## ANEXO 1

## DESCRIPCIÓN DEL SERVICIO

| No. DE REQUISICIÓN | PARTIDA | DESCRIPCIÓN DEL SERVICIO | CANT. | UNIDAD DE MEDIDA |
|---|---|---|---|---|
| S-045/2024 | 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), proporcionando una dirección electrónica mediante un escrito 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, 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 de la firma del contrato, el cual tendrá una vigencia hasta el 31 de diciembre del año en curso.

**"EL PROVEEDOR"** deberá realizar la instalación, configuración, puesta en operación y pruebas de funcionalidad 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, así como brindar el soporte técnico por un periodo de 12 (doce) meses.

**"EL PROVEEDOR"** entregará dentro de los 5 (cinco) días hábiles posteriores a la instalación, configuración, puesta en operación y pruebas de funcionalidad, 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, dentro de los 20 (veinte) días hábiles contados a partir de la acreditación de la renovación del licenciamiento.

**"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"** está obligado a guardar indefinidamente absoluta confidencialidad sobre la información que se derive de la renovación del licenciamiento del software de Detección y Respuesta a Incidentes Informáticos (XDR) objeto del contrato, por lo cual no podrá utilizar, publicar, difundir, divulgar, proporcionar, ceder o comunicar, en forma parcial o total, por ningún medio, ya sea electrónico, informático, escrito, colectivo, individual o a terceras personas ajenas a la presente prestación del servicio, cualquier tipo de información o datos, sean de acceso restringido o no, respecto a la ubicación, capacidad funcionamiento o equipos instalados.

## II. DESCRIPCIÓN

A continuación, se describen las características mínimas de la renovación del licenciamiento del Software de Detección y Respuesta a Incidentes Informáticos (XDR), para 13,500 equipos.

| No. | DESCRIPCIÓN DEL SERVICIO | CARACTERÍSTICAS TÉCNICAS | CANTIDAD | UNIDAD DE MEDIDA |
|---|---|---|---|---|
| 1 | Renovación del licenciamiento del Software de Detección y Respuesta a Incidentes Informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad | Soportar los diferentes sistemas operativos que conforman **"LA CONVOCANTE",** entre ellos se encuentran: Windows XP, 7, 8, 8.1, 10, 11 y Windows Server 2008, 2012, 2016, 2019, 2022 estos son enunciativos mas no limitativos.<br><br>**1. Funciones Principales:**<br><br>• Los equipos a proteger deberán de utilizar un sólo agente de protección, detección y respuesta ligero<br>• Análisis local y prevención de amenazas con aprendizaje máquina de manera local (inferencia).<br>• Análisis dinámico de prevención de amenazas con base en el comportamiento de los procesos en ejecución.<br>• Protección contra vulnerabilidades no parchadas (Virtual Patching) que brinde protección oportuna a las pocas horas de la publicación de la vulnerabilidad.<br>• Módulos de protección, prevención y mejoras para el agente instalado que puedan correr en Sistemas operativos Windows y Linux para protección de:<br>○ Ransomware<br>○ APC<br>○ Amenazas basadas en comportamiento<br>○ Protección contra el secuestro del control de flujos<br>○ Protección contra la ejecución de procesos hijo<br>○ Protección de vulnerabilidad de la librería del panel de control de windows<br>○ Protección contra la ejecución de procesos en memoria definidas sólo para datos | 1 | Licencia |

| | | | | |
|---|---|---|---|---|
| | | ○ Protección contra el secuestro de librerías dinámicas de enlaces<br>○ Previene el acceso a metadatos cruciales de las librerías ligadas dinámicas de fuentes no confiables<br>○ Protección de secuestro de Dylib<br>○ Protección contra la técnica de identificación (Fingerprinting) de los navegadores<br>○ Protección contra el mal manejo de los archivos de fuentes<br>○ Mejoras a la funcionalidad de Gatekeeper<br>○ Detención de ejecución de archivos maliciosos definidos por el administrados independientemente de cualquier otro veredicto<br>○ Prevención del uso de funciones del sistema para pasar DEP y ASLR<br>○ Bloqueo de ejecución de código malicioso durante la descentralización de objetos Java en servidores.<br>○ Protección contra un ataque justo a tiempo que pase por alto las mitigaciones de memoria del sistema operativo.<br>○ Monitor de integridad del kernel<br>○ Análisis local de archivos desconocidos.<br>○ Ejecutables, librerías dinámicas de enlaces y macros para determinar si son malware. El análisis deberá usar las características, atributos y un modelo estadístico generado por aprendizaje máquina para hacer inferencia.<br>○ Protección contra archivos PHP que vengan de un servidor web<br>○ Protección local contra la escalación de privilegios<br>○ Análisis de inspección de paquetes de red para detectar comportamiento malicioso<br>○ Protección contra el mapeo de la localidad 0 en el espacio de memoria.<br>○ Protección contra la ejecución no autorizada de rutas locales<br>○ Protección contra la ejecución no autorizada de rutas en la red<br>○ Protección contra la ejecución no autorizada de medios removibles<br>○ Bloqueo de redirección de flujos de entrada/salida a sockets en la red<br>○ Protección contra el secuestro de las estructuras de manejo de excepciones<br>○ Protección de áreas de la memoria usadas comúnmente para albergar cargas útiles contra técnicas de heap spray<br>○ Prevención de vulnerabilidades lógicas shell-link<br>○ Protección contra la carga dinámica de librerías desde ubicaciones no seguras<br>○ Prevención del uso de llamadas al sistema para pasar por alto las protecciones del SO<br>○ Mejoras o implementación de ASLR con | | |

| | | | | |
|---|---|---|---|---|
| | | mejor entropía, robustez y cumplimiento estricto<br>○ Detección de intentos para carga de drivers vulnerables<br>○ Uso de técnicas de aprendizaje máquina (inferencia) de manera local para determinar si un archivo es malware, además de poder enviarlo a una nube para un análisis profundo con base en un comportamiento humano para evitar técnicas de evasión de sandbox o ambientes virtuales, con componentes de deep learning y actualizaciones en tiempo real.<br>○ Identificación de ejecución de archivos grises o maliciosos en máquinas diferentes a las que detectaron el archivo original y generación de alertas<br>• Prevención de amenazas conocidas usando AI como lo son el hash de archivos<br>• Integración automática con un servicio de prevención de malware en la nube, con reporte de análisis y con soporte de recepción de archivos de cuando menos 100MB de tamaño<br>• Distribución de firmas de un archivo analizado en la nube a todos los dispositivos conectados en 5 minutos o menos<br>• Deberá soportar perfiles de seguridad y excepciones<br>• Deberá de soportar escaneos bajo demanda, agendados o periódicos inclusive generados por el usuario final ya sea para todo el equipo, un folder o un archivo<br><br>**1.2. Protecciones para el dispositivo final**<br><br>• El agente deberá de soportar un cortafuego en el huésped o controlar el firewall nativo del SO a través de una API<br>• El agente deberá poder crear políticas y reglas de encriptación del disco duro con Bitlocker y FileVault<br>• El agente deberá tener control sobre los permisos de uso de los dispositivos USB del huésped del agente<br>• El agente deberá soportar la creación de reglas de prevención personalizables con base en los indicadores de compromiso del comportamiento del equipo para detener las cadenas de causalidad<br>• El agente deberá de tener compatibilidad con un cliente para acceso remoto seguro a los equipos con agentes instalados para manejo e investigación de las alertas y casos.<br><br>**1.3 Requerimientos de visibilidad y detección**<br><br>• Análisis de comportamiento para perfilar y detectar las anomalías indicativas de un ataque analizando el tráfico de la red, los eventos del equipo y los eventos del usuario a través del tiempo<br>• Analítica de identidad para detectar amenazas de los usuarios como lo son movimientos laterales<br>• Reglas de detección predefinidas y personalizables | | |

| | | | | |
|---|---|---|---|---|
| | | basadas en la detección de comportamiento<br>• Reglas de correlación que puedan de manera retroactiva detectar ataques<br>• Capacidad de ingesta de datos de fuentes de inteligencia de amenazas de terceros<br>• Detección de técnicas de ataque a lo largo de la vida del ataque incluyendo el descubrimiento, movimientos laterales, comando y control y exfiltraciones<br>• Habilidad demostrada para detectar las tácticas y técnicas de los atacantes a través de las evaluaciones de MITRE ATT&CK<br>• Cuenta de detecciones mayores a 200 para las pruebas APT3, APT29 y Carbanak + FIN7 y visibilidad mayor a 100 para Wizard Spider + Sandworm<br>• Marcado de las alertas e incidentes según las tácticas y técnicas de MITRE ATT&CK<br>• Manejo de activos con cuando menos las siguientes funciones:<br>○ Visibilidad de los activos de en la red para descubrir dispositivos rebeldes<br>○ Evaluación de vulnerabilidades para identificar y cuantificar las vulnerabilidades. Se requiere que la información se obtenga, en tiempo real, incluyendo la severidad y métricas.<br>○ Calificaciones de riesgo de los usuarios<br>○ Inventario de activos con información relevante como, primer registro, hostname, dirección ip, ultima vista, dirección MAC, etc.<br>• Análisis de datos forenses que opere antes y después de un incidente<br><br>**1.4 Requerimientos de investigación de incidentes**<br><br>• Análisis de causa raíz automático de cualquier alerta, incluyendo alertas de red si los datos están disponibles<br>• Visualización de la cadena de ejecución que lleva a una alerta<br>• Vista de análisis de tiempos para ver las acciones y alertas en una línea del tiempo<br>• Una vista completa de los usuarios con calificaciones asociadas de riesgo, que tome la información de los usuarios de múltiples fuentes<br>• Una vista de investigación de eventos y artefactos especificamente de la nube<br>• Motor para generación de queries que permita buscar en cualquier área de la plataforma:<br>○ para indicadores de compromiso y comportamiento de los endpoints<br>○ para procesos en ejecución en el dispositivo<br>○ para archivos y modificación de archivos en el dispositivo<br>○ para actividad de la red<br>○ para registros de las computadoras en donde están instalados los agentes<br>○ para buscar en bitácoras de eventos en las en los clientes<br>○ para buscar en bitácoras de seguridad y datos en bruto en caso de tener ingesta de dispositivos de terceros como lo son cortafuegos, | | |

| | | | | |
|---|---|---|---|---|
| | | servidores, etc<br>• El motor debe soportar comodines, expresiones regulares, JSON, agregación de datos, manipulación de campos y valores, unión de datos de diferentes fuentes y visualizaciones de los datos<br>• Agrupamiento automático de información relevante como IP, información de HASH, inteligencia de amenazas y eventos relacionados en una sola vista para simplificar el proceso de investigación<br>• Identificadores de eventos bloqueados por el dispositivo, cortafuegos u otra tecnología de prevención<br>• Confección automática de información de los dispositivos, red, información de identidad de la nube, alertas de seguridad y eventos<br>• Reducción de ruido generado por alertas innecesarias<br><br>**1.5 Requerimientos de manejos de incidentes**<br><br>•Agrupamiento automático de alertas relacionadas de varias fuentes en un solo incidente<br>•Vista de supervisión de incidentes con información relevante del incidente y un despliegue de las tácticas de ataque de MITRE<br>•Calificación de incidentes a la medida<br>•Listado de artefactos notables de alertas y la información de inteligencia de amenazas relevante<br>•Listado de usuarios y hosts involucrados en un incidente para determinar rápidamente el alcance de un incidente<br>•Asignación de incidentes a miembros del equipo<br>•Capacidad de agregar comentarios a los incidentes<br>•Manejo de la vida de un incidente de punta a punta (nuevo, en investigación, cerrado, etc)<br>•Capacidad de unir incidentes<br>•Capacidad de envío de datos de incidentes e integración con aplicaciones de manejo de casos de terceros<br><br>**1.6 Requerimientos de inteligencia de amenazas**<br><br>•Capacidad de alertar acerca de objetos maliciosos conocidos en el dispositivo sin la necesidad de reglas de indicadores de compromiso.<br>•Capacidad de escanear de manera automática datos históricos de indicadores de compromiso conforme son añadidos al sistema y poder levantar alarmas.<br>•Integración sin necesidad de configuración con cuando menos 1 servicio de inteligencia de amenazas para marcadores y contexto adicional de los artefactos clave.<br>•Ingestión de inteligencia de amenazas de fuentes de terceros en cuando menos formatos JSON y CSV<br>•Interacción con los indicadores de compromiso por medio de APIs para poder integrar la plataforma con otros desarrollos<br>•Capacidad de importar múltiples indicadores de compromiso usando una API soportando cuando menos un ritmo de 600 alertas por minuto<br>•Severidad del nivel de los indicadores de compromiso configurable | | |

| | | | | |
|---|---|---|---|---|
| | | **1.7 Requerimientos de respuesta a incidentes**<br><br>•Que la plataforma de gestión cuente con una terminal remota para poderse conectar a los dispositivos que cuenten con el agente<br>•Capacidad de uso de la CMD, PowerShell y comandos de Python y soporte para scripts en Windows 7, 8 y 10<br>•Capacidad de uso de bash sin restricciones y comandos en pythons para Windows y Linux<br>•Capacidad de ejecutar scripts de Python de manera simultánea en los dispositivos en Windows y Linux<br>•Scripts predefinidos que permitan a analistas de cualquier nivel recolectar datos, investigar y responder amenazas de manera sencilla.<br>•Aislamiento remoto de uno o múltiples dispositivos excepto con la nube de gestión para evitar que la amenaza continúe.<br>•Borrado remoto de ficheros de uno o varios dispositivos.<br>•Función de búsqueda y destrucción de archivos maliciosos en los dispositivos<br>•Deberá de contar con una vista que despliegue el resultado de la ejecución del script para confirmar que se ejecutó de manera correcta o incorrecta<br>•Recolección automática o manual de la colección de archivos y objetos que están en cuarentena<br>•Capacidad para ver, suspender o terminar los procesos en ejecución o descargar archivos binarios a través de un gestor gráfico de tareas para Windows y Linux<br>•Sugerencias de remediación para restablecer el dispositivo a su estado original<br>•Integración con cortafuegos para bloquear el acceso a dominios maliciosos<br>•Integración con sistemas de orquestación, automatización y respuesta para solución y análisis de incidentes<br><br>**1.8 Recolección de datos y requerimientos de integración de datos**<br><br>•Capacidad de ingesta virtual de cualquier fuente de datos incluyendo equipos de red, endpoints, nube, identidad, aplicaciones, HR, y cualquier otra fuente de datos para cacería de amenazas, correlación y detección<br><br>**1.9 Requerimientos de recursos y soporte para el agente**<br><br>•Soporte para todas las versiones recientes de Windows incluyendo Windows Server<br>•Soporte para Chrome OS<br>•Soporte para las principales distribuciones de Linux<br>•Auditoría completa para todas las acciones del sistema.<br>•Capacidad de empujar a las agentes actualizaciones desde la consola de administración<br>•Capacidad de actualizar los agentes de manera automática<br>•Capacidad de actualizar los agentes entre pares para optimizar el consumo de capacidad de la red<br>•Control granular sobre los agentes para las notificaciones, visibilidad en la barra de tareas, | | |

| | | | | |
|---|---|---|---|---|
| | | notificaciones personalizadas de las notificaciones y la opción de restringir las opciones en las respuestas<br>•Soporte para VDI no persistentes<br>•Capacidad de soportar de manera temporal sesiones para máquinas que de manera repetida se revierten a imágenes en las que el agente no está instalado<br><br>**1.10 Despliegue, gestión y seguridad**<br><br>•Escalable, basada en la nube y uso de agentes.<br>•Una única consola de gestión web tanto para la seguridad de los dispositivos como para la detección extendida y respuesta.<br>•Control de acceso basado en roles con permisos granulares para un mejor control de los analistas.<br>•Autenticación soportando SSO con SAML 2.0 para la gestión.<br>•Tablero personalizable para información de la operación y estado de la seguridad.<br>•Integración con Kubernetes para despliegues y gestión en un ambiente de contenedores.<br>•Servicio de intermediario local para agregar y gestionar la comunicación entre terminales y una consola gestionada en la nube<br>•APIs estándar para permitir la integración de herramientas de gestión de terceros para realizar acciones administrativas<br><br>**1.11 Retención de datos y requerimientos de cobertura**<br><br>•Visibilidad en los movimientos laterales en la red y en otras partes de la infraestructura<br>•Detección y respuesta para amenazas involucradas en dispositivos gestionados y no gestionados<br>•Detección y respuesta para amenazas que involucran a usuarios remotos<br>•Detección y respuesta para amenazas que involucran servidores en la nube<br>•Recolección y centralización continua de todos los datos para hacer análisis de comportamiento<br>•Retención de cuando menos 30 días y con opción a un tiempo ilimitado<br>•Un año de retención para las bitácoras de auditoría de actividad administrativa e investigativa<br><br>**1.12 Requerimientos de servicios administrados**<br><br>•Monitoreo y caza de amenazas 24/7<br>•Continuidad en la caceria de amenazas en dispositivos gestionados o no gestionados analizando la red y los datos de la terminal<br>•Generación y entrega de reportes de amenazas y reportes de impacto por correo electrónico, syslog, slack y alertas en la consola de administración<br>•Capacidad para ingerir, priorizar y clasificar alertas de todos los proveedores<br>•Identificación y validación de amenazas críticas en una hora o menos<br>•Visibilidad de las fuentes de datos que incluye | | |

| | | | | |
|---|---|---|---|---|
| | | dispositivos terminales, paquetes y sesiones de red y paquetes, sesiones y configuraciones de la nube<br>•Monitoreo y detección de anomalías en el comportamiento de dispositivos no gestionados<br>•Monitoreo y detección de anomalías en el comportamiento de los usuarios<br>•Ajuste fino de las herramientas al ambiente individual del cliente, incluyendo reglas y excepciones a la medida<br>•Acceso a soporte con especialistas vía teléfono, email o sistema de mensajería<br>•Acceso a herramientas de soporte a través de un portal web del fabricante. | | |

## 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 para brindar el soporte técnico; así como la instalación, configuración, puesta en operación y pruebas de funcionalidad 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, nivel de escalamiento que incluya nombre, cargo, teléfono de oficina y teléfono móvil 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 de la garantía del licenciamiento no habrá limitante en cuanto al número de reportes y horas 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 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 por un período de 12 (doce) meses, contados a partir del momento de la entrega de la acreditación de la instalación, configuración, puesta en operación y pruebas de funcionalidad 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). Esta será impartida al personal de "**LA CONVOCANTE"** designado por la Dirección General de Tecnología y Sistemas Informáticos, considerando un mínimo de 4 integrantes sin exceder de 10 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.