ANEXO 1

DESCRIPCIÓN DEL SERVICIO

No. DE REQUISICIÓN	PARTIDA	DESCRIPCIÓN DE LOS SERVICIOS	CANT.	UNIDAD DE MEDIDA
S-101/2025	ÚNICA	CONTRATACIÓN DEL SERVICIO PARA LA RENOVACIÓN DEL LICENCIAMIENTO DEL SOFTWARE DE DETECCIÓN Y RESPUESTA A INCIDENTES INFORMÁTICOS (XDR), QUE INCLUYE INSTALACIÓN, CONFIGURACIÓN, PUESTA EN OPERACIÓN Y PRUEBAS DE FUNCIONALIDAD	1	SERVICIO

I. REQUERIMIENTOS GENERALES.

Se prevé la renovación de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR) en su versión más reciente.

"EL PROVEEDOR" deberá realizar la renovación de licenciamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR) LAB Destino (Libre Abordo Destino), acreditando este con la entrega del certificado en original físicos y/o por medios electrónicos sin costo adicional para **"LA CONVOCANTE"**, la cual se llevará a cabo en la Dirección General de Tecnología y Sistemas Informáticos ubicada Av. Coyoacán No. 1635 Edificio "A" piso 1 Col. Del Valle, Alcaldía Benito Juárez, Ciudad de México, C.P. 03100, en un horario de 09:00 a 21:00 horas de lunes a viernes en un periodo no mayor a 5 (cinco) días hábiles contados a partir del siguiente día hábil de la formalización del contrato.

"EL PROVEEDOR" deberá realizar la configuración y puesta en operación del servicio de renovación de licenciamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR), en un plazo no mayor a 20 (veinte) días hábiles contados a partir de la acreditación de la renovación del licenciamiento.

En caso de ser un fabricante diferente al actual **"EL PROVEEDOR"** deberá mantener el licenciamiento de la solución actual del software de Detección y Respuesta a incidentes Informáticos (XDR), durante el tiempo que dure la instalación, configuración, puesta en operación y pruebas de funcionalidad de la nueva solución.

"EL PROVEEDOR" entregará dentro de los 5 (cinco) días hábiles posteriores a la instalación, configuración, puesta en operación y pruebas de funcionalidad de la entrega del certificado de la renovación de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), una memoria técnica a detalle de la instalación, configuración, puesta en operación, y pruebas de funcionalidad de la renovación, así como, la información adicional que derive del mismo. Dicha memoria será previamente revisada y validada por **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos.

"EL PROVEEDOR" realizará pruebas de funcionalidad a entera satisfacción de **"LA CONVOCANTE"**, a través de la Dirección General de Tecnología y Sistemas Informáticos, los resultados de las pruebas de funcionalidad formaran parte de la memoria técnica a entregar.

"EL PROVEEDOR" proporcionará una dirección electrónica mediante escrito y/o medio electrónico dirigido a **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos, para proceder

a la descarga del certificado de licenciamiento de la renovación del software de Detección y Respuesta a Incidentes Informáticos (XDR) en su versión más reciente.

"EL PROVEEDOR" dará acceso a **"LA CONVOCANTE"** para obtener los derechos de uso que sean aplicables a la renovación del licenciamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR), al medio que sea señalado al momento de la entrega del certificado de renovación de licenciamiento.

"EL PROVEEDOR" será responsable, en caso de ser necesario, de la creación y/o modificación de las políticas, reglas, excepciones y configuraciones existentes dentro de la infraestructura tecnológica de **"LA CONVOCANTE"** para garantizar la correcta continuidad en la operación de los equipos de cómputo, así como los dispositivos tecnológicos conectados a la red institucional.

Consideraciones de Confidencialidad

"**EL PROVEEDOR**" deberá entregar un escrito bajo protesta de decir verdad en donde acredite que se hace responsable, en caso de que violen derechos de autor, propiedad intelectual o industrial, marcas o patentes a nivel nacional o internacional liberando de toda responsabilidad a "**LA CONVOCANTE**" sobre la presente relación contractual

II. DESCRIPCIÓN

Las especificaciones y características técnicas en las tablas son enunciativas y no limitativas por lo que "**EL LICITANTE**" o **"LOS LICITANTES"** deberá manifestar en su propuesta técnica las especificaciones y características técnicas ofertadas.

No.	DESCRIPCIÓN DEL SERVICIO	CARACTERÍSTICAS TÉCNICAS	CANTIDAD	UNIDAD DE MEDIDA
1	Renovación del licenciamiento del Software (XDR)	Licenciamiento del Software de Detección y Respuesta a Incidentes Informáticos (XDR) para 13,500 equipos. Consola On-premise y/o en nube Soportar los diferentes sistemas operativos que conforman **"LA CONVOCANTE",** entre ellos se encuentran: Windows, 7, 8, 8.1, 10 y Windows Server 2008, 2012, 2016, 2019, 2022. Los sistemas operativos mencionados anteriormente son para fines enunciativos mas no limitativos. Buen funcionamiento en equipos de cómputo que tengan bajos recursos a fin de que el rendimiento del equipo no disminuya. **1. Funciones Principales:** • La solución debe ser una sólida solución de	1	Licencia

		ciberseguridad para defender la infraestructura de TI corporativa contra ciberamenazas sofisticadas, incluidas aquellas que no pueden ser detectadas por las aplicaciones EPP instaladas en los activos corporativos. • La solución debe proporcionar visibilidad, correlación y automatización total. También debe aprovechar una amplia gama de herramientas de respuesta y fuentes de datos, incluidos activos de terminales y datos de red y nube. • La solución debe analizar los datos de múltiples fuentes para identificar amenazas, crear alertas para posibles incidentes y proporcionar las herramientas para responder a ellos. • Acciones de respuesta de productos de terceros y escenarios de respuesta entre productos. • Análisis dinámico de prevención de amenazas con aprendizaje base en el comportamiento de los procesos en ejecución y máquina de manera local (inferencia). • Protección contra vulnerabilidades no parchadas en Sistemas operativos Windows y Linux (virtual patching). • La solución deberá permitir analizar archivos de formatos, ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. • La solución deberá emitir sugerencias de remediación para restablecer el dispositivo a su estado original. • Módulos de seguridad para protección: ○ Protección contra amenazas basadas en comportamiento. ○ Protección contra la ejecución de procesos en memoria. ○ Detención de ejecución de archivos maliciosos ○ Bloqueo de ejecución de código malicioso ○ Protección contra la ejecución no autorizada de rutas locales ○ Protección contra la ejecución no autorizada de rutas en la red ○ Protección contra la ejecución no autorizada de medios removibles • Deberá Soportar: ○ Perfiles de seguridad y excepciones ○ Creación de políticas de seguridad personalizables. ○ Lanzamiento remoto de tareas de escaneo y actualización. ○ Escaneos bajo demanda, agendados o		

		periódicos. • Contar con: ○ Protecciones para dispositivo final ○ Detección y bloqueo por medio de la integración del marco MITRE ATT&CK ○ Mapear las técnicas utilizadas con base al framework de MITRE ATT&CK. ○ Visibilidad y trazabilidad de incidentes detectados ○ Requerimientos de visibilidad y detección ○ Requerimientos de investigación, manejo de incidentes, inteligencia de amenazas y respuesta de incidentes ○ Recolección de datos y requerimientos de integración de datos ○ Análisis de Sandbox		

- El agente deberá:
  - Soportar o controlar el firewall nativo del SO a través de una API
  - Tener control sobre los permisos de uso de los dispositivos USB del huésped
  - Escaneo de USB al insertarlos al PC.
  - Tener la capacidad de bloquear ejecución de archivos ejecutables .exe .msi, etc desde medios extraíbles.
  - Soportar la creación de reglas de prevención personalizables con base en los indicadores de compromiso.
  - Analizar comportamiento de anomalías de tráfico de red, eventos del equipo y del usuario
  - Soportar control de aplicaciones por Hash, MD5
  - Capacidad habilitada para bloquear la ejecución de software mediante políticas de listas blancas y listas negras
  - Contar con reglas de detección predefinidas, personalizable y de correlación.
  - Conexión remota al endpoint para visualización de archivos y uso de consola CMD.
  - Terminar el proceso malicioso activo sobre el equipo y el resto de endpoints.
  - Tener la capacidad de aislamiento de la red del endpoint infectado.
  - Contar con una contraseña de desinstalación
- Manejo de activos con cuando menos las siguientes funciones:
  - Evaluación de vulnerabilidades para identificar y cuantificar estas
  - Obtener la información en tiempo real incluyendo la severidad y métricas.
  - Generación de Informes ejecutivos descargables a partir de plantillas existentes y personalizables.
  - Inventario de activos con información relevante.
- Análisis de datos forenses antes y después de un incidente
- Análisis de causa raíz automático de cualquier alerta con reportes gerenciales
- La solución deberá aplicar técnicas de inteligencia artificial, analítica y machine learning experta sobre los datos recolectados y telemetría integrando sensores desde los endpoints, servidores o correo con el fin de generar alertas de alta fidelidad.
- Generación de query que permita buscar en la plataforma y generar indicadores de:
  - Compromiso, comportamiento y ejecución
  - Actividad de la red
  - Registros de las computadoras
  - Bitácoras de eventos
  - Bitácoras de seguridad

III. PERFIL DEL PROVEEDOR

"**EL PROVEEDOR**" deberá:

1. Presentar carta membretada emitida por el fabricante en la que lo respalde y avale como distribuidor autorizado, certificado y/o exclusivo del licenciamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR) objeto del presente anexo.

2. Presentar escrito bajo protesta de decir verdad donde indique que cuenta con la infraestructura para realizar la renovación del licenciamiento del Software de Detección y Respuesta a Incidentes Informáticos (XDR) que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad.

3. Presentar un escrito bajo protesta de decir verdad en donde manifieste que cuenta con un Ingeniero con certificación técnica vigente en la herramienta XDR, para brindar el soporte técnico; así como la instalación, configuración y puesta en operación que se requiera para la renovación de licenciamiento del Software de Detección y Respuesta a Incidentes Informáticos (XDR) ofertado, dicho escrito deberá anexar copia simple del certificado correspondiente, y original para cotejo.

4. Presentar al menos 3 carátulas de contratos formalizados en copia simple y original o copia certificada para cotejo en donde demuestre que tiene experiencia del manejo y soporte técnico de la tecnología XDR y EDR.

5. Presentar un escrito bajo protesta de decir verdad en donde manifieste que cuenta con un servicio automático de notificación temprana de las actualizaciones existentes para el Software de Detección y Respuesta a Incidentes Informáticos (XDR) que estén disponibles dentro de la renovación del licenciamiento.

6. Escrito bajo protesta de decir verdad que se hace responsable de que, en caso de realizar la renovación del licenciamiento, se viole derecho de autor, propiedad intelectual o industrial, marcas y patentes a nivel nacional o internacional sobre el licenciamiento que oferta.

IV. SOPORTE TÉCNICO

1. **"EL PROVEEDOR"** deberá contar con un centro de atención de soporte técnico especializado, el cual tendrá la capacidad de concentrar todas las solicitudes de soporte técnico en un único punto de contacto del tipo mesa de ayuda; asimismo, deberá presentar el procedimiento para levantar tickets de soporte vía telefónica y correo electrónico los 7 días de la semana, las 24 (veinticuatro) horas del día. Durante el periodo de garantía del servicio.

2. **"EL PROVEEDOR"** deberá presentar una lista de las direcciones de Internet, números telefónicos y correos electrónicos del área de soporte técnico, directorio de escalamiento que incluya nombre, cargo, teléfono de oficina y teléfono del personal que participará.

NOMBRE DEL CONTACTO	CARGO	TELÉFONO DE OFICINA	TELÉFONO MÓVIL	CORREO ELECTRÓNICO	DIRECCIÓN DE INTERNET	NIVEL DE ESCALAMIENTO

3. **"EL PROVEEDOR"** mantendrá permanentemente actualizado los datos del Centro de Atención de soporte técnico ya sea por cambios de domicilio, teléfono o de cualquier otra índole.

4. El sitio WEB de soporte técnico deberá contar con servicio automático de notificación temprana de las nuevas versiones del software de Detección y Respuesta a Incidentes Informáticos (XDR) que estén disponibles para el tipo de licenciamiento adquirido.

5. Durante la vigencia del licenciamiento no habrá limitante en cuanto al número de reportes y horas hombre de soporte técnico; incluido las visitas en sitio que determine la Dirección General de Tecnología y Sistemas Informáticos.

6. Una vez generado el reporte por la Dirección General de Tecnología y Sistemas Informáticos (vía telefónica y correo electrónico), el tiempo máximo para que **"EL PROVEEDOR"** se ponga en contacto vía telefónica y correo electrónico para su atención no deberá ser mayor a 30 (treinta) minutos.

7. La vigencia del servicio de Soporte Técnico será conforme el tiempo de vigencia de la garantía del licenciamiento.

TIEMPOS DE RESPUESTA ANTE INCIDENTES

Será catalogado como reportes urgentes:

I. La pérdida de un 100 % de los servicios.
II. La infección masiva de virus o malware informático en cualquier área de **"LA CONVOCANTE"**.
III. Eventos no previstos en estos numerales que sean catalogados como urgentes por la Dirección General de Tecnología y Sistemas Informáticos y que estén directamente relacionados con el servicio de renovación objeto del contrato.

Tiempo de respuesta ante reportes urgentes:

i. El tiempo máximo de solución vía telefónica no deberá exceder de 1(una) hora. En caso contrario deberá de presentarse en sitio.
ii. El tiempo máximo para llegar a sitio será de 2 (dos) horas. El tiempo máximo para el diagnóstico del problema será de 2 (dos) horas y la solución no deberá superar un periodo de 4 (cuatro) horas, en caso contrario, se deberá escalar el reporte con el fabricante y la respuesta final no deberá exceder las 24 (veinticuatro) horas, a partir del escalamiento.
iii. **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos podrá solicitar a **"EL PROVEEDOR"** un análisis integral, sin costo adicional para la **"LA CONVOCANTE"** que especifique por lo menos:
    a. Bitácora de detección, definición de la infección y solución aplicada.

Será catalogado como reportes normales:

I. Aquellos eventos que no se encuentren en los numerales de reportes urgentes y que estén provocando un mal funcionamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR) para el cual se renovó el licenciamiento.

Tiempo de respuesta ante reportes normales:

I. El tiempo máximo de solución de reportes vía telefónica y correo electrónico no deberá exceder de 3 (tres) horas. De lo contrario se procederá agendar una visita en sitio para la solución del mismo.

II. La visita en sitio podrá programarse al día siguiente hábil después de no haber sido solucionado el reporte vía telefónica y correo electrónico, el tiempo de reparación del software no deberá ser mayor a 72 (setenta y dos) horas.

V. GARANTÍAS

1. La renovación de licenciamiento del Software de Detección y Respuesta a Incidentes Informáticos (XDR) deberá tener una garantía y soporte técnico de 12 (doce) meses, contados a partir del momento de la entrega de la acreditación de la instalación del mismo a entera satisfacción de **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos.

2. Durante la vigencia de la garantía del licenciamiento, **"EL PROVEDOR"** se compromete a proporcionar a **"LA CONVOCANTE"** las nuevas versiones y actualizaciones de la renovación de licenciamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR) que hayan sido liberadas o mejoradas por el fabricante sin costo adicional para **"LA CONVOCANTE"**

3. El licenciamiento del software deberá ser original y funcionar correctamente.

4. **"EL PROVEEDOR"** se comprometerá a dar cumplimiento a esta garantía.

VI. TRANSFERENCIA DE CONOCIMIENTOS.

1. **"EL PROVEEDOR"** llevará a cabo la transferencia de conocimientos especializado teórico-práctico en el manejo del software de Detección y Respuesta a Incidentes Informáticos (XDR), una vez concluida la instalación, configuración y puesta en operación, la cual será impartida al personal de **"LA CONVOCANTE"** designado por la Dirección General de Tecnología y Sistemas Informáticos, considerando un mínimo de 4 integrantes durante la vigencia del contrato.

2. La transferencia de conocimientos será sin costo adicional para **"LA CONVOCANTE"** quien decidirá en coordinación con **"EL PROVEEDOR"** el horario, fechas, temas y lugar para su realización, entregando por escrito y correo electrónico estos, una vez validado y aprobado por el personal de la Dirección General de Tecnología y Sistemas Informáticos.

3. Una vez concluida la transferencia de conocimientos **"EL PROVEEDOR"** hará entrega de una constancia y/o diploma a los participantes en donde acredite la conclusión de la misma, la cual deberá ser validada por **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos.