO DE EL SALVADOR | MINISTERIO DE SALUD

CONVOCATORIA

MINISTERIO DE SALUD
REPÚBLICA DE EL SALVADOR, CENTROAMÉRICA
HOSPITAL NACIONAL EL SALVADOR
AVISO DE CONVOCATORIA DE SOLICITUD DE EXPRESION DE INTERES
FUENTE DE FINANCIAMIENTO: FONDOS GENERALES -TELEMEDICINA

El Hospital Nacional El Salvador, de conformidad a lo previsto en el artículo 8 de la Ley General para la Modernización Digital del Estado y el romano VIII del Lineamiento para la Ejecución del Procedimiento Administrativo establecido en la LEY GENERAL PARA LA MODERNIZACION DIGITAL DEL ESTADO, convoca a personas naturales y jurídicas, nacionales y extranjeras a participar en el siguiente proceso de contratación, que tienen por objeto la contratación de los bienes relacionados siguientes:

REF.: LGMDE-HNES-UCP-2026-001
Contratación: "Suministro de equipamiento Tecnológico para la atención y operación de servicios de DOCTOR SV, Hospital Nacional El Salvador"

Objeto de la adquisición de los productos siguientes:

Bienes requeridos					
ÍTEM	CÓDIGO SINAB	CÓDIGO ONU	DESCRIPCIÓN DE BIENES Y SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD
1	60204205	43211503	COMPUTADORA PORTÁTIL DE PRESTACIONES MEDIAS CON SISTEMA OPERATIVO Y OFIMÁTICA PRIVATIVOS	C/U	500
2	60201332	43211902	MONITOR LCD DE 27"	C/U	250
3	80303040	43233205	LICENCIA CLIENTE DE ANTIVIRUS	C/U	800
4	81209060	81112204	SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO DE SOFTWARE	C/U	1

Condiciones Generales y Particulares de la Solicitud de Expresión de Interés:
Descargar documento en el enlace siguiente https://hes.gob.sv/servicios/documentos-procesos-de-compra/
Para expresar interés en participar:
Enviar su propuesta a los correos electrónico: karen.valles@salud.gob.sv, indicando en el asunto el nombre de la contratación y el proyecto.
El periodo para enviar expresiones de interés cerrará a las 15:00 horas del día 22 de enero de 2026 Zona horaria de El Salvador (GMT-6). Las propuestas deberán incluir el formulario de identificación de proveedor (Anexo 2).

Nota: no se recibirán expresión de interés después de la hora señalada.

Distrito de San Salvador y Capital de la República, San Salvador Centro, Departamento de San Salvador
22 de enero de 2026

ANEXO 1

SOLICITUD DE EXPRESIÓN DE INTERES REF.: LGMDE-HNES-UCP-2026-001

Contratación: "Suministro de equipamiento Tecnológico para la atención y operación de servicios de DOCTOR SV, Hospital Nacional El Salvador"

Fuente De Financiamiento: FONDOS GENERALES -TELEMEDICINA

El Hospital Nacional El Salvador (HNES) invita a personas naturales y jurídicas, nacionales o extranjeras a participar en el proceso de Solicitud de Expresión de Interés (SEI) que se regirá bajo las condiciones siguientes:

I. CONDICIONES GENERALES DEL PROCESO ADMINISTRATIVO DE CONTRATACIÓN.

A. NATURALEZA Y NORMATIVA APLICABLE.

La presente SEI se regirá de conformidad a lo previsto en la Ley General para la Modernización Digital del Estado y el Lineamiento para la Ejecución del Procedimiento Administrativo establecido en la Ley General para la Modernización Digital del Estado.

La presente SEI consistirá en una convocatoria pública a proveedores nacionales y extranjeros, domiciliados o no, para que presenten su manifestación de interés a través de una propuesta técnica y económica, que será evaluada bajo criterios de selección claros y precisos, basados en la metodología de análisis de calidad-costo. En ese sentido, el presente procedimiento no requiere la presentación de documentación legales ni financieros.

La normativa aplicable podrá ser consultada en la siguiente dirección web: https://portal.modernizacion.gob.sv/#/home.

B. FASES DEL PROCESO ADMINISTRATIVO

En cumplimiento a lo establecido en el numeral 4 "Procedimiento en caso de financiamiento por donación o contratos de préstamos, para la adquisición a través de Licitación Pública Internacional", del romano VIII "Procedimiento Administrativo" del Lineamiento para la Ejecución del Procedimiento Administrativo establecido en la Ley General para la Modernización Digital del Estado, esta Solicitud de Expresión de Interés se realizará la manera siguiente:

1. Publicación del Solicitud de Expresión de Interés: la convocatoria se realizará en medios de comunicación nacionales e internacionales, de manera enunciativa y no limitativa, por medio de prensa escrita y los canales de sus redes sociales oficiales. El documento podrá ser descargado desde la página web oficial del HNES o ingresando al enlace siguiente https://hes.gob.sv/servicios/documentos-procesos-de-compra/, a partir del mismo día de la publicación de su convocatoria.

2. Período de consultas, respuestas y adendas: para consultas deberá remitirlas por escrito, en físico en las instalaciones de la Unidad de Informática y Telecomunicaciones del Hospital Nacional El Salvador, ubicadas en Avenida De La Revolución #222, San Salvador Centro, San Salvador, El Salvador, C.A. o por correo electrónico a la dirección karen.valles@salud.gob.sv, a más tardar las diez (15:00) horas, Zona horaria de El Salvador (GMT-6), del día 22 de enero del corriente año. El HNES podrá responder las consultas y realizar adendas al presente documento hasta antes de la hora y fecha establecida para la recepción de propuestas.

3. Recepción de propuestas: será hasta las 15:00 horas, zona horaria de El Salvador (GMT-6), del día **22 de enero** del corriente año.

4. Evaluación de propuestas: el HNES evaluará las propuestas en un período máximo de cinco (5) días hábiles a partir del siguiente a la fecha de recepción.

5. Plazo de inconformidades: En caso de recibir más de una expresión de interés, los proponentes podrán presentar su escrito de inconformidad dentro de dos (2) días hábiles contados a partir del siguiente a la notificación de los resultados.

6. Notificaciones: el HNES notificará a los proponentes el resultado de la evaluación, la admisión y resolución de escrito de inconformidad, cuando aplique, desde la emisión del respectivo acto, hasta en un plazo máximo de dos (2) días hábiles posteriores.

C. SUPLETORIEDAD.

Cualquier aspecto de índole legal, jurisdiccional, administrativo o técnico que no se encuentre regulado en el presente documento será convenido en el respectivo contrato o adendas al contrato, cuando sea procedente.

D. RESULTADO DE LA EVALUACIÓN.

Una vez evaluadas las propuestas derivadas de la presente Solicitud de Expresión de Interés y habiendo sido finalizado y aprobado el informe respectivo sin que se hubiese recibido escrito de inconformidad o que este haya sido resuelto, el HNES podrá iniciar un procedimiento de contratación bajo la Ley de Compras Públicas y/o Ley de Bolsas de Productos y Servicios, pudiendo generar las invitaciones y/o incluir los proveedores que cumplieron los requisitos técnicos en las listas cortas, según aplique.

En caso de que, la propuesta más favorable provenga de alguno de los sujetos intervinientes en el Convenio de Alianza Estratégica para la Modernización Digital del Estado o que esta sea la única propuesta y haya cumplido con los criterios de evaluación establecidos, el HNES podrá emitir orden de pedido, de conformidad a los establecido en la ley.

El resultado de la evaluación que hace referencia este apartado será notificado a todos los proponentes.

II. CONDICIONES PARTICULARES DEL PROCESO ADMINISTRATIVO DE CONTRATACIÓN.

A. ESPECIFICACIONES TECNICAS DEL SERVICIO

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad	Plazo de entrega requerido
1	60204205	43211503	COMPUTADORA PORTÁTIL DE PRESTACIONES MEDIAS CON SISTEMA OPERATIVO Y OFIMÁTICA PRIVATIVOS	500	15 días calendario.
2	60201332	43211902	MONITOR LCD DE 27"	250	15 días calendario.
3	80303040	43233205	LICENCIA CLIENTE DE ANTIVIRUS	800	15 días calendario
4	81209060	81112204	SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO DE SOFTWARE	1	5 días hábiles

El Suministro de equipamiento tecnológico institucional, destinado a fortalecer la capacidad operativa del Hospital Nacional El Salvador para la atención y operación de los servicios de telemedicina, conforme a las cantidades y condiciones establecidas en los Términos de Referencia.

Licenciamiento e implementación de una solución integral de seguridad informática para endpoints, que incluya protección avanzada contra amenazas, capacidades de detección y respuesta (EDR), consola centralizada de administración y servicios en la nube asociados, en cumplimiento de los requerimientos técnicos definidos en los Términos de Referencia.

Prestación de servicios asociados a la solución de seguridad endpoint, tales como administración centralizada, control de dispositivos, protección web y de correo, mecanismos de respuesta ante incidentes y funcionalidades de cifrado de datos, orientados a salvaguardar la información institucional y clínica.

servicio de soporte técnico y mantenimiento de software, con el propósito de asegurar su continuidad operativa, atención oportuna de incidencias y cumplimiento de los niveles de servicio establecidos, el servicio requerido comprende diagnóstico, configuración, atención de incidencias, ajustes permitidos y mantenimiento lógico del software biométrico, así como la gestión de licencias, control de fechas de vencimiento y coordinación de renovaciones, sin incluir reposición de hardware, partes, accesorios ni la adquisición de nuevos equipos. La necesidad de contar con mantenimientos preventivos lógicos periódicos, atención de fallas de software y firmware bajo demanda, y servicios de soporte remoto y presencial cuando aplique, con tiempos de respuesta y resolución definidos, a fin de minimizar indisponibilidades y asegurar la operatividad de los dispositivos.

El suministro requerido consiste en:

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad
1	60204205	43211503	COMPUTADORA PORTÁTIL DE PRESTACIONES MEDIAS CON SISTEMA OPERATIVO Y OFIMÁTICA PRIVATIVOS	500

Especificaciones Técnicas	COMPUTADORA PORTÁTIL PARA REQUERIMIENTOS ESPECIALES CON SISTEMA OPERATIVO WINDOWS Especificaciones mínimas: • Procesadores admitidos: Intel Core Ultra 5 (Series 2), 225U. • Cache 12MB mínimo, 10 núcleos mínimo, (hasta 4.60 GHz) • Memoria RAM: 16GB DDR5-SDRAM 1 x 16GB como mínimo. • Disco duro: 512 GB M.2 NVMe PCIe SSD mínimo. • Pantalla: 39,6 cm (15,6"), sin función táctil, FHD, 60 Hz, antirreflectante, 1920 x 1200 píxeles, mínimo • Tarjeta de Video: Tarjeta gráfica Intel® Graphics • Sistema operativo: Windows 11 Pro 64-bit español • Sistema de audio, altavoces de calidad, micrófono, conector de audio universal. • Cámara 720p HD como mínimo • Tarjeta inalámbrica Intel Wi-Fi 6E AX211, 2x2, 802.11ax • Bluetooth • Teclado en español. • Batería de 3 celdas y 45 Wh (integrada) • 1 USB 3.2 Gen 1 (3.1 Gen 1) Type-A ports, mínimo • 1 USB 3.2 Gen 2 (3.1 Gen 2) Type-C ports, mínimo • 1 USB Type-C DisplayPort Alternate Mode PowerShare • 1 puerto video HDMI 1.4, mínimo • 1 puerto de audio universal • Fuente de alimentación: Adaptador robusto de CA de 65 W Auriculares de 2 oídos con cable USB 2.0 o superior y Jack 3.5mm, Estéreo con aislamiento y voz nítida con micrófono antirruido, Protección de picos acústicos, Diadema ligera durabilidad, ajuste personalizado, Control de llamadas desde cable con botones de volumen, tecla mute, Compatible con Softphones y aplicaciones de videoconferencias. Certificaciones con Sellos de regulación: CE, FCC, KCC, RCM, UL, Certificaciones industriales: Microsoft Teams, Zoom, Avaya, Cisco, Alcatel Lucent y Astra Con mouse Inalámbrico óptico bluetooth con Scroll, de la misma marca del equipo Características Eléctricas: • Voltaje: 100-240 VAC • Frecuencia: 50/60 Hertz • Fuente de poder, Adaptador externo 65W • Cable de alimentación con toma corriente macho polarizado.

Lugar de entrega	Almacén del Hospital Nacional El Salvador, ubicado en Avenida De La Revolución #222, distrito de San Salvador, municipio de San Salvador Centro, departamento de San Salvador.
Plazo de entrega	Máximo 15 días calendario
Garantía	Garantía mínima de un (1) año contra desperfectos de fabricación La garantía de los equipos debe ser respaldada con el fabricante, incluida sus partes para un (1) año, servicio en sitio.

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad
2	60201332	43211902	MONITOR LCD DE 27"	250

Especificaciones Técnicas	● Monitor estilo Curvo ● Tamaño de pantalla: 27" ● Tipo de panel: VA ● Resolución: FHD (1,920x 1,080) ● Relación de aspecto: 16:9 ● Curvatura de pantalla: 1800 ● Brillo (Típico): 250cd/㎡, Brillo (Mínimo): 200 cd/㎡ ● Proporción de Contraste Estático: 3,000:1(Typ.) ● Tiempo de Respuesta: 4(GTG) ● Tasa de Refresco: Max 100Hz ● Ángulo de Visión (HN): 178º(H)/178º(V) ● Tamaño del Monitor Activo (HorizontalxVertical)(mm): 596.736x335.664mm ● Soporte de Color: Max 16.?M ● Cobertura sRGB: 95% ● 1 interfaz HDMI, 1 interfaz VGA ● Fuente de alimentación: AC 100-240V ● Se debe incluir cable de alimentación y cable HDMI
Lugar de entrega	Almacén del Hospital Nacional El Salvador, ubicado en Avenida De La Revolución #222, distrito de San Salvador, municipio de San Salvador Centro, departamento de San Salvador
Plazo de entrega	Máximo 15 días calendario.
Garantía	● Garantía mínima de un (1) año contra desperfectos de fabricación ● La garantía de los equipos debe ser respaldada con el fabricante, incluida sus partes para un (1) año, servicio en sitio. ● El fabricante debe contar con un centro de atención de llamadas de reparación o asistencia técnica.

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad
3	80303040	43233205	LICENCIA CLIENTE DE ANTIVIRUS	800

Información General	1.1 El fabricante de las soluciones ofertadas debe contar con, al menos, 25 años de presencia en el mercado global. 1.2 El proveedor de la solución ofertadas debe contar con un equipo de investigación y soporte de por lo menos cinco (5) analistas de investigación de amenazas basados en el país de origen del proveedor. 1.3 El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APT's y malware avanzado y debe haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) durante el 2023.

Características Generales	Se debe proveer una solución tecnológica que incluya una poderosa protección de endpoints basada en IA, controles de seguridad flexibles y características de EDR incorporadas.
	La solución debe contar con una consola fácil de usar, opciones de implementación en la nube y on-premises, así como también una variedad de funciones que simplifiquen la vida del usuario, reduciendo la complejidad y aumentando la eficiencia.
	La solución debe proteger endpoints y servers, sean estos Windows, Linux, macOS, así como también dispositivos móviles iOS y Android.
	La solución debe disponer de una única licencia que debe permitir el uso de la consola nube u on-premise, como así también de todos los endpoints y servers que disponga la organización, independientemente del sistema operativo del dispositivo en cuestión.
	La solución debe permitir la implementación de puntos de distribución en diferentes segmentos de red o ubicaciones geográficas de la organización que permita la distribución de actualizaciones, sondeo de red, instalación remota de aplicaciones, obtención de información sobre equipos de un grupo de administración, y/o difusión de dominio, entre otras.
	La solución debe incluir una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos del fabricante, ofreciendo un recurso en línea que permita conocer la reputación de los archivos, los recursos web y el software, garantizando respuestas más rápidas ante nuevas amenazas, mejorando el rendimiento de algunos componentes de protección y reduciendo el riesgo probable de que se produzcan falsos positivos.
	La solución debe contar con la capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en los endpoints y servidores, sin la necesidad de la contraseña de remoción del actual antivirus.
	La solución debe disponer de la capacidad de instalar remotamente la solución de antivirus en los endpoints y servidores Windows, a través de la administración

Protección para Endpoints, Consola de Administración y Reporteo	compartida, login script y/o GPO de Active Directory.
	La solución debe contar con la capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto.
	La solución debe disponer de la capacidad de importar la estructura de Active Directory para encontrar máquinas.
	La solución debe contar con la capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección.
	La solución debe disponer de la capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente.
	La solución debe combinar protección basada en firmas, análisis heurístico y de comportamiento, junto con tecnologías asistidas por la nube para proteger los endpoints contra amenazas de malware conocidas, desconocidas y avanzadas.
	La solución debe permitir habilitar la protección con contraseña con el fin de restringir el acceso de los usuarios a la solución en la estación de trabajo según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).
	La solución debe proporcionar mecanismos de autoprotección con el fin de evitar que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de la solución propuesta.
	La solución debe permitir realizar un análisis personalizado para cualquiera de los siguientes objetos: Memoria del sistema, Objetos cargados en el inicio del sistema operativo, Copia de seguridad del sistema operativo, Buzón de correo de Microsoft Outlook, Unidades de disco duro, Unidades extraíbles y unidades de red o Cualquier archivo seleccionado.
	La solución debe permitir realizar un análisis en segundo plano de manera que la aplicación no le muestre ninguna notificación al usuario y que tenga menos impacto en los recursos del equipo, para cualquiera de los siguientes objetos: objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema.
	La solución debe permitir establecer una programación para el análisis, de manera que se pueda realizar de forma manual o según programación.
	La solución debe permitir analizar archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos.
	La solución debe permitir analizar archivos protegidos con contraseña.
	La solución debe incorporar un componente de protección frente a amenazas web que permita evitar la descarga de archivos maliciosos de Internet y también bloquee sitios web maliciosos y de phishing.
	La solución debe analizar tráfico HTTP, HTTPS y FTP.
	La solución debe bloquear el tráfico HTTP que no cumple con los estándares RFC.

	La solución debe incluir un componente de protección frente a amenazas en el correo que permita analizar los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas.
	La solución de protección frente a amenazas en el correo debe ser compatible con POP3, SMTP, IMAP y NNTP.
	La solución de protección frente a amenazas en el correo debe intentar desinfectar un objeto infectado en un mensaje entrante o saliente. Si el objeto no se puede desinfectar, el componente de protección en el correo deberá eliminar el objeto infectado y añadir información sobre la acción realizada al asunto del mensaje, por ejemplo: [Se ha procesado el mensaje] <asunto del mensaje>.
	La solución debe incluir un componente de protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red.
	La solución debe bloquear la conexión de red con el equipo atacante.
	La solución debe incluir una base de datos que ofrezca descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos.
	La solución debe bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado de al menos una hora.
	La solución debe permitir seleccionar el protocolo y el puerto que se van a usar para la comunicación y permitir actividades de red específicas.
	La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques a la red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC.
	La solución debe incluir un componente de Firewall de escritorio que bloquee las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local.
	El componente de firewall de escritorio debe proporcionar protección del equipo con la ayuda de bases de datos antivirus, el servicio de inteligencia global en la nube y reglas de red predefinidas.
	El componente de firewall de escritorio debe incluir un componente prevención de intrusiones en el host que proporcione acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de derechos de aplicación.
	El componente de firewall de escritorio debe controlar la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE.
	El componente de prevención de ataques a nivel de USB debe permitir que los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente se consideren autorizados después de la instalación del componente.
	El componente de prevención de ataques a nivel de USB debe bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado.
	El componente de prevención de ataques a nivel de USB debe permitir utilizar un teclado en pantalla para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (p.ej., escáneres de códigos de barras).

	La solución debe incluir un componente de protección AMSI diseñado para ser compatible con Antimalware Scan Interface de Microsoft.
	La solución debe incluir un componente de prevención de exploits que permita detectar código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración.
	El componente de prevención de exploits debe incluir un mecanismo de protección de la memoria de procesos del sistema, de manera que la solución bloquee los procesos externos que intentan acceder a los procesos del sistema.
	La solución debe incluir un componente de prevención de intrusiones en el host que evite que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo.
	El componente de prevención de intrusiones en el host debe activar la protección del acceso a audio y vídeo, de manera que se evite que los ciberdelincuentes puedan usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web), controlando cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada.
	La solución debe incluir un componente de motor de reparación que le permita revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo.
	El componente de motor de reparación debe permitir anular la actividad de malware en el sistema operativo a los siguientes tipos de actividad de malware: - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red) - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado - Restaura los archivos que el malware ha modificado o eliminado - Elimina las claves del registro que el malware ha creado - No restaura las claves del registro que el malware ha modificado o eliminado - Finaliza los procesos iniciados por el malware - Finaliza los procesos en los que haya penetrado una aplicación maliciosa - No reanuda procesos que el malware haya suspendido - Bloquea la actividad de red del malware - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado
	El componente de control web debe permitir supervisar tráfico HTTP y HTTPS.
	El componente de control web debe permitir configurar el acceso a los sitios web a través de estos criterios: - Categorías de sitios web - Tipo de datos - Direcciones individuales

	El componente de control web debe utilizar al menos los siguientes filtros: - Filtrar por contenido y tipo de datos - Filtrar por direcciones de recursos web - Filtrar por nombres de usuarios y grupos de usuarios
	El componente de control web debe permitir seleccionar alguna de las siguientes acciones: - Permitir - Bloquear - Advertir
	La solución debe incluir un componente de control de dispositivos que administre el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi), con el fin de proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos.
	El componente de control de dispositivos debe permitir la creación de reglas de acceso que permitan ajustar la configuración que determina qué usuarios pueden usar dispositivos instalados en un equipo o conectados a él.
	El componente de control de dispositivos debe permitir crear reglas del acceso para los siguientes tipos de dispositivo, mínimamente: - Discos duros - Unidades extraíbles (incluidas las unidades flash USB) - Disquetes - Unidades de CD/DVD - Dispositivos portátiles (MTP) - Impresoras locales - Impresoras de red - Módems - Unidades de cinta - Dispositivos multifuncionales - Lectores de tarjetas inteligentes - Dispositivos Windows CE USB ActiveSync - Adaptadores de red externos - Bluetooth - Cámaras y escáneres
	El componente de control de dispositivos debe proporcionar funciones de Anti-Bridging con el fin de impedir establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red.
	La solución debe incluir un componente de control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios.

	El componente de control de aplicaciones debe poder funcionar en dos modos: - Lista de rechazados. En este modo, el control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de control de aplicaciones. - Lista de permitidos: en este modo, el control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de control de aplicaciones.
	El componente de control de aplicaciones debe crear una imagen propietaria de los programas que garantizan el funcionamiento normal del sistema operativo.
	El componente de control de aplicaciones debe realizar un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR, cuando se añade contenido manualmente.
	La solución debe permitir agregar un Widget de alertas de EDR que muestre información sobre la cantidad de alertas en los dispositivos durante el último mes.
	La solución debe incluir una API abierta (OpenAPI) que permita personalizar escenarios operativos y tareas a través de la consola de gestión central.
	La solución debe incluir, dentro de su licenciamiento, la conexión a una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos en línea del fabricante, que permita conocer la reputación de los archivos, los recursos web y aplicaciones, de manera que la solución de una respuesta más rápida a las amenazas, mejore el rendimiento de los componentes de protección y reduzca la probabilidad de falsas alarmas.
	La solución debe contar, dentro de su licenciamiento, con integración y acceso con un Portal de Inteligencia contra Amenazas, que permita consultar información sobre la reputación de archivos y URL's.
	La solución debe proveer información sobre el dispositivo protegido en el que se produce la alerta (por ejemplo, nombre del dispositivo, dirección IP, dirección MAC, lista de usuarios, sistema operativo, entre otros).
	La solución debe proveer información relacionada con los cambios en el registro asociados con la alerta.
	La solución debe permitir establecer exclusiones de aislamiento de red. Es decir que las conexiones de red que cumplan las condiciones de la exclusión especificada no se bloquearán en los dispositivos después de que se active el aislamiento de red.
	La solución debe incluir, dentro de su licenciamiento, un SandBox basado en Nube que permita detectar amenazas complejas en los equipos de los usuarios.
	La solución debe permitir enviar automáticamente al Sandbox basado en Nube los archivos que es necesario analizar.
	La solución debe permitir ver los informes de alertas detectadas por la tecnología de Sandbox basado en Nube.
	La solución debe permitir crear tareas de Análisis de IoC con el fin de encontrar indicadores de compromiso en el dispositivo y realizar acciones de respuesta a la

	amenaza.
	La solución debe permitir ejecutar una de las siguientes acciones de respuesta disponibles para los IoC detectados: - Aislar el dispositivo de la red - Ejecutar análisis de áreas críticas - Poner la copia en cuarentena y eliminar el objeto
	El componente de cifrado de datos debe utilizar el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard") con sus variantes de cifrado "fuerte" (AES256) como la de cifrado "ligero" (AES56). 3.85 El componente de cifrado de datos debe ofrecer las siguientes características de protección de datos: - Cifrado de archivos en unidades locales del equipo - Cifrado de unidades extraíbles - Gestión de reglas de acceso de las aplicaciones a los archivos cifrados - Creación de paquetes cifrados - Cifrado de disco completo
	El componente de cifrado de datos debe ser compatible con los sistemas de archivos FAT32, NTFS y exFAT.
	El componente de cifrado de datos debe permitir gestionar el cifrado de Microsoft BitLocker desde la consola central.
	El componente de cifrado de datos debe incluir los siguientes estados de cifrado: - No cumple la directiva; cancelado por el usuario. El usuario ha cancelado el cifrado de datos. - No cumple la directiva debido a un error. Error de cifrado de datos; por ejemplo, falta una licencia. - Aplicando la directiva. Reinicio necesario. Cifrado de datos en curso en el equipo. Reinicie el equipo para completar el cifrado de datos. - No se ha especificado ninguna directiva de cifrado. El cifrado de datos está desactivado en la configuración de directiva. - No compatible. Los componentes de cifrado de datos no están instalados en el equipo. - Aplicando la directiva. El cifrado y el descifrado de datos está en curso en el equipo.
Plataforma de Entrenamiento	La solución propuesta debe incluir formación en ciberseguridad dentro de la aplicación.
	La solución propuesta debe dividir el entrenamiento en varios módulos, donde cada uno de los módulos debe estar en una serie de secciones.
	Los módulos propuestos deben incluir teoría relevante y capacidad de realizar tareas interactivas en un entorno simulado.
	La solución propuesta debe permitir descargar un certificado que acredite los logros una vez completadas todas las secciones de un módulo.

	La solución propuesta debe ser 100% en nube.
	Los módulos propuestos deben ser de entrenamientos en ciberseguridad agnósticos entre los que se encuentren Respuestas a Incidentes, Software Malicioso, Aseguramiento de Directorio Activo y Seguridad para servidores, entre otros.
Condiciones Generales	El proveedor dede de contar con un SOC local, el cual debera de contar con analistas locales, debera de presentar planilla de ISSS.
	El proveedor debe de ser partnert de la marca ofertada, debera de presentar carta de fabricante
	El proveedor debera de cumplir con las siguientes certificaciones que avalan su experiencia en analisis de eventos de ciberseguridad: EC-COUNCIL CERTIFIED INCIDENT HANDLER EC-COUNCIL CERTIFIED SOC ANALYST
Lugar de entrega	Almacén del Hospital Nacional El Salvador, ubicado en Avenida de la Revolución #222, municipio y departamento de San Salvador.
Plazo de entrega	Máximo 15 días calendario
Vigencia	Licenciamiento durante 1 año

ítem	**Código SINAB**	**Código ONU**	**Denominación del bien o servicio**	**Cantidad**
4	81209060	81112204	SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO DE SOFTWARE	1

Especificaciones Técnicas	● Contrato de soporte de equipos biométricos ● Soporte de software, licenciamiento y mantenimiento de equipos biométricos existentes ● Cantidad: 7 dispositivos · Año: 2021, Marca: HFSECURITY · Modelo: FR05M ● Diagnóstico, configuración, atención de incidencias, ajustes permitidos y reportes del software biométrico ● Gestión de licencias, control de fechas de vencimiento y coordinación de renovaciones ● Dos (2) mantenimientos preventivos lógicos por año ● Atención de fallas de software y firmware bajo demanda ● Soporte remoto y presencial cuando aplique ● Tiempo de respuesta ≤ 4 horas · Tiempo de resolución ≤ 24 horas ● Tiempo de respuesta ≤ 8 horas · Tiempo de resolución ≤ 48 horas ● Tiempo de respuesta ≤ 24 horas · Tiempo de resolución ≤ 72 horas ● Tiempo de respuesta ≤ 48 horas · Tiempo de resolución ≤ 5 días hábiles ● Reportes de incidencias, informes mensuales, reportes de mantenimiento y actas de conformidad ● Duración Doce (12) meses

	● No incluir reposición de hardware, partes, accesorios ni adquisición de nuevos equipos
Lugar de entrega	Almacén del Hospital Nacional El Salvador, ubicado en Avenida De La Revolución #222, distrito de San Salvador, municipio de San Salvador Centro, departamento de San Salvador
Plazo de entrega	5 días después de recibida Orden de Compra
Garantía	● Garantía mínima de un (1) año contra desperfectos de fabricación

1. CONDICIONES ESPECIALES

Se evaluará la capacidad técnica del oferente para suministrar los bienes y prestar los servicios requeridos, considerando:

- la oferta debe cumplir íntegramente con las especificaciones técnicas mínimas establecidas en los Términos de Referencia para cada uno de los ítems solicitados

- Experiencia comprobada en la provisión de equipamiento tecnológico informático empresarial: anexar al menos dos cartas de referencia, deberán tener tipo de bien suministrado o servicio contratado, clasificación de la atención brindada por el personal del contratista, con referencia del último año.

- Experiencia en la prestación de servicios de soporte técnico y mantenimiento de software, conforme al alcance definido en el TDR: El proveedor debe de presentar una tabla de escalonamiento que refleje correos, números de teléfono en caso de ser necesario reportar una escalación en caso de requerir un soporte.

- Los plazos establecidos en los presentes Términos de Referencia son de carácter obligatorio; en consecuencia, el proveedor deberá considerar que no procederá consulta, solicitud ni apelación relacionada con la ampliación de los tiempos definidos o prorroga de entrega injustificada de los mismo, debiendo cumplir estrictamente con los plazos establecidos.

- Se requiere qué los bienes cuenten con garantía mínima conforme a lo establecido en los Términos de Referencia.

- De la oferta se requiere qué Incluya todos los costos asociados al suministro de bienes, licenciamiento y prestación de servicios requeridos.

B. CRITERIOS DE EVALUACIÓN Y SELECCIÓN

CRITERIOS DE EVALUACIÓN:

De conformidad a lo establecido en el numeral 7 “Regla Especial para la evaluación de propuestas provenientes del Procedimiento de Licitación Pública Internacional” del romano VIII “Procedimiento Administrativo” del "Lineamiento para la Ejecución del Procedimiento Administrativo establecido en la Ley General para la Modernización Digital del Estado”, la evaluación consistirá en la velicación del cumplimiento de las características técnicas del servicio, y valoración calidad-precio:

PRIMERA ETAPA. Velicación del cumplimiento de las características técnicas del servicio.

El oferente deberá demostrar el cumplimiento de las especificaciones técnicas requeridas:

criterios de evaluación	**CUMPLE/PUNTOS**	**NO CUMPLE/PUNTOS**
a) Especificaciones Técnicas	70	0
b) Tiempos de entrega	15	0
c) Condiciones especiales	15	0
Porcentaje Total……	**100%**	**0**

Puntaje mínimo de aprobación de primera etapa: 100 PUNTOS

*El oferente podrá cumplir este criterio con documentación propia, de su sociedad matriz y/o afiliadas.

SEGUNDA ETAPA. Relación calidad-precio.
Consiste en la verificación de la oferta más ventajosa por medio de la ponderación de la calidad y del precio. Para esta verificación el puntaje obtenido en la segunda etapa será ponderada con base al ochenta por ciento (80%), mientras que, la propuesta económica será ponderará con base al veinte por ciento (20%). Para obtener la ponderación de la calidad se dividirá el puntaje obtenido entre 80 y se multiplicará por 100. La ponderación de la propuesta económica se realizará colocando a la propuesta de menor valor el veinte por ciento (20%), a la siguiente propuesta de menor precio se le otorgará un puntaje de quince por ciento (15%), a la siguiente de diez por ciento (10%), todas las demás ofertas serán puntuadas con 5 por ciento (5%).

CRITERIO	**PUNTUACION MÁXIMA**
CALIDAD	80 puntos
PRECIO	20 puntos

Durante la evaluación, el Hospital Nacional El Salvador podrá realizar comunicaciones con los oferentes con el estricto objetivo de obtener y/o comprender los elementos necesarios para concluir la evaluación, realizando prevenciones y aceptando subsanaciones, dejando constancia de dicha comunicación en el expediente de la contratación con base a los principios de igualdad y transparencia. No podrá aceptarse subsanación que modifique la oferta económica ni podrá prevenirse en más de una ocasión un mismo asunto. El plazo de subsanación será establecido por el HNES en la comunicación correspondiente.

Una vez finalizada la evaluación se emitirá el informe correspondiente, el cual determinará cuál es la propuesta más favorable y se procederá de conformidad a lo establecido en el literal E. "Resultado de la Evaluación" del romano I "CONDICIONES GENERALES DEL PROCESO ADMINISTRATIVO DE CONTRATACIÓN", de la presente Solicitud de Expresión de Interés.

A. EXCLUSION DE PROPUESTAS.

No se evaluarán propuestas de oferentes que se encuentran en el Registro de Sanciones de COMPRASAL y en las listas de sancionados con inhabilitación para contratar emitidas por el Banco Mundial y Banco Interamericano de Desarrollo.

B. IMPUGNACIONES.

Los proponentes dispondrán de dos (2) días para interponer "Escrito de Inconformidad" en el cual deberán exponer de manera clara los argumentos de su disensión, de conformidad a los criterios evaluados y a su propuesta presentada. En caso de recibir solo una propuesta, no será necesario esperar el transcurso del plazo en cuestión y podrá continuarse con las siguientes etapas del proceso, según corresponda.

Recibido el escrito, el HNES convocará los evaluadores que conocieron las propuestas, quienes evaluarán el escrito y sus elementos y decidirán si se mantiene la elección de la Oferta más favorable o se modifica. Esta decisión pasará a aprobación de la máxima Autoridad de la institución o su delegado y posteriormente deberá ser notificada a los interesados. El procedimiento anterior se realizará en un plazo no mayor a diez (10) días hábiles a partir de la recepción del escrito de inconformidad.

C. CONFIDENCIALIDAD:

Toda información relacionada con el servicio será considerada como confidencial, salvo en los casos en que dicha información haya sido publicada por el Contratante o cualquier otra institución pública, u obre en registros públicos. En ningún caso podrá divulgarse y deberá protegerse toda información confidencial y en particular los datos personales, por lo que el ingreso, tratamiento y resguardo de dicha información deberá atender a lo dispuesto en la legislación correspondiente.

A efecto de dar cumplimiento a lo anterior, el Contratista deberá implementar:

- Medidas, políticas y procedimientos que garanticen la confidencialidad y privacidad de la información médica y los datos personales de los pacientes.
- Medidas de seguridad robustas dentro del sistema, como la encriptación de datos, el acceso restringido a la información y el monitoreo de actividades sospechosas.
- Capacitaciones del personal sobre la importancia de la confidencialidad y la protección de datos y la adhesión a las regulaciones y estándares aplicables.

El incumplimiento a la confidencialidad conllevará las responsabilidades penales, civiles y administrativas correspondientes.

ANEXO No. 2

FORMULARIO DE IDENTIFICACIÓN DEL OFERTANTE

FORMULARIO DE INFORMACIÓN/IDENTIFICACIÓN DEL OFERTANTE		
a) Referencia de Solicitud de Expresión de Interés.		
b) Nombre de la Contratación		
c) Nombre del proyecto		
d) Nombre completo de la persona natural o jurídica que está ofertando.		
e) Nacionalidad		
f) Nombre comercial de la empresa		
g) Giro o finalidad		
h) Clasificación de empresa (micro, pequeña, media o gran empresa) (aplica empresas nacionales)	Según CONAMYPE	
	Según Ministerio de Hacienda	
i) N° Registro de Contribuyente		
j) Número de Identificación Tributaria de la empresa.		
k) Dirección de la empresa		
l) Número de teléfono		
m) Correo electrónico		
n) Nombre del Representante Legal o Apoderado (aplica si es persona jurídica)		
o) Datos de la persona que labora para el ofertante y que será el contacto con la Institución.	Nombre	
	Cargo	
	Teléfono fijo	
	Teléfono celular	
	Correo electrónico	
Nombre, Firma del representante y sello de la empresa.		