ANEXO 1

DESCRIPCIÓN DEL SERVICIO

REQ.	PARTIDA	DESCRIPCIÓN DEL SERVICIO	CANTIDAD	UNIDAD DE MEDIDA
S-074/2026	ÚNICA	CONTRATACIÓN DE LA RENOVACIÓN DEL SERVICIO DE 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 del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, en su versión más reciente.

"EL PROVEEDOR" cumplirá con la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad 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 de la firma del contrato o de manera inmediata y sincronizada al momento en que la vigencia del licenciamiento actual expire, asegurando en todo momento la continuidad operativa de la plataforma durante 12 (doce) meses contados a partir de la entrega del certificado del licenciamiento.

"EL PROVEEDOR" se obliga a entregar dentro de los 3 (tres) días hábiles posteriores a la firma del contrato un plan de trabajo para la instalación, configuración, puesta en operación y pruebas de funcionalidad de la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad.

"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 formarán parte de la memoria técnica a entregar.

"LA CONVOCANTE", a través de la Dirección General de Tecnologías y Sistemas Informáticos, verificará que la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, implementado cumpla en su totalidad con las características ofertadas.

"EL PROVEEDOR" deberá realizar la instalación, configuración, puesta en operación y pruebas de funcionalidad de la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, en un plazo no mayor a 30 (treinta) 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 contados a partir de la entrega del certificado.

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" tiene la responsabilidad de entregar, dentro de los 5 (cinco) días hábiles posteriores a la instalación, configuración, puesta en operación y pruebas de funcionalidad de la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, una **memoria técnica a detalle** que documente exhaustivamente dichas actividades, así como toda la información técnica que derive de las mismas.

De manera general, **"El PROVEEDOR**" deberá incluir evidencia en dicho documento del desglose de la arquitectura, los parámetros de configuración técnica, las políticas de seguridad, así como cualquier ajuste personalizado y criterios de optimización realizados para garantizar la plena operatividad y estabilidad del servicio realizado, esta configuración deberá estar respaldada por personal certificado. Dicha memoria será previamente revisada y validada por personal designado por la Dirección General de Tecnología y Sistemas Informáticos, quien verificará que los ajustes se alineen con los estándares y requerimientos institucionales.

"EL PROVEEDOR" dará acceso a **"LA CONVOCANTE"** para obtener los derechos de uso que sean aplicables a la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, 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 dónde está obligado a guardar indefinidamente absoluta confidencialidad sobre la información que se derive de la prestación del servicio, por lo cual no podrá utilizar, publicar, difundir, divulgar en forma parcial o total a terceras personas ajenas a la presente relación de servicio.

Uso de marcas y patentes

"**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

"EL PROVEEDOR" deberá apegarse estrictamente a los requerimientos establecidos en el presente documento; asimismo, es importante señalar que las especificaciones y características técnicas aquí descritas son de carácter enunciativo más no limitativo, por lo que **"EL PROVEEDOR"** tendrá la obligación de manifestar detalladamente en su propuesta técnica las especificaciones y características técnicas finales ofertadas para el cumplimiento óptimo del servicio.

No.	DESCRIPCIÓN DEL SERVICIO	CARACTERÍSTICAS TÉCNICAS	CANTIDAD	UNIDAD DE MEDIDA
1	Renovación del servicio de licenciamiento del software de detección y respuesta a Incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad	Consola On-premise y/o en nube Soporta los diferentes sistemas operativos que conforman **"LA CONVOCANTE"**, entre ellos se encuentran: Windows, 7, 8, 8.1, 10, 11 y Windows Server 2008, 2012, 2016, 2019, 2022 y 2025. Los sistemas operativos mencionados anteriormente son para fines enunciativos más 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 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 basado 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:	1	SERVICIO

		○ 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 Se requiere la renovación de licenciamiento de los siguientes componentes del software XDR: 1. Consola de administración. 2. Licencia de Software de detección y respuesta a incidentes informáticos (XDR) para 11,000 equipos. 3. Implementación total del alcance de los agentes contratados. 4. Puesta a punto de la plataforma y todos sus componentes licenciados con base en las mejores prácticas.		

1. 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, personalizables 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

2. 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.

3. Análisis de datos forenses antes y después de un incidente

4. Análisis de causa raíz automático de cualquier alerta con reportes gerenciales

5. 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.

6 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 servicio de 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 del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos

(XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, 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 detección y respuesta a Incidentes informáticos (XDR).

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 de detección y respuesta a incidentes Informáticos (XDR) que estén disponibles dentro de la renovación del licenciamiento.

6. **"EL PROVEEDOR"** se obliga a entregar a **"LA CONVOCANTE"** a la firma del contrato, una Póliza de Seguro de Responsabilidad Civil vigente, emitida por una institución aseguradora legalmente autorizada para operar en territorio nacional, la cual deberá cubrir daños físicos y materiales, afectaciones o responsabilidades derivadas de la prestación de los servicios objeto del presente Anexo Técnico y en caso de renovación durante la vigencia contractual, deberá proporcionar la actualización correspondiente a la Fiscalía General de Justicia de la Ciudad de México.

   La póliza deberá permanecer vigente durante toda la ejecución contractual y contemplar, al menos, cobertura respecto de:

   - Daños a la infraestructura tecnológica y de comunicaciones.
   - Afectaciones derivadas de errores, omisiones o negligencia en la prestación del servicio.
   - Riesgos asociados a actividades de administración, configuración, operación o soporte de herramientas de ciberseguridad y gestión de vulnerabilidades.
   - Daños ocasionados por intervención del personal técnico asignado al proyecto.
   - Responsabilidad derivada de incidentes que afecten la disponibilidad, integridad o confidencialidad de la información institucional, cuando éstos sean atribuibles al proveedor.

La indemnización correspondiente, se hará conforme a lo dispuesto en el artículo 1915 y demás relativos del Código Civil para el Distrito Federal, y en correlación con la Ley Federal del Trabajo, sin perjuicio de las acciones legales que **"LA CONVOCANTE"** considere pertinentes, así como con el Lineamiento Septuagésimo de los Lineamientos.

La falta de presentación de dicha póliza, su vencimiento o cancelación durante la prestación del servicio podrá ser motivo de incumplimiento contractual y dará lugar a las acciones administrativas y legales que correspondan conforme a la normatividad aplicable y a las condiciones contractuales establecidas.

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 actualizados 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 renovación del servicio de licenciamiento.

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:

1. La pérdida de un 100 % de los servicios.
2. La infección masiva de virus o malware informático en cualquier área de **"LA CONVOCANTE"**.
3. 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:

1. El tiempo máximo de solución vía telefónica no deberá exceder de 1(una) hora. En caso contrario deberá de presentarse en sitio.
2. 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.
3. **"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:

1. 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:

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

"LA CONVOCANTE" con fundamento en el artículo 69 de la **LADF**, artículos 57 y 58 del **RLADF** y los Lineamientos Septuagésimo segundo, Septuagésimo tercero y Septuagésimo cuarto de los Lineamientos, aplicará penas convencionales por incumplimiento o atraso en la prestación del servicio a **"EL PROVEEDOR"**, se calcularán tomando como base el monto total del servicio, conforme a lo siguiente, de manera enunciativa más no limitativa:

Penalización (Incumplimiento)	Porcentaje (El porcentaje por incumplimiento será calculado sobre el monto total del servicio)	Cómputo
Entrega del certificado de la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, en original físicos y/o por medios electrónicos.	3.0%	Se aplicará por cada día natural de incumplimiento o atraso, a partir de la fecha que se indica como entrega en el numeral I. Requerimientos Generales.
Entrega del Plan de trabajo para la Instalación, Configuración, puesta en operación y pruebas de funcionalidad.	3.0%	Se aplicará por cada día natural de incumplimiento o atraso, a partir de la fecha que se indica como entrega en el numeral I Requerimientos Generales.
Entrega de Memoria técnica a detalle	3.0%	Se aplicará por cada día natural de incumplimiento o atraso, pasados los 5 días hábiles posteriores de la

		instalación, configuración y puesta en operación que indica el plan de trabajo.
Incumplimiento en el tiempo de respuesta para reportes urgentes, tiempo de solución de reportes urgentes, tiempo de respuesta para reportes normales y tiempo de solución de reportes normales.	3.0%	Se aplicará por cada hora ante incidente urgente o normal que no sea atendido dentro de los tiempos máximos establecidos en el presente Anexo y por cada hora ante incidente urgente o normal que no sea solucionado dentro de los tiempos máximos establecidos en el presente Anexo.
Transferencia de conocimiento con acreditación de certificación.	3.0%	Se aplicará por cada día natural de atraso, a partir de la fecha de validación y aprobación por el personal de la Dirección General de Tecnología y Sistemas Informáticos.

VI. GARANTÍAS DEL SERVICIO

1. La renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad, deberá tener una garantía y soporte técnico de 12 (doce) meses, contados a partir del momento de la entrega del certificado de licenciamiento en original físicos y/o por medios electrónicos a **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos.

    a. **"EL PROVEEDOR"** se compromete a dar cumplimiento a esta garantía.

2. Durante la vigencia de la garantía del licenciamiento, **"EL PROVEEDOR"** se compromete a proporcionar a **"LA CONVOCANTE"** las nuevas versiones y actualizaciones de la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad 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.

VII. GARANTÍA DE CUMPLIMIENTO.

Con la finalidad de garantizar el cumplimiento de todas y cada una de las obligaciones derivadas del contrato que se formalice con motivo del presente procedimiento de contratación, **"EL PROVEEDOR"** deberá presentar una fianza de cumplimiento expedida por una institución afianzadora legalmente autorizada para operar en los Estados Unidos Mexicanos.

Dicha fianza deberá constituirse a favor de la Fiscalía General de Justicia de la Ciudad de México por un importe equivalente al 10% (diez por ciento) del monto total del contrato, sin incluir el Impuesto al Valor Agregado (IVA), y deberá permanecer vigente durante toda la ejecución contractual, incluyendo el periodo de garantía establecido para el licenciamiento.

La fianza tendrá por objeto garantizar el cumplimiento oportuno y adecuado de las obligaciones contractuales asumidas por **"EL PROVEEDOR"**, incluyendo la entrega del licenciamiento, la instalación, configuración, puesta en operación, pruebas de funcionalidad, soporte técnico, actualización de versiones, corrección de fallas, atención de incidencias y demás obligaciones establecidas en el contrato y su Anexo Técnico.

VIII. TRANSFERENCIA DE CONOCIMIENTOS.

1. **"EL PROVEEDOR"** llevará a cabo la transferencia de conocimientos especializado teórico-práctico en el manejo de la renovación del servicio de licenciamiento del software de detección y respuesta a incidentes informáticos (XDR), que incluye instalación, configuración, puesta en operación y pruebas de funcionalidad 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.

IX. ACTA ENTREGA DEL SERVICIO

"EL PROVEEDOR" y **"LA CONVOCANTE"** a través de la Dirección General de Tecnología y Sistemas Informáticos elaborarán en conjunto un acta entrega del servicio una vez concluidas todas y cada una de las entregas establecidas en el presente anexo.