



CONTRATO CERRADO PARA LA PRESTACIÓN DEL SERVICIO INTEGRAL DE CIBERSEGURIDAD, QUE CELEBRAN, POR UNA PARTE, EL EJECUTIVO FEDERAL POR CONDUCTO DEL INSTITUTO NACIONAL PARA LA EDUCACIÓN DE LOS ADULTOS, EN LO SUCESIVO “EL INEA”, REPRESENTADO POR LA C. MARÍA ISABEL MONTOYA OBREGÓN, EN SU CARÁCTER DE APODERADA LEGAL Y TITULAR DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS, ASISTIDA EN ESTE ACTO POR LA C. MARÍA DOLORES DURÁN MÁRQUEZ, EN SU CARÁCTER DE SUBDIRECTORA DE RECURSOS TECNOLÓGICOS; QUIEN FUNGIRÁ COMO PERSONA ADMINISTRADORA DEL CONTRATO, ASÍ TAMBIÉN POR EL C. ROBERTO RAMÍREZ GUZMÁN, EN SU CARÁCTER DE JEFE DE DEPARTAMENTO DE SOPORTE TÉCNICO, CENTRO DE DATOS Y COMUNICACIONES, QUIEN FUNGIRÁ COMO PERSONA SUPERVISORA DEL CONTRATO Y POR LA OTRA, EXECUDATA, S.A. DE C.V., EN LO SUCESIVO “EL PROVEEDOR”, REPRESENTADA POR EL C. FRANCISCO VALENTE RAMOS O'REILLY, EN SU CARÁCTER DE ADMINISTRADOR ÚNICO, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ “LAS PARTES”, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

I. “EL INEA” declara que:

I.1 Es un Organismo Descentralizado de la Administración Pública Federal, agrupado en el sector coordinado por la Secretaría de Educación Pública y Subsecretaría de Educación Básica con personalidad jurídica y patrimonio propio, creado por Decreto Presidencial el 28 de agosto de 1981, publicado en el Diario Oficial de la Federación (DOF) el 31 de ese mismo mes y año, reformado por diverso de fecha 17 de agosto de 2012, publicado en el DOF el 23 de agosto de 2012.

I.2 Conforme a la escritura pública número 79,644 de fecha 20 de febrero de 2024, pasada ante la fe de la Lic. Liliana Gutiérrez Robles, titular de la notaría pública número 44 de la Ciudad de México, la C. María Isabel Montoya Obregón con R.F.C. MOOI570119MR9, Apoderada legal y Titular de Unidad de Administración y Finanzas de **“EL INEA”**, es la persona servidora pública que cuenta con facultades legales para celebrar el presente contrato, quien podrá ser sustituida en cualquier momento en su cargo o funciones, sin que por ello, sea necesario celebrar un convenio modificatorio.

I.3 De conformidad con el Manual General de Organización del INEA 2020, suscribe el presente instrumento la C. María Dolores Durán Márquez, con R.F.C. DUMD6808112R5, en su carácter de Subdirectora de Recursos Tecnológicos, persona facultada para administrar el cumplimiento de las obligaciones que deriven del objeto del contrato, quien podrá ser sustituido en cualquier momento, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, informando a **“EL PROVEEDOR”**.

I.4 De conformidad con el *Manual General de Organización del INEA 2020*, suscribe el presente instrumento el C. Roberto Ramírez Guzmán, con R.F.C. RAGR740522162, en su carácter de Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones, persona facultada para supervisar que se brinde el servicio conforme a los términos y



condiciones establecidos en el contrato y su **“Anexo Único”** (el cual se conforma por las proposiciones técnica y económica) que forma parte integrante del mismo.

I.5 La adjudicación del presente contrato se realizó mediante el procedimiento de Invitación a cuando menos Tres Personas Nacional Electrónica IA-11-MDA-011MDA001-N-60-2024, al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 26 fracción II, 26 Bis fracción II, 27, 28 fracción I, 29, 40 párrafo tercero, 42 párrafos primero y tercero, 43 y 45 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **“LAASSP”**, y demás aplicables de su Reglamento, notificando el fallo al segundo lugar de dicho procedimiento en fecha 11 de junio de 2024 en CompraNet.

I.6 “EL INEA” cuenta con suficiencia presupuestaria otorgada mediante cédula SRT/027/24 en la partida presupuestal 33901 “Servicios profesionales, científicos y técnicos integrales” de fecha 7 de mayo de 2024, emitida por la Subdirección de Presupuesto y Recursos Financieros.

I.7 Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes INE810901CP4.

I.8 Tiene establecido su domicilio en calle Francisco Márquez número 160, colonia Condesa, demarcación territorial Cuauhtémoc, código postal 06140, Ciudad de México, mismo que señala para los fines y efectos legales del presente.

II. “EL PROVEEDOR” declara que:

II.1 Es una persona moral legalmente constituida conforme a las leyes mexicanas, lo que acredita a través de la escritura pública número 73,727 de fecha 7 de diciembre de 2009, otorgada ante la fe del Licenciado Javier Ceballos Lujambio, titular de la notaría pública número 110 del Distrito Federal, hoy Ciudad de México, misma que no ha sufrido modificaciones; denominada EXECUDATA, S.A DE C.V., cuyo objeto social es el diseño, fabricación, creación, registro, maquila, compra, venta, importación o exportación, comercialización, distribución, alquiler o renta, de todo tipo de programas de computación electrónica, nacionales o extranjeros, para usos tanto del hogar como oficina industrial o comercio, dentro y fuera de la república Mexicana, entre otros; con número de Inscripción en el Registro Público de Comercio 411730 de fecha 11 de febrero de 2010.

II.2 El C. Francisco Valente Ramos O’Reilly, en su carácter de Administrador Único, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada, como lo acredita con la escritura pública antes referida, mismas que bajo protesta de decir verdad manifiesta no le han sido limitadas ni revocadas en forma alguna.

II.3 Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para su cumplimiento.

II.4 Cuenta con su Registro Federal de Contribuyentes EXE0912089N5.

II.5 Acredita el cumplimiento de sus obligaciones fiscales en términos de lo dispuesto en el artículo 32-D del Código Fiscal de la Federación vigente, incluyendo las de Aportaciones



Patronales y Entero de Descuentos, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y las de Seguridad Social ante el Instituto Mexicano del Seguro Social, conforme a las Opiniones de Cumplimiento de Obligaciones Fiscales emitidas por el SAT, INFONAVIT e IMSS, respectivamente.

II.6 Tiene establecido su domicilio en calle Rodrigo Cifuentes número 34, colonia San José Insurgentes, demarcación territorial Benito Juárez, código postal 03900, Ciudad de México, mismo que señala para los fines y efectos legales del presente.

III. “LAS PARTES” declaran que:

III.1 Es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

“EL PROVEEDOR” acepta y se obliga a proporcionar a “EL INEA” el *servicio integral de ciberseguridad*, en los términos y condiciones establecidos en la convocatoria, este contrato y su “Anexo Único” (el cual se conforma por las proposiciones económica y técnica) que forma parte integrante del mismo.

SEGUNDA. MONTO DEL CONTRATO.

“EL INEA” pagará a “EL PROVEEDOR” como contraprestación por el servicio objeto de este contrato, la cantidad de **\$5,188,952.16 (Cinco millones ciento ochenta y ocho mil novecientos cincuenta y dos pesos 16/100 M.N.)** más impuestos que ascienden a **\$830,232.35 (Ochocientos treinta mil doscientos treinta y dos pesos 35/100 M.N.)** dando un total de **\$6,019,184.51 (Seis millones diecinueve mil ciento ochenta y cuatro pesos 51/100 M.N.)**.

El monto total, será ejercido conforme a los precios unitarios ofertados por “EL PROVEEDOR”:

Descripción	Precio Unitario Mensual
Servicio Integral Ciberseguridad	\$444,767.58
Servicio EDR	\$296,511.30

Conforme al “Anexo Único”.

El precio es considerado fijo y en moneda nacional peso mexicano hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en el *servicio integral de ciberseguridad*, por lo que “EL PROVEEDOR” no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.



TERCERA. ANTICIPO.

Para el presente contrato **“EL INEA”** no otorgará anticipo a **“EL PROVEEDOR”**.

CUARTA. FORMA Y LUGAR DE PAGO.

“EL INEA” efectuará el pago a través de transferencia electrónica en pesos de los Estados Unidos Mexicanos, a mes vencido conforme a los servicios efectivamente prestados y a entera satisfacción del Administrador (a) del contrato y de acuerdo con lo establecido en su **“Anexo Único”** que forma parte integrante de este contrato.

Con fundamento en el artículo 51 de la **“LAASSP”**, el pago no podrá exceder de 20 (veinte) días naturales contados a partir de la entrega de la factura respectiva, previa a la prestación del servicio en los términos del instrumento jurídico y a entera satisfacción del Administrador (a) del contrato, según lo establecido en el **“Anexo Único”**.

Para que **“EL INEA”** esté en condiciones de iniciar las gestiones de pago, **“EL PROVEEDOR”** de conformidad a lo establecido en el **“Anexo Único”** y a los artículos **29** y **29-A** del **Código Fiscal de la Federación** y los correlativos de su Reglamento, está obligado a enviar al Supervisor (a) del contrato el **comprobante fiscal digital (CFDI)**, así como sus archivos electrónicos **.XML** y **.PDF**

“EL PROVEEDOR” para la elaboración del **CFDI** deberán considerar lo siguiente:

- **Emitido a nombre de:** Instituto Nacional para la Educación de los Adultos.
- **RFC:** INE810901CP4.
- **Domicilio:** Calle Francisco Márquez número 160, colonia Condesa, código postal 06140, demarcación territorial Cuauhtémoc, Ciudad de México.
- **Régimen Fiscal:** 603 personas morales con fines no lucrativos.
- **Uso del CFDI:** Gastos en general.
- **Rubro concepto/descripción:** indicar si es pago único, o el número de pago que corresponda, ejemplo: primer o segundo pago del contrato, número de contrato o convenio, mes de pago en caso de que aplique y descripción breve del servicio realizado o producto adquirido.
- **Forma de pago:** Transferencia electrónica.
- **Método de pago:** Pago en parcialidades o diferido (PPD)
- **Todos los CFDI deberán ser emitidos en la versión 4.0.**

“EL PROVEEDOR”, antes de emitir el **CFDI** para su pago, deberá enviar al Supervisor (a) del contrato, por medio de correo electrónico, un proyecto del mismo. Lo anterior, con la finalidad de que el Supervisor (a) valide o realice las observaciones correspondientes y posteriormente **“EL PROVEEDOR”** emita y envíe la versión final del **CFDI**.

“EL PROVEEDOR” deberá enviar vía correo electrónico al Supervisor (a), dentro de los primeros 3 (tres) días naturales del mes calendario o del mes que corresponda, la versión final timbrada del **CFDI (dentro de este plazo queda comprendido el párrafo que antecede)**; éste último contará con 3 (tres) días hábiles a partir de la recepción del **CFDI**, para devolverla con las observaciones pertinentes o, en su caso iniciar la gestión de pago con la aceptación de la versión final timbrada.



Una vez aceptada la versión final timbrada del **CFDI**, el Administrador (a) del contrato la enviará junto con sus archivos electrónicos **.XML y .PDF**, por correo electrónico al Departamento de Control Presupuestal (**DCP**) (ifrias@inea.gob.mx y dpc_control@inea.gob.mx).

El Administrador (a) del contrato, independientemente de lo señalado en el párrafo previo, también deberá entregar a la Subdirección de Presupuesto y Recursos Financieros (**SPRF**), dentro de los primeros 12 (doce) días naturales del mes de que se trate, contados a partir de la recepción de la factura timbrada y soporte documental respectivo, el oficio o nota debidamente firmado por el mismo, a través del cual se entrega el soporte documental del pago correspondiente y que contendrá lo siguiente:

- 3 (tres) tantos de la *Solicitud de Recursos para Pedidos y Contratos*, firmada en original por el Administrador (a) del contrato correspondiente y el Titular del área requirente.
- Impresión de **CFDI**, XML y verificación del **SAT**.
- Copia del oficio de liberación de pago firmado por el Administrador (a) del contrato.
- Copia del oficio de supervisión del servicio dirigido al Administrador (a) del contrato y que será firmado por el Supervisor (a).
- Copia de la suficiencia presupuestal
- Para el trámite del **primer pago** deberá también adjuntar a la solicitud copia del contrato o convenio.
- En caso de **último pago** deberá también adjuntar copias de la Constancia de cumplimiento y del finiquito conforme lo consigne el contrato.

Si por algún motivo se cancela el **CFDI** durante el proceso de pago, será responsabilidad de **“EL PROVEEDOR”** notificar por escrito al Administrador (a) del contrato, quien a su vez informará por escrito a la **SPRF**.

Los pagos se efectuarán a través de cuentas por liquidar certificadas (CLC), apoyados en los mecanismos de banca electrónica del Sistema Integral de Administración Financiera Federal (**SIAFF**) de la Tesorería de la Federación mediante enlace con el Sistema de Contabilidad y Presupuesto (**SICOP**) por instrucción de la **Unidad de Administración y Finanzas** mediante **transferencia electrónica de recursos** a la cuenta bancaria señalada por **“EL PROVEEDOR”** previamente registrada, por el importe del servicio proporcionado.

Para dar cumplimiento a lo anterior, será indispensable que **“EL PROVEEDOR”** entregue al Departamento de Tesorería (**DT**) de **“EL INEA”**, dentro de los 3 (tres) días hábiles posteriores al fallo, la documentación de forma física y electrónica que se cita abajo, con la finalidad de dar de alta en los Sistemas Federales de pago, **SICOP** y **SIAFF** de la Tesorería de la Federación:

- a) Acta constitutiva inscrita en el Registro Público de la Propiedad y del Comercio, así como sus respectivas modificaciones.
- b) Copia del instrumento notarial donde consten las facultades de representante y/o apoderado legal.
- c) Identificación oficial vigente (credencial de elector o cartilla del servicio militar nacional o cédula profesional o pasaporte) de la persona que se ostente como representante y/o apoderado legal.



- d)** Copia de la Constancia de Situación Fiscal y Registro Federal de Contribuyentes (RFC) expedido por la Secretaría de la Hacienda y Crédito Público (SHCP) no mayor a 3 (tres) meses.
- e)** Formato del Catálogo de Beneficiarios debidamente requisitado, con sello de la empresa y firma autógrafa del representante y/o apoderado legal, que podrá descargar para su llenado en la siguiente liga: https://www.sep.gob.mx/es/sep1/Formatos_Vigentes, o solicitarlo al DT a las siguientes direcciones de correo electrónico: juangc@inea.gob.mx; dt_pagos@inea.gob.mx.
- f)** Constancia del domicilio fiscal no mayor a 3 (tres) meses.
- g)** Para el caso de personas físicas, copia del CURP.
- h)** Constancia de la institución financiera sobre la existencia de la cuenta de cheques abierta a nombre del beneficiario, que incluya el número de cuenta con once posiciones, así como la clave bancaria estandarizada (CLABE) con dieciocho posiciones, que permita realizar transferencias electrónicas de fondos a través de los sistemas federales de pagos, esta debe incluir la sucursal de apertura de la cuenta bancaria.

“EL INEA” pagará a **“EL PROVEEDOR”**, conforme a las condiciones que se consignan en el contrato, y quedará condicionado proporcionalmente, al pago que **“EL PROVEEDOR”** deba efectuar por concepto de penas convencionales determinadas y verificadas por el Administrador (a) del contrato.

El Administrador (a) y **“EL PROVEEDOR”**, serán los únicos responsables de realizar el cálculo en caso de pagos en exceso, **“EL PROVEEDOR”** deberá reintegrar dichas cantidades, más las cargas financieras correspondientes, conforme a una tasa que será igual a la establecida por la Ley de Ingresos de la Federación en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades pagadas en exceso en cada caso y se computarán por días naturales desde la fecha de pago hasta la fecha en que se pongan efectivamente las cantidades a disposición de **“EL INEA”**. Para el efecto anterior, **“EL PROVEEDOR”** autoriza en este acto a **“EL INEA”** a deducir dichas cantidades de cualquier crédito pendiente de pago.

- **“EL PROVEEDOR”** mediante oficio, firmado por el representante y/o apoderado legal, lo entregará al DT, en el que solicitará una clave RAP para efectuar el depósito referenciado a la cuenta bancaria Institucional por la devolución del recurso pagado en exceso.
- **“EL PROVEEDOR”** deberá remitir el comprobante de pago al DT por el monto de la devolución del recurso y en su caso, pagar las cargas financieras que pudieran generarse en caso de no devolver el recurso en el ejercicio fiscal correspondiente.

El Administrador (a) y/o Supervisor (a) del contrato será responsable de dar seguimiento al pago de **“EL PROVEEDOR”**, de cualquier accesorio que se genere por incumplimiento al contrato y hasta su liberación.



Si el **“EL PROVEEDOR”** estuviere inconforme con la liquidación del pago, tendrá un plazo de 10 (diez) días naturales, a partir de la fecha en que se haya formulado la liquidación del pago, para hacer por escrito la reclamación dirigida a la **Unidad de Administración y Finanzas**. Si transcurrido este plazo, **“EL PROVEEDOR”** no la efectúa, se considerará que la liquidación del pago, quedará definitivamente aceptada por él y sin derecho a ulterior reclamación.

De acuerdo a la obligación de emitir facturas **“CFDI con Complemento para la Recepción de Pagos”** en cumplimiento a la regla **2.7.1.32.** de la Resolución Miscelánea Fiscal para el ejercicio 2024.

Los escenarios para emitir el **CFDI** con Complemento para la Recepción de Pagos (Recibo Electrónico de Pagos), son los siguientes:

1. Al emitir el **CFDI** y hacer el pago en ese momento, **no hay obligación de emitir el complemento de pago**, el **CFDI** debe contener los siguientes datos en la forma de pago: 03 Transferencia electrónica de fondos, Método de pago: PUE (Pago en una sola Exhibición).
2. Al emitir el **CFDI** y **el pago se hace posteriormente**, es decir al hacer un **pago diferido (PPD)** del total de la factura, **se deberá emitir el complemento de pago**. El **CFDI** del complemento deberá tener los siguientes datos: Cantidad: 1; Unidad: ACT; Descripción: Pago; Clave Prod. Serv. 84111506 Servicios de facturación. Precio unitario 0 (cero); Importe 0 (cero).
3. Al emitir el **CFDI** y el pago se hace **en parcialidades (PPD)** **se deberá hacer el complemento por el pago de cada parcialidad**. El **CFDI** del complemento deberá tener los siguientes datos: Cantidad: 1; Unidad: ACT; Descripción: Pago; Clave Prod. Serv. 84111506 Servicios de facturación. Precio unitario 0 (cero); Importe 0 (cero).

El Supervisor (a) del contrato solicitará a **“EL PROVEEDOR”** el **“CFDI con Complemento para la Recepción de Pagos”**, quien la deberá emitir en el periodo de 10 (diez) días naturales del mes inmediato siguiente en que se recibieron los pagos.

“EL PROVEEDOR” enviará los **“CFDI con Complemento para la Recepción de Pagos”** al correo electrónico del Administrador (a) del contrato y al correo del Departamento de Contabilidad (**DC**) Idelrio@inea.gob.mx. En caso de que no se emitan el o los Recibos Electrónicos de Pagos (**REP**) hay 2 opciones:

1. En la página del **SAT** se ingresa una solicitud de conciliación con **“EL PROVEEDOR”** para determinar cuántos **REP** están pendientes y requerir la inmediata entrega de estos comprobantes.
2. Denuncia ante la autoridad fiscal.

El **DT** enviará por correo electrónico semanalmente los comprobantes de pago en formato digital (CLC) al Administrador (a) y al Supervisor (a) del contrato.



QUINTA. LUGAR, PLAZOS Y CONDICIONES DEL SERVICIO.

La prestación del servicio, se realizará conforme a los plazos, condiciones y entregables establecidos por **"EL INEA"** en el **"Anexo Único"**, el cual forma parte del presente contrato.

La prestación del servicio será en los domicilios señalados en el **"Anexo Único"** y fechas establecidas en el mismo.

En los casos que derivado de la verificación se detecten defectos o discrepancias en la prestación del servicio o incumplimiento en las especificaciones técnicas, **"EL PROVEEDOR"** contará con un plazo de 10 días naturales para la reposición o corrección, contados a partir del momento de la notificación por correo electrónico y/o escrito que realice el Supervisor (a) del contrato, sin costo adicional para **"EL INEA"**.

SEXTA. VIGENCIA.

"LAS PARTES" convienen en que la vigencia del contrato será a partir del día 12 de junio de 2024 y hasta el 31 de diciembre 2024.

La vigencia del servicio será a partir del día 12 de junio de 2024 y hasta el 31 de diciembre de 2024, conforme al **"Anexo Único"**.

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que **"EL INEA"** por razones fundadas y explícitas podrá ampliar el monto o la cantidad del servicio, de conformidad con el artículo 52 de la **"LAASSP"**, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

"EL INEA", podrá ampliar la vigencia del presente instrumento, siempre y cuando, no implique incremento del monto contratado o de la cantidad de los servicios prestado, siendo necesario que se obtenga el previo consentimiento de **"EL PROVEEDOR"**.

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"EL INEA"**, se podrá modificar el plazo del presente instrumento jurídico, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES"**.

En los supuestos previstos en los dos párrafos anteriores, no procederá la aplicación de penas convencionales por atraso.

Cualquier modificación al presente contrato deberá formalizarse por escrito, y deberá suscribirse por el servidor público de **"EL INEA"** que lo haya hecho, o quien lo sustituya o esté facultado para ello, para lo cual **"EL PROVEEDOR"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 91, último párrafo del Reglamento de la **"LAASSP"**, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.



“EL INEA” se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un proveedor comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA

A) CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 48, fracción II, 49, fracción I de la **“LAASSP”**, 85, fracción III, y 103 de su Reglamento, y 166 de la Ley de Instituciones de Seguros y de Fianzas, **“EL PROVEEDOR”** se obliga a constituir una garantía **divisible**, la cual sólo se hará efectiva en la proporción correspondiente al incumplimiento de la obligación principal, mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor de **“EL INEA”**, por un importe equivalente al **10%** del monto total del contrato, sin incluir el Impuesto al Valor Agregado (I.V.A.).

Dicha fianza deberá ser entregada a **“EL INEA”**, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del presente contrato.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **“EL PROVEEDOR”** incumpla con la entrega de la garantía en el plazo establecido, **“EL INEA”** podrá rescindir el contrato y dará vista a la Oficina de Representación en **“EL INEA”** para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **“EL PROVEEDOR”**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **“EL INEA”** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **“EL PROVEEDOR”** se obliga a entregar a **“EL INEA”**, dentro de los 10 (diez días) naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo **91** del Reglamento de la **“LAASSP”**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato, podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por **“EL PROVEEDOR”** cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a **“EL INEA”** a más tardar dentro de los primeros 10 (diez) días naturales del ejercicio fiscal que corresponda.

Una vez cumplidas las obligaciones a satisfacción de la persona Administradora, o la persona servidora pública facultada por **“EL INEA”** procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía cumplimiento del contrato, lo que comunicará a **“EL PROVEEDOR”**.



NOVENA. OBLIGACIONES DE “EL PROVEEDOR”.

“EL PROVEEDOR”, se obliga a:

- a) La prestación del servicio será en las fechas, plazos y lugares establecidos conforme a lo pactado en el presente contrato y su **“Anexo Único”**.
- b) Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y su **“Anexo Único”**.
- c) Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **“EL INEA”** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.
- d) Proporcionar la información que le sea requerida por la Secretaría de la Función Pública y la Oficina de Representación en **“EL INEA”**, de conformidad con el artículo 107 del Reglamento de la **“LAASSP”**.

DÉCIMA. OBLIGACIONES DE “EL INEA”.

“EL INEA”, se obliga a:

- a) Otorgar las facilidades necesarias, a efecto de que **“EL PROVEEDOR”** lleve a cabo en los términos convenidos, la prestación del servicio objeto del contrato.
- b) Realizar el pago correspondiente en tiempo y forma.
- c) Extender a **“EL PROVEEDOR”**, por conducto del servidor público facultado, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA PRIMERA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DEL SERVICIO.

“EL INEA” designa como persona Administradora del presente contrato, a la C. María Dolores Durán Márquez, con R.F.C. DUMD6808112R5, en su carácter de Subdirectora de Recursos Tecnológicos, quien será responsable de dar seguimiento y verificar el cumplimiento de las obligaciones y especificaciones establecidas en el **“Anexo Único”**, así como determinar la aplicación y cálculo de penas convencionales y deductivas deriven del objeto del presente instrumento jurídico.

Por otro lado, se nombra como persona Supervisora del presente contrato, al C. Roberto Ramírez Guzmán, con R.F.C. RAGR740522162, en su carácter de Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones, quien será responsable de que la prestación del servicio se cumpla con las especificaciones solicitadas y entrega puntal de estos, establecidos en el instrumento jurídico y su **“Anexo Único”**.

La prestación del servicio se tendrá por recibido previa revisión de la persona Administradora del presente contrato, los cuales consistirán en la verificación del cumplimiento de las especificaciones establecidas en el **“Anexo Único”**.



“EL INEA”, a través de la persona Supervisora del contrato, rechazará el servicio, que no cumplan las especificaciones establecidas en este contrato y en su “Anexo Único”, obligándose “EL PROVEEDOR” en este supuesto a realizarlo nuevamente bajo su responsabilidad y sin costo adicional para “EL INEA”, sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondientes.

“EL INEA”, a través de la persona Administradora del contrato, podrá aceptar los servicios que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en su “Anexo Único”, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición del servicio, cuando la naturaleza propia de éstos lo permita.

DÉCIMA SEGUNDA. DEDUCCIONES.

“EL INEA” aplicará deducciones al pago de los servicios no prestados oportunamente con motivo del incumplimiento parcial, por atraso o deficiente, del **5%** conforme a lo estipulado en las cláusulas del presente contrato y su “Anexo Único”. Las cantidades a deducir se aplicarán en el **CFDI** o factura electrónica que “EL PROVEEDOR” presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

De no existir pagos pendientes, se requerirá a “EL PROVEEDOR” que realice el pago de la deductiva a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de “EL INEA”. En caso de negativa se procederá a hacer efectiva la garantía de cumplimiento del contrato.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir impuestos.

La notificación y cálculo de las deducciones correspondientes la realizará la persona Supervisora del contrato, por escrito o vía correo electrónico a “EL PROVEEDOR”.

DÉCIMA TERCERA. PENAS CONVENCIONALES.

En caso que “EL PROVEEDOR” incurra en atraso en el inicio de la prestación del servicio objeto del presente contrato, conforme a lo establecido en el “Anexo Único” parte integral de este instrumento jurídico, “EL INEA” por conducto de la persona Administradora del contrato aplicará la pena convencional equivalente al **5%** del valor del costo mensual del servicio, por cada día natural de atraso sobre el monto total del contrato, sin exceder el monto de la garantía, de conformidad con este instrumento legal y su “Anexo Único”.

La persona Administradora del contrato, notificará a “EL PROVEEDOR” por escrito o vía correo electrónico, el cálculo de la pena convencional del atraso en el cumplimiento de la obligación de que se trate.

El pago de prestación del servicio quedará condicionado, proporcionalmente, al pago que “EL PROVEEDOR” deba efectuar por concepto de penas convencionales por atraso; en el supuesto que el contrato sea rescindido en términos de lo previsto en la *Cláusula Vigésima Segunda de Rescisión*, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

El pago de la pena podrá efectuarse a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de “EL INEA”; o bien, a través de un



comprobante de egreso (CFDI de Egreso) conocido comúnmente como Nota de Crédito, en el momento en el que emita el comprobante de Ingreso (Factura o CFDI de Ingreso) por concepto del servicio, en términos de las disposiciones jurídicas aplicables.

El importe de la pena convencional, no podrá exceder el equivalente al monto total de la garantía de cumplimiento del contrato, y en el caso de no haberse requerido esta garantía, no deberá exceder del 20% (veinte por ciento) del monto total del contrato.

Cuando **“EL PROVEEDOR”** quede exceptuado de la presentación de la garantía de cumplimiento, en los supuestos previsto en la **“LAASSP”**, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del 20% (veinte por ciento) del monto del servicio prestado fuera de la fecha convenida, de conformidad con lo establecido en el tercer párrafo del artículo 96 del Reglamento de la **“LAASSP”**.

DÉCIMA CUARTA. LICENCIAS, AUTORIZACIONES Y PERMISOS

“EL PROVEEDOR” se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

DÉCIMA QUINTA. PÓLIZA DE RESPONSABILIDAD CIVIL.

Para la prestación del servicio materia del presente contrato, no se requiere que **“EL PROVEEDOR”** contrate una póliza de seguro por responsabilidad civil.

DÉCIMA SEXTA. TRANSPORTE.

“EL PROVEEDOR” se obliga bajo su costa y riesgo, a transportar los bienes e insumos necesarios para la prestación del servicio, desde su lugar de origen, hasta las instalaciones señaladas en el **“Anexo Único”** del presente contrato.

DÉCIMA SÉPTIMA. IMPUESTOS Y DERECHOS.

Los impuestos, derechos y gastos que procedan con motivo de la prestación del servicio, objeto del presente contrato, serán pagados por **“EL PROVEEDOR”**, mismos que no serán repercutidos a **“EL INEA”**.

“EL INEA” sólo cubrirá, cuando aplique, lo correspondiente al Impuesto al Valor Agregado (I.V.A.), en términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.

DÉCIMA OCTAVA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

“EL PROVEEDOR” no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de **“EL INEA”**.

DÉCIMA NOVENA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.

“EL PROVEEDOR” será responsable en caso de infringir patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, con motivo del cumplimiento de las obligaciones del presente contrato, por lo que se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a **“EL INEA”** o a terceros.



De presentarse alguna reclamación en contra de **“EL INEA”**, por cualquiera de las causas antes mencionadas, **“EL PROVEEDOR”**, se obliga a salvaguardar los derechos e intereses de **“EL INEA”** de cualquier controversia, liberándolo de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole, sacándola en paz y a salvo.

En caso de que **“EL INEA”** tuviese que erogar recursos por cualquiera de estos conceptos, **“EL PROVEEDOR”** se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

VIGÉSIMA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.

“LAS PARTES” acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratarán de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo establecido en las Leyes General y Federal respectivamente, de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, y demás legislación aplicable.

Para el tratamiento de los datos personales que **“LAS PARTES”** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **“EL PROVEEDOR”** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

Asimismo, **“EL PROVEEDOR”** deberá observar lo establecido en el **“Anexo Único”** aplicable a la Confidencialidad de la información del presente contrato.

VIGÉSIMA PRIMERA. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DEL SERVICIO.

Con fundamento en el artículo 55 Bis de la **“LAASSP”** y 102, fracción II, de su Reglamento, **“EL INEA”** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación del servicio, de manera temporal, quedando obligado a pagar a **“EL PROVEEDOR”**, aquel servicio que hubiese sido efectivamente prestados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el contrato podrá continuar produciendo todos sus efectos legales, si **“EL INEA”** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA SEGUNDA. TERMINACIÓN ANTICIPADA DEL CONTRATO.

“EL INEA” cuando concurren razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de prestar el servicio originalmente contratado y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **“EL INEA”**, o se determine la nulidad total o parcial de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría de la Función Pública, podrá



dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **“EL INEA”**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **“EL INEA”** determine dar por terminado anticipadamente el contrato, lo notificará a **“EL PROVEEDOR”** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen fundado y motivado, en el que, se precisarán las razones o causas que dieron origen a la misma y pagará a **“EL PROVEEDOR”** la parte proporcional de los servicios prestados, así como los gastos no recuperables en que haya incurrido, previa solicitud por escrito, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato, limitándose según corresponda a los conceptos establecidos en la fracción I del artículo 102 del Reglamento de la **“LAASSP”**.

VIGÉSIMA TERCERA. RESCISIÓN.

“EL INEA” podrá en cualquier momento rescindir administrativamente el presente contrato y hacer efectiva la fianza de cumplimiento, cuando **“EL PROVEEDOR”** incurra en incumplimiento de sus obligaciones contractuales, sin necesidad de acudir a los tribunales competentes en la materia, por lo que, de manera enunciativa, más no limitativa, se entenderá por incumplimiento:

- a) Contravenir los términos pactados para la prestación del servicio, establecidos en el presente contrato;
- b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
- c) Ceder los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **“EL INEA”**;
- d) Suspender total o parcialmente y sin causa justificada la prestación del servicio objeto del presente contrato;
- e) No realizar la prestación del servicio en tiempo y forma conforme a lo establecido en el presente contrato y su **“Anexo Único”**;
- f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen;
- g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio;
- h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;
- i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
- j) En caso de que la suma de las penas convencionales o las deducciones al pago, iguallen el monto total de la garantía de cumplimiento del contrato y/o alcanzan el 20% (veinte



por ciento) del monto total de este contrato cuando no se haya requerido la garantía de cumplimiento;

- k) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **“EL INEA”** en los términos de lo dispuesto en la *Cláusula Vigésima de Confidencialidad y Protección de Datos Personales* del presente instrumento jurídico;
- l) Impedir el desempeño normal de labores de **“EL INEA”**;
- m) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de **“EL INEA”**, cuando sea extranjero, e
- n) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.

Para el caso de optar por la rescisión del contrato, **“EL INEA”** comunicará por escrito a **“EL PROVEEDOR”** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir del día siguiente de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término **“EL INEA”**, en un plazo de 15 (quince) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho valer **“EL PROVEEDOR”**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **“EL PROVEEDOR”** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **“EL INEA”** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **“EL PROVEEDOR”**.

Iniciado un procedimiento de conciliación **“EL INEA”** podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se brinda los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de **“EL INEA”** de que continúa vigente la necesidad del servicio, aplicando, en su caso, las penas convencionales correspondientes.

“EL INEA” podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, **“EL INEA”** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, **“EL INEA”** establecerá con **“EL PROVEEDOR”**, otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre



deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 52 de la **“LAASSP”**.

No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **“EL INEA”** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **“EL PROVEEDOR”** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 51, párrafo cuarto de la **“LAASSP”**.

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **“EL INEA”**.

VIGÉSIMA CUARTA. RELACIÓN Y EXCLUSIÓN LABORAL.

“EL PROVEEDOR” reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en la prestación del servicio, por lo que, deslinda de toda responsabilidad a **“EL INEA”** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

“EL PROVEEDOR” asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **“EL INEA”**, así como en la ejecución de la prestación del servicio objeto del presente contrato.

Para cualquier caso no previsto, **“EL PROVEEDOR”** exime expresamente a **“EL INEA”** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **“EL INEA”** reciba una demanda laboral por parte de trabajadores de **“EL PROVEEDOR”**, en la que se demande la solidaridad y/o sustitución patronal a **“EL INEA”**, **EL PROVEEDOR”** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA QUINTA. DISCREPANCIAS.

“LAS PARTES” convienen que, en caso de discrepancia entre la convocatoria de la invitación cuando menos tres personas, nacional electrónica y el contrato, prevalecerá lo establecido en la convocatoria, de conformidad con el artículo 81, fracción IV del Reglamento de la **“LAASSP”**.

VIGÉSIMA SEXTA. CONCILIACIÓN.

“LAS PARTES” acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 77, 78 y 79 de la **“LAASSP”**, 126 al 136 de su Reglamento.



VIGÉSIMA SÉPTIMA. DOMICILIOS.

“LAS PARTES” señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal.

VIGÉSIMA OCTAVA. LEGISLACIÓN APLICABLE.

“LAS PARTES” se obligan a sujetarse estrictamente para la prestación del servicio objeto del presente contrato a todas y cada una de las cláusulas que lo integran, su “Anexo Único” que forman parte integral del mismo, a la “LAASSP” y su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Federal de Procedimientos Civiles; Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

VIGÉSIMA NOVENA. JURISDICCIÓN.

“LAS PARTES” convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con sede en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

Por lo anterior expuesto, “LAS PARTES”, manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman electrónicamente dentro de los 15 días establecidos en la “LAASSP”.

**POR:
“EL INEA”**

NOMBRE	CARGO	R.F.C
MARÍA ISABEL MONTOYA OBREGÓN	APODERADA LEGAL Y TITULAR DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS	MOOI570119MR9
MARÍA DOLORES DURÁN MÁRQUEZ	ADMINISTRADORA DEL CONTRATO Y SUBDIRECTORA DE RECURSOS TECNOLÓGICOS	DUMD6808112R5
ROBERTO RAMÍREZ GUZMÁN	SUPERVISOR DEL CONTRATO Y JEFE DE DEPARTAMENTO DE SOPORTE TÉCNICO, CENTRO DE DATOS Y COMUNICACIONES	RAGR740522162

**POR:
“EL PROVEEDOR”**

NOMBRE	R.F.C.
EXECUDATA, S.A. DE C.V.	EXE0912089N5





**FORMATO A-2
FORMATO DE PROPOSICIÓN ECONÓMICA**

Ciudad de México, a 27 de mayo de 2024

Nombre del Proveedor: EXECUDATA, S.A. DE C.V.
Domicilio fiscal: RODRIGO CIFUENTES 34 INT 5, COL. SAN JOSÉ INSURGENTES, 03900 BENITO JUÁREZ, CDMX – MEXICO
R.F.C.: EXE0912089N5 Teléfono: 55.5211.5779

Partida	Descripción	Costo mensual	Costo total (junio a diciembre 2024)
1	Servicio Integral de Ciberseguridad	\$444,767.58	\$3,113,373.06
	Servicio EDR	\$296,511.30	\$2,075,579.10
		SUBTOTAL	\$5,188,952.16
		I.V.A.	\$830,232.35
		TOTAL	\$6,019,184.51
IMPORTE CON LETRA: SEIS MILLONES DIECINUEVE MIL CIENTO OCHENTA Y CUATRO PESOS 51/100 M.N., I.V.A. incluido			

Firma:
Nombre: FRANCISCO VALENTE RAMOS O'REILLY
Cargo: ADMINISTRADOR ÚNICO

NOTAS:

1. Se deberá cotizar la totalidad de los conceptos, no importando que la cantidad inicial de servicios por concepto este en cero servicios.
2. En la columna de "costo unitario" deberá anotar el precio unitario con números en moneda nacional y con dos decimales sin incluir el I.V.A.
3. En la columna de "costo total" deberá anotar el importe total, de cada servicio solicitado con números en moneda nacional y con dos decimales sin incluir el I.V.A.
4. En el campo de subtotal, se deberá anotar con números en moneda nacional con dos decimales
5. En el campo del I.V.A. anotar con números en moneda nacional con dos decimales
6. En el campo de total, deberá anotar el importe que resulte de sumar subtotal y con el I.V.A.
7. Deberá anotar el importe total con letra.

Atentamente

**FRANCISCO VALENTE RAMOS O'REILLY
ADMINISTRADOR ÚNICO**

INEA Invitación a tres personas IA-11-MDA-011MDA001-N-60-2024

Página 1 de 1

**EXECUDATA SA DE CV, TEL 5552115779 DIR. RODRIGO CIFUENTES 34 INT 5,
COL. SAN JOSÉ INSURGENTES, 03900 BJ CDMX - MEXICO**



ANEXO 1
Especificaciones Técnicas

UNIDAD DE ADMINISTRACIÓN Y FINANZAS SUBDIRECCIÓN DE RECURSOS TECNOLÓGICOS			
SERVICIO INTEGRAL DE CIBERSEGURIDAD			
ÁREA REQUERENTE	Subdirección de Recursos Tecnológicos		
NOMBRE DEL TITULAR DEL ÁREA REQUERENTE Y RESPONSABLE DE ADMINISTRAR Y SUPERVISAR EL CUMPLIMIENTO DEL CONTRATO	Titular del Área Requiriente y Administrador del Contrato o Pedido. María Dolores Durán Márquez Subdirectora de Recursos Tecnológicos Supervisor del Contrato o Pedido Roberto Ramírez Guzmán Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones		
% PENALIZACIÓN	EXECUDATA, S.A. DE C.V. se obliga a pagar al INEA una pena convencional por no presentar los entregables iniciales y/o los mensuales en los plazos establecidos en el apartado “ ENTREGABLES ” del presente anexo. Dicha pena será del 5% del valor del costo mensual del servicio, por cada día natural de atraso. El total de la pena convencional no podrá exceder el límite de la garantía de cumplimiento sin considerar el impuesto del valor agregado (I.V.A), de conformidad con lo establecido en el artículo 53 de la LAASSP.	% DE DEDUCCIÓN	Se aplicará una deductiva a EXECUDATA, S.A. DE C.V. por el cumplimiento parcial o deficiente en la prestación del servicio. Dicha deductiva corresponderá del 5 % sobre el monto de la facturación del mes inmediato anterior correspondiente al no cumplir con los niveles de servicio establecidos en el apartado “ MECANISMOS DE COMPROBACIÓN, SUPERVISIÓN Y VERIFICACIÓN DE LO ESTABLECIDO EN PEDIDOS Y/O CONTRATOS ” del presente anexo. Lo anterior, de conformidad en lo establecido en el artículo 53 bis de la LAASSP. Igual porcentaje, se aplicará como deductiva en los casos que el Proveedor suspenda el servicio por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado en términos de la normatividad aplicable, por cada día natural que suspenda el servicio.
TIPO DE GARANTÍA	DIVISIBLE <input checked="" type="checkbox"/>	INDIVISIBLE	
OTRAS GARANTÍAS QUE SE DEBERÁN DE CONSIDERAR, INDICAR EL O LOS TIPOS DE GARANTÍA O DE RESPONSABILIDAD CIVIL SEÑALANDO VIGENCIA	No aplica	PARTIDA PRESUPUESTAL	33901



PERIODO DE GARANTÍA DEL SERVICIO	No aplica	PLAZO PARA LA NOTIFICACIÓN REPOSICIÓN DEL BIEN	10 días naturales
REQUIERE PRUEBAS	No	REQUIERE MUESTRA	No
MÉTODO PARA EJECUTAR LA PRUEBA Y RESULTADO MÍNIMO	No aplica		
PRESENTACIÓN Y CONDICIONES DE LA MUESTRA.	No aplica		
REQUIERE ANTICIPO	No	PORCENTAJE DE ANTICIPO: No aplica	
ORIGEN DE LOS BIENES	No aplica		
NORMAS QUE APLICAN	ISO/IEC 27035-1 ISO/IEC 27035-2		
MÉTODO DE EVALUACIÓN (sólo aplica en Licitación o Invitación)	PUNTOS Y PORCENTAJES	COSTO BENEFICIO	BINARIO X
MODALIDAD DE CONTRATO	ABIERTO <input type="checkbox"/>	CERRADO	<input checked="" type="checkbox"/>
ES UNA CONTRATACIÓN PLURIANUAL	SI <input type="checkbox"/>	NO	<input checked="" type="checkbox"/>
VIGENCIA DEL PEDIDO Y/O CONTRATO.	Vigencia del Contrato: Del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre 2024. Vigencia del servicio: Del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre 2024.		
LUGAR Y CONDICIONES DE LA ENTREGA DE LOS SERVICIOS.	EXECUDATA, S.A. DE C.V. entregará el servicio en los siguientes domicilios: Oficinas Centrales y Unidad de Operación Ciudad de México: Calle Francisco Márquez 160, Col. Condesa, Alcaldía Cuauhtémoc, C.P. 06140, Ciudad de México. En los siguientes lugares la atención del servicio podrá ser de forma remota: Unidad de Operación Baja California: Av. Reforma Esq. México #599, Zona Centro, C.P. 21000, Mexicali, Baja California. Unidad de Operación Estado de México: Calle Lago Atabasca 103, Colonia Nueva Oxtotitlán, C.P. 50100, Toluca de Lerdo, Estado de México Unidad de Operación Michoacán de Ocampo: Av. Francisco I. Madero Pte. # 6000, Colonia Sindurio C.P. 58337, Morelia, Michoacán de Ocampo. Unidad de Operación Nuevo León: Calle Platón Sánchez 202, Nte, Colonia Centro C.P. 64000 Monterrey, Nuevo León. Unidad de Operación Querétaro: Av. Luis Vega y Monroy s/n, Colonia Centro Sur, C.P. 76090, Querétaro, Querétaro.		
MECANISMOS DE COMPROBACIÓN, SUPERVISIÓN Y VERIFICACIÓN DE LO ESTABLECIDO	El servicio solicitado requiere de una adecuada determinación y cumplimiento de los niveles de servicio y de la información requerida en los entregables iniciales y periódicos que nos permitirá la supervisión y revisión de los servicios proporcionados, además de: <ul style="list-style-type: none"> • Dotar al servicio de la información necesaria para que pueda realizar un seguimiento detallado y para 		

<p>EN CONTRATOS</p>	<p>poder evaluar el rendimiento.</p> <ul style="list-style-type: none"> • Optimizar la calidad del servicio ofertado. • Gestionar el conocimiento según los informes entregados y que permitan al INEA, tomar decisiones mejor informadas. • Entregar el procedimiento de recepción de reportes y atención de fallas, dentro de los 5 días hábiles posteriores a la fecha de adjudicación del contrato • Por ello, EXECUDATA, S.A. DE C.V. de resultar adjudicado, cubrirá los siguientes niveles de servicio, indicadores de desempeño y paquete de reportes que se describen a continuación: <table border="1" data-bbox="431 474 1414 1738"> <tr> <td data-bbox="431 474 792 699"> <p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p> </td> <td data-bbox="800 474 1414 699"> <ul style="list-style-type: none"> • Disponibilidad mensual de la solución de Correlación de eventos: 99.5 %. • Tiempo de identificación, notificación comportamientos anómalos, cambios, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> *Prioridad Crítica 20 Minutos *Prioridad Alta: 40 Minutos *Prioridad Media: 60 Minutos *Prioridad Baja: 120 Minutos </td> </tr> <tr> <td data-bbox="431 699 792 1094"> <p>S2.- Equipo de respuesta ante incidentes de seguridad computacional.</p> </td> <td data-bbox="800 699 1414 1094"> <ul style="list-style-type: none"> • Tiempo de reacción del equipo de respuesta a incidentes (pudiendo ser de manera remota): <ul style="list-style-type: none"> * Prioridad Crítica 20 Minutos * Prioridad Alta 40 Minutos * Prioridad Media 60 Minutos * Prioridad Baja 120 Minutos • Tiempo de solución de acuerdo con los tiempos determinados en el plan de trabajo de remediación correspondientes, autorizado por el INEA. • Tiempo de investigación e identificación de causa raíz de incidentes, comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 8 Horas continuas * Prioridad Alta 12 Horas continuas * Prioridad Media 24 Horas continuas * Prioridad Baja 48 Horas continuas </td> </tr> <tr> <td data-bbox="431 1094 792 1591"> <p>S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR -Endpoint Detection and Response).</p> </td> <td data-bbox="800 1094 1414 1591"> <ul style="list-style-type: none"> • Disponibilidad mensual de la solución de EndPoint Detection and Response: 99.5%. • Tiempo de identificación, notificación comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 30 Minutos * Prioridad Alta 60 Minutos * Prioridad Media 120 Minutos * Prioridad Baja 180 Minutos • Tiempo de solución <ul style="list-style-type: none"> * Prioridad Crítica 4 Horas * Prioridad Alta 1 día natural * Prioridad Media 2 días naturales * Prioridad Baja 4 días naturales • Tiempo de investigación e identificación de causa raíz de incidentes, comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 8 Horas continuas * Prioridad Alta 12 Horas continuas * Prioridad Media 24 Horas continuas * Prioridad Baja 48 Horas continuas </td> </tr> <tr> <td data-bbox="431 1591 792 1738"> <p>S4. Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.</p> </td> <td data-bbox="800 1591 1414 1738"> <ul style="list-style-type: none"> • Disponibilidad mensual del servicio de ciberpatrullaje: 99.5%. • Disponibilidad mensual del servicio de ciberinteligencia: 99.5%. • Análisis de vulnerabilidades, pruebas de penetración verificación, de suficiencia de controles de seguridad e Ingeniería social de acuerdo a los tiempos comprometidos en los planes de trabajo autorizados por el INEA. </td> </tr> </table> <p data-bbox="431 1745 1414 1793">Nota: El responsable de catalogar la prioridad del evento es el personal designado por el INEA, en casos reactivos, en caso de una notificación proactiva no aplica tiempo de notificación.</p> <p data-bbox="431 1814 1414 1854">EXECUDATA, S.A. DE C.V. tiene conocimiento respecto a que todos los tickets tendrán asignada una prioridad entre el ingeniero de soporte técnico EXECUDATA, S.A. DE C.V. y el contacto autorizado por el INEA, de</p>	<p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p>	<ul style="list-style-type: none"> • Disponibilidad mensual de la solución de Correlación de eventos: 99.5 %. • Tiempo de identificación, notificación comportamientos anómalos, cambios, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> *Prioridad Crítica 20 Minutos *Prioridad Alta: 40 Minutos *Prioridad Media: 60 Minutos *Prioridad Baja: 120 Minutos 	<p>S2.- Equipo de respuesta ante incidentes de seguridad computacional.</p>	<ul style="list-style-type: none"> • Tiempo de reacción del equipo de respuesta a incidentes (pudiendo ser de manera remota): <ul style="list-style-type: none"> * Prioridad Crítica 20 Minutos * Prioridad Alta 40 Minutos * Prioridad Media 60 Minutos * Prioridad Baja 120 Minutos • Tiempo de solución de acuerdo con los tiempos determinados en el plan de trabajo de remediación correspondientes, autorizado por el INEA. • Tiempo de investigación e identificación de causa raíz de incidentes, comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 8 Horas continuas * Prioridad Alta 12 Horas continuas * Prioridad Media 24 Horas continuas * Prioridad Baja 48 Horas continuas 	<p>S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR -Endpoint Detection and Response).</p>	<ul style="list-style-type: none"> • Disponibilidad mensual de la solución de EndPoint Detection and Response: 99.5%. • Tiempo de identificación, notificación comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 30 Minutos * Prioridad Alta 60 Minutos * Prioridad Media 120 Minutos * Prioridad Baja 180 Minutos • Tiempo de solución <ul style="list-style-type: none"> * Prioridad Crítica 4 Horas * Prioridad Alta 1 día natural * Prioridad Media 2 días naturales * Prioridad Baja 4 días naturales • Tiempo de investigación e identificación de causa raíz de incidentes, comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 8 Horas continuas * Prioridad Alta 12 Horas continuas * Prioridad Media 24 Horas continuas * Prioridad Baja 48 Horas continuas 	<p>S4. Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.</p>	<ul style="list-style-type: none"> • Disponibilidad mensual del servicio de ciberpatrullaje: 99.5%. • Disponibilidad mensual del servicio de ciberinteligencia: 99.5%. • Análisis de vulnerabilidades, pruebas de penetración verificación, de suficiencia de controles de seguridad e Ingeniería social de acuerdo a los tiempos comprometidos en los planes de trabajo autorizados por el INEA.
<p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p>	<ul style="list-style-type: none"> • Disponibilidad mensual de la solución de Correlación de eventos: 99.5 %. • Tiempo de identificación, notificación comportamientos anómalos, cambios, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> *Prioridad Crítica 20 Minutos *Prioridad Alta: 40 Minutos *Prioridad Media: 60 Minutos *Prioridad Baja: 120 Minutos 								
<p>S2.- Equipo de respuesta ante incidentes de seguridad computacional.</p>	<ul style="list-style-type: none"> • Tiempo de reacción del equipo de respuesta a incidentes (pudiendo ser de manera remota): <ul style="list-style-type: none"> * Prioridad Crítica 20 Minutos * Prioridad Alta 40 Minutos * Prioridad Media 60 Minutos * Prioridad Baja 120 Minutos • Tiempo de solución de acuerdo con los tiempos determinados en el plan de trabajo de remediación correspondientes, autorizado por el INEA. • Tiempo de investigación e identificación de causa raíz de incidentes, comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 8 Horas continuas * Prioridad Alta 12 Horas continuas * Prioridad Media 24 Horas continuas * Prioridad Baja 48 Horas continuas 								
<p>S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR -Endpoint Detection and Response).</p>	<ul style="list-style-type: none"> • Disponibilidad mensual de la solución de EndPoint Detection and Response: 99.5%. • Tiempo de identificación, notificación comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 30 Minutos * Prioridad Alta 60 Minutos * Prioridad Media 120 Minutos * Prioridad Baja 180 Minutos • Tiempo de solución <ul style="list-style-type: none"> * Prioridad Crítica 4 Horas * Prioridad Alta 1 día natural * Prioridad Media 2 días naturales * Prioridad Baja 4 días naturales • Tiempo de investigación e identificación de causa raíz de incidentes, comportamientos anómalos, boletines o notificaciones de seguridad: <ul style="list-style-type: none"> * Prioridad Crítica 8 Horas continuas * Prioridad Alta 12 Horas continuas * Prioridad Media 24 Horas continuas * Prioridad Baja 48 Horas continuas 								
<p>S4. Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.</p>	<ul style="list-style-type: none"> • Disponibilidad mensual del servicio de ciberpatrullaje: 99.5%. • Disponibilidad mensual del servicio de ciberinteligencia: 99.5%. • Análisis de vulnerabilidades, pruebas de penetración verificación, de suficiencia de controles de seguridad e Ingeniería social de acuerdo a los tiempos comprometidos en los planes de trabajo autorizados por el INEA. 								

	<p>acuerdo con los siguientes criterios:</p> <p>Los criterios para determinar la Propiedad sobre el factor de riesgo, están basados en CVSS (Common Vulnerability Score System).</p> <table border="1" data-bbox="431 369 1386 779"> <thead> <tr> <th colspan="2" rowspan="2">Prioridad = Impacto X Urgencia</th> <th colspan="4">Impacto</th> </tr> <tr> <th>Crítica</th> <th>Alta</th> <th>Media</th> <th>Baja</th> </tr> </thead> <tbody> <tr> <td rowspan="4">Urgencia</td> <td>Crítica 9.0-10.0</td> <td>9-0-10.0</td> <td>7.0-8.9</td> <td>4.0-6.9</td> <td>0.1-3.9</td> </tr> <tr> <td>Alta 7.0-8.9</td> <td>7.0-8.9</td> <td>7.0-8.9</td> <td>4.0-6.9</td> <td>0.1-3.9</td> </tr> <tr> <td>Media 4.0-6.9</td> <td>4.0-6.9</td> <td>4.0-6.9</td> <td>4.0-6.9</td> <td>0.1-3.9</td> </tr> <tr> <td>Baja 0.1-3.9</td> <td>0.1-3.9</td> <td>0.1-3.9</td> <td>0.1-3.9</td> <td>0.1-3.9</td> </tr> </tbody> </table>	Prioridad = Impacto X Urgencia		Impacto				Crítica	Alta	Media	Baja	Urgencia	Crítica 9.0-10.0	9-0-10.0	7.0-8.9	4.0-6.9	0.1-3.9	Alta 7.0-8.9	7.0-8.9	7.0-8.9	4.0-6.9	0.1-3.9	Media 4.0-6.9	4.0-6.9	4.0-6.9	4.0-6.9	0.1-3.9	Baja 0.1-3.9	0.1-3.9	0.1-3.9	0.1-3.9	0.1-3.9
Prioridad = Impacto X Urgencia				Impacto																												
		Crítica	Alta	Media	Baja																											
Urgencia	Crítica 9.0-10.0	9-0-10.0	7.0-8.9	4.0-6.9	0.1-3.9																											
	Alta 7.0-8.9	7.0-8.9	7.0-8.9	4.0-6.9	0.1-3.9																											
	Media 4.0-6.9	4.0-6.9	4.0-6.9	4.0-6.9	0.1-3.9																											
	Baja 0.1-3.9	0.1-3.9	0.1-3.9	0.1-3.9	0.1-3.9																											
<p>ENTREGABLES</p>	<p>EXECUDATA, S.A. DE C.V., enlista el resumen de los reportes y entregables que serán considerados y documentados para cada uno de los servicios:</p> <p>Entregables iniciales:</p> <table border="1" data-bbox="431 951 1421 1869"> <tr> <td data-bbox="431 951 769 1869"> <p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p> </td> <td data-bbox="769 951 1421 1869"> <ul style="list-style-type: none"> Documento de Diseño y definición de la Arquitectura de la solución, cuarenta y cinco (15) días naturales posteriores al fallo. Organigrama del personal que va a cubrir el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. Relación de hardware, software y licenciamiento para el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. Plan de trabajo para la implementación, configuración y puesta en operación de la solución de monitoreo en un periodo no mayor a cinco (5) días naturales posteriores al fallo. Memoria Técnica, diagramas de topología y esquemas de las soluciones (10 días hábiles al terminar la implementación y cuando la infraestructura sea modificada). Carta bajo protesta de decir verdad firmado por el representante legal de que cualquier componente tecnológico, hardware y software de operación empleado para la entrega de servicio será actualizado durante toda la vigencia del contrato, entrega inmediata para firma del contrato. Carta bajo protesta de decir verdad firmada por el representante legal que en caso de que el servicio sea auditado por cualquier entidad fiscalizadora, deberá proporcionar la información de soporte necesaria (procedimientos, información de licenciamiento, estadísticas o cualquier otro documento que sea evidencia del servicio), incluyendo la visita a las instalaciones de así ser requerido, por parte del INEA o los órganos fiscalizadores en su nombre, entrega inmediata para firma del contrato. Carta de liberación del servicio (Una vez realizada la implementación y puesta en marcha). Respaldo de Configuraciones (Una vez realizada la Implementación y puesta en marcha). Reporte de planeación de Capacidades: Detalle de las tecnologías dentro del alcance del servicio, tendencias, hallazgos y recomendaciones. Firma de aceptación y apego a Políticas de seguridad internas del servicio de ciberseguridad (Una vez realizada la </td> </tr> </table>	<p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p>	<ul style="list-style-type: none"> Documento de Diseño y definición de la Arquitectura de la solución, cuarenta y cinco (15) días naturales posteriores al fallo. Organigrama del personal que va a cubrir el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. Relación de hardware, software y licenciamiento para el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. Plan de trabajo para la implementación, configuración y puesta en operación de la solución de monitoreo en un periodo no mayor a cinco (5) días naturales posteriores al fallo. Memoria Técnica, diagramas de topología y esquemas de las soluciones (10 días hábiles al terminar la implementación y cuando la infraestructura sea modificada). Carta bajo protesta de decir verdad firmado por el representante legal de que cualquier componente tecnológico, hardware y software de operación empleado para la entrega de servicio será actualizado durante toda la vigencia del contrato, entrega inmediata para firma del contrato. Carta bajo protesta de decir verdad firmada por el representante legal que en caso de que el servicio sea auditado por cualquier entidad fiscalizadora, deberá proporcionar la información de soporte necesaria (procedimientos, información de licenciamiento, estadísticas o cualquier otro documento que sea evidencia del servicio), incluyendo la visita a las instalaciones de así ser requerido, por parte del INEA o los órganos fiscalizadores en su nombre, entrega inmediata para firma del contrato. Carta de liberación del servicio (Una vez realizada la implementación y puesta en marcha). Respaldo de Configuraciones (Una vez realizada la Implementación y puesta en marcha). Reporte de planeación de Capacidades: Detalle de las tecnologías dentro del alcance del servicio, tendencias, hallazgos y recomendaciones. Firma de aceptación y apego a Políticas de seguridad internas del servicio de ciberseguridad (Una vez realizada la 																													
<p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p>	<ul style="list-style-type: none"> Documento de Diseño y definición de la Arquitectura de la solución, cuarenta y cinco (15) días naturales posteriores al fallo. Organigrama del personal que va a cubrir el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. Relación de hardware, software y licenciamiento para el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. Plan de trabajo para la implementación, configuración y puesta en operación de la solución de monitoreo en un periodo no mayor a cinco (5) días naturales posteriores al fallo. Memoria Técnica, diagramas de topología y esquemas de las soluciones (10 días hábiles al terminar la implementación y cuando la infraestructura sea modificada). Carta bajo protesta de decir verdad firmado por el representante legal de que cualquier componente tecnológico, hardware y software de operación empleado para la entrega de servicio será actualizado durante toda la vigencia del contrato, entrega inmediata para firma del contrato. Carta bajo protesta de decir verdad firmada por el representante legal que en caso de que el servicio sea auditado por cualquier entidad fiscalizadora, deberá proporcionar la información de soporte necesaria (procedimientos, información de licenciamiento, estadísticas o cualquier otro documento que sea evidencia del servicio), incluyendo la visita a las instalaciones de así ser requerido, por parte del INEA o los órganos fiscalizadores en su nombre, entrega inmediata para firma del contrato. Carta de liberación del servicio (Una vez realizada la implementación y puesta en marcha). Respaldo de Configuraciones (Una vez realizada la Implementación y puesta en marcha). Reporte de planeación de Capacidades: Detalle de las tecnologías dentro del alcance del servicio, tendencias, hallazgos y recomendaciones. Firma de aceptación y apego a Políticas de seguridad internas del servicio de ciberseguridad (Una vez realizada la 																															

	<p>S2. Equipo de respuesta ante incidentes de seguridad computacional.</p>	<p>Implementación y puesta en marcha).</p> <ul style="list-style-type: none"> • Proceso que considere las siguientes actividades: Detección, Clasificación, Atención y Contención, Investigación, Análisis, Diagnóstico, Solución y Erradicación, Recuperación y Mejora, cuarenta y cinco (15) días naturales posteriores al fallo. • Organigrama del personal que va a cubrir el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. • Proceso definido para la categorización y análisis de riesgo sobre los incidentes, así como establecer canales de comunicación con el personal técnico que designe el servicio, tales como correo electrónico, teléfono, chat, etc, cuarenta y cinco (15) días naturales posteriores al fallo. • Definición y autorización de los Niveles de escalamiento, cinco (5) días naturales posteriores al fallo. • Carta de liberación del servicio (Una vez realizada la implementación y puesta en marcha). • Respaldo de Configuraciones (Una vez realizada la implementación y puesta en marcha). • Reporte de Planeación de Capacidades: Detalle de las tecnologías dentro del alcance del servicio, tendencias, hallazgos y recomendaciones (cuarenta y cinco (15) días naturales posteriores al fallo). • Firma de aceptación y apego a Políticas de seguridad internas del servicio de ciberseguridad (Una vez realizada la Implementación y puesta en marcha).
	<p>S3. Servicio administrado de una solución de seguridad para equipos de cómputo (EDR - EndPoint Detection and Response).</p>	<ul style="list-style-type: none"> • Documento de Diseño y definición de la Arquitectura de la solución, mencionando la compatibilidad y convivencia con el antivirus contratado por el INEA, cuarenta y cinco (15) días naturales posteriores al fallo. • Organigrama del personal que va a cubrir el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. • Plan de trabajo para implementar, configurar, monitorear y administrar la solución centralizada de seguridad para equipos de cómputo, cinco (5) días naturales posteriores al fallo. • Relación de hardware y software para el servicio. Detalle de los procedimientos y metodologías a aplicar en el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. • Memoria técnica de la configuración de servicio. Cuentas de acceso a la solución tecnológica • Carta de liberación del servicio (Una vez realizada la implementación y puesta en marcha). • Respaldo de Configuraciones (Una vez realizada la implementación y puesta en marcha). • Reporte de Planeación de Capacidades: Detalle de las tecnologías dentro del alcance del servicio, tendencias, hallazgos y recomendaciones (cuarenta y cinco (15) días naturales posteriores al fallo). • Firma de aceptación y apego a Políticas de seguridad internas del servicio de ciberseguridad (Una vez realizada la Implementación y puesta en marcha).
	<p>S4. Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.</p>	<ul style="list-style-type: none"> • Procesos y metodologías para atender el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. • Organigrama del personal que va a cubrir el servicio, cuarenta y cinco (15) días naturales posteriores al fallo. • Carta de liberación del servicio (Una vez realizada la implementación y puesta en marcha). • Respaldo de Configuraciones (Una vez realizada la implementación y puesta en marcha). • Reporte de Planeación de Capacidades: Detalle de las tecnologías dentro del alcance del servicio, tendencias, hallazgos y recomendaciones. • Firma de aceptación y apego a Políticas de seguridad internas del servicio de ciberseguridad. Metodologías de:

		<ul style="list-style-type: none"> *Pruebas de penetración, *Ciberpatrullaje, *Detección de Amenazas Sospechosas, *Análisis de Vulnerabilidades y Pruebas de Penetración • Ingeniería social. <p>(5 días después de realizada la Actividad).</p>
Entregables periódicos		
Servicio	Entregable	Periodicidad
S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.	<ul style="list-style-type: none"> • Estadístico Mensual de eventos de actividad sospechosa, detecciones identificadas, bloqueadas y/o contenidas, así como el detalle de las acciones realizadas en el servicio. • Informe ejecutivo de eventos • Informe detallado 	Mensual
S2.- Equipo de respuesta ante incidentes de seguridad computacional.	<ul style="list-style-type: none"> • Notificaciones a los contactos definidos en el servicio en caso de incidentes. 	Inmediata
	<ul style="list-style-type: none"> • Para todo incidente que sea clasificado como prioridad alta y/o crítica, deberá realizarse un análisis de causa raíz y su reporte respectivo. • Reportes de los incidentes identificados, que incluya los expedientes, trazabilidad de los eventos, documentación de la mitigación y evidencias de los hallazgos. 	Mensual
S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR - Endpoint Detection and Response).	<ul style="list-style-type: none"> • Notificaciones a los contactos definidos en el servicio en caso de un incidente. 	Inmediata
	<ul style="list-style-type: none"> • Reportes de Operación: incidentes, riesgos y problemas ocurridos en el período. • Informe del monitoreo proactivo de cualquier vulnerabilidad, notificación, alerta o bug que sea identificado en la infraestructura del INEA. 	Mensual
S4.- Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.	<ul style="list-style-type: none"> • Informe del análisis de vulnerabilidades a toda la infraestructura tecnológica del INEA. 	Trimestral
	<ul style="list-style-type: none"> • Pruebas de penetración y pentesting en ambiente productivo que considere: notificaciones de seguridad oportuna, así como notificación de vulnerabilidades. 	Bajo demanda
	<ul style="list-style-type: none"> • Análisis de vulnerabilidades de código dinámico y estático bajo demanda con 40 eventos para liberación de aplicativos a producción. 	Bajo demanda
	<ul style="list-style-type: none"> • Boletín informativo con la información analizada sobre vulnerabilidades identificadas, métodos de explotación, recomendaciones de mitigación y, en caso de que corresponda el plan de remediación propuesto. 	Mensual
	<ul style="list-style-type: none"> • Para todo incidente que sea clasificado como prioridad alta y/o crítica, deberá realizarse un análisis de causa raíz y entregar el informe respectivo. 	Mensual
	<ul style="list-style-type: none"> • Reporte técnico de los hallazgos de las pruebas de penetración. • Este reporte debe incluir todos los hallazgos reportados y detallados para cada uno de los dispositivos que conforman la muestra, así como las recomendaciones para su remediación. 	Bajo demanda

	<ul style="list-style-type: none"> El reporte debe contar con un anexo en formato Excel que muestre la matriz de vulnerabilidades por severidad, equipo, dirección IP, protocolo, puerto, plataforma afectada, nombre de la vulnerabilidad, descripción, remediación, referencias y evidencia de la vulnerabilidad como mínimo. Dicho reporte deberá ser entregado 7 días hábiles posterior a la finalización de los ejercicios. 	
	<p>Reporte ejecutivo de las pruebas de penetración. Resumen enfocado a la alta dirección sobre hallazgos y con un enfoque más de administración que facilite la toma de decisiones, identificando los vectores de ataque, se deben incorporar recomendaciones y análisis de evolución respecto a los ejercicios anteriores. Dicho reporte se debe entregar 7 días hábiles posterior a la finalización de los ejercicios.</p>	Bajo demanda
	<ul style="list-style-type: none"> Presentación ejecutiva de las pruebas de penetración. Dicha presentación se realizará 3 días hábiles posterior a la entrega de reportes o en la fecha que se determine en conjunto con el servicio de ciberseguridad, se deberá realizar una presentación ejecutiva de los hallazgos identificados. 	Bajo demanda
	<ul style="list-style-type: none"> Pruebas de Ingeniería social El reporte se definirá según el escenario a desplegar a criterio del proveedor adjudicado, siempre y cuando, se muestre el detalle de los objetivos evaluados, el método, el procedimiento, los resultados obtenidos, vectores de ataque y las recomendaciones de mitigación. 	Bajo demanda
	<ul style="list-style-type: none"> Informe del ejercicio de pruebas de penetración interna y externa 	Al término de la prueba
	<ul style="list-style-type: none"> Informe del evento de validación de remediaciones. 	Al término de la prueba
	<ul style="list-style-type: none"> Informe del ejercicio de ingeniería social 	Al término de la prueba
	<ul style="list-style-type: none"> Informe de hallazgos del servicio de ciberinteligencia como fuente de información para el proceso de Respuesta de incidentes de Seguridad. 	Mensual
	<ul style="list-style-type: none"> Reporte Mensual de Ciberpatrullaje. 	Mensual
<p>Nota: La estructura de todos los reportes anteriormente señalados se definirá en la reunión de kickoff del proyecto entre EXECUDATA, S.A. DE C.V. de resultar adjudicado y el personal técnico que designe el servicio de ciberseguridad para tal efecto.</p>		
<p>Entregables finales:</p>		
<p>S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.</p>	<ul style="list-style-type: none"> Memoria Técnica final, diagramas de topología y esquemas de las soluciones, cinco (5) días naturales posteriores a la finalización del contrato. Almacenamiento histórico local de información por el período de la vigencia del contrato, cinco (5) días naturales posteriores a la finalización. Procedimiento de borrado seguro de la herramienta y entregará evidencia y reporte de tratamiento correspondiente, cinco (5) días 	

	<p>S2.- Equipo de respuesta ante incidentes de seguridad computacional.</p> <p>S3. Servicio administrado de una solución de seguridad para equipos de cómputo (EDR - Endpoint Detection and Response).</p> <p>S4.- Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.</p>	<p>naturales posteriores a la finalización del contrato.</p> <ul style="list-style-type: none"> Respaldo de los Reportes de los incidentes identificados durante la vigencia del servicio, incluyendo los expedientes, trazabilidad de los eventos, documentación de la mitigación y evidencias de los hallazgos, dos (2) días naturales posteriores a la finalización del contrato Almacenamiento histórico local de información por el periodo de la vigencia del contrato. Procedimiento de borrado seguro de la herramienta y entregará evidencia y reporte del tratamiento correspondiente, cinco (5) días naturales posteriores a la finalización del contrato. <ul style="list-style-type: none"> Entregar la información de todos los logs y respaldos de información y evidencias al INEA y ayudar en las tareas de migración como la desinstalación de los agentes, treinta (30) días posteriores a la finalización del contrato. Almacenamiento histórico local de información por el periodo de la vigencia del contrato. Procedimiento de borrado seguro de la herramienta y entregará evidencia y reporte del tratamiento correspondiente, cinco (5) días naturales posteriores a la finalización del contrato. <ul style="list-style-type: none"> Entregar la información de todos los logs y respaldos de información y evidencias al INEA y ayudar en las tareas de migración como la desinstalación de los agentes, treinta (30) días posteriores a la finalización del contrato. Almacenamiento histórico local de información por el periodo de la vigencia del contrato. Procedimiento de borrado seguro de la herramienta y entregará evidencia y reporte del tratamiento correspondiente, cinco (5) días naturales posteriores a la finalización del contrato.
<p>FORMA Y PLAZO DE PAGO</p>	<p>El pago correspondiente se realizará en moneda nacional (pesos mexicanos) a mes vencido durante la vigencia del contrato por servicios efectivamente devengados, dentro de los 20 días naturales contados a partir de la entrega de la factura, previa validación de los entregables a entera satisfacción del Administrador del Contrato en términos del presente anexo técnico.</p> <p>Lo anterior, quedará condicionado proporcionalmente al pago que mi representada deba efectuar por concepto de penas convencionales o deducciones con motivo del incumplimiento parcial o total al mes correspondiente, en que pudiera incurrir respecto al servicio.</p> <p>Para el presente procedimiento queda especificado que el pago por el servicio comenzará a correr a partir del siguiente día hábil de que el servicio quede debidamente configurado y en operación a entera satisfacción del INEA.</p>	
<p>NOMBRE Y CARGO DEL ADMINISTRADOR Y DEL SUPERVISOR DEL INSTRUMENTO JURÍDICO</p>	<p>María Dolores Durán Márquez Subdirectora de Recursos Tecnológicos Titular del Área Requirente y Administradora del Contrato.</p> <p>Roberto Ramírez Guzmán Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones Supervisor del Contrato</p>	
<p>FORMA Y TÉRMINOS EN QUE SE REALIZARÁ LA VERIFICACIÓN DE LAS ESPECIFICACIONES Y LA ACEPTACIÓN DE LOS BIENES O SERVICIOS.</p>	<p>La aceptación del servicio se notificará mediante oficio de liberación para el pago.</p>	
<p>1. Descripción del servicio</p> <p>1. Con la finalidad de dar cumplimiento a los controles de seguridad indicados en el proceso Administración de la Seguridad de la Información (ASI) y Operación de los Controles (OPEC) del acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la administración pública federal publicado en el DOF el 06 de septiembre de 2021 y las atribuciones del</p>		



Subdirección de Recursos Tecnológicos se requiere contratar los siguientes servicios en una solución integral para el Instituto:

- S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.
- S2.- Equipo de respuesta ante incidentes de seguridad computacional.
- S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR -Endpoint Detection and Response).
- S4.- Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.

Ciberseguridad es dar seguridad en el ciberespacio. El ciber espacio está integrado por los siguientes elementos: redes interconectadas, aplicaciones interconectadas, información, personas e Internet, de acuerdo con la definición de la norma ISO/IEC 27032.

Cabe señalar que se privilegiara el uso de herramientas de software libre para brindar el servicio, siempre y cuando no comprometa la integridad del mismo y no se ponga en riesgo la información del Instituto.

Los servicios deberán ser entregados con base en la descripción detallada en la sección siguiente. Estos deberán ser realizados durante la vigencia del contrato y con estricto apego a las políticas y procedimientos de seguridad del INEA, las cuales serán dadas a conocer únicamente al licitante adjudicado.

El alcance de la Infraestructura Tecnológica del INEA, consta de:

Infraestructura tecnológica del INEA	Cantidades
Infraestructura de telecomunicaciones.	121
Servidores de Aplicaciones y base de datos	91
Sistemas de información	79
Equipos de cómputo de usuarios (escritorio y portátiles)	1000

En ninguna circunstancia la solución tecnológica de **EXECUDATA, S.A. DE C.V.** pondrá en riesgo la información o la infraestructura del INEA, por lo que mi representada monitoreará y remediará cualquier vulnerabilidad de su infraestructura de forma inmediata.

En caso de presentarse alguna vulnerabilidad se desconectará inmediatamente de la infraestructura del INEA durante el tiempo que remedie las vulnerabilidades, para evitar propagar el riesgo que esta implique, por lo que se sujetará a las deductivas y penas convencionales por no prestar el servicio durante este periodo.

En caso de que el INEA cambie o agregue algún o algunos equipos activos de su infraestructura, **EXECUDATA, S.A. DE C.V.** se compromete a actualizar los agentes para estos equipos en los sistemas correlacionadores de eventos para mantener el monitoreo y los registros correspondientes.

EXECUDATA, S.A. DE C.V. se constituye como único patrón del personal que ocupe para llevar a cabo las acciones derivadas del presente procedimiento de contratación y será el único responsable de las obligaciones laborales que en virtud de disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social, les deriven frente a dicho personal, liberando al INEA de cualquier responsabilidad laboral al respecto.

Antecedentes

En el Instituto se han tenido dos eventos de ransomware, los cuales han causado un retraso en la operación de la Subdirección de Presupuesto y Recursos Financieros, teniendo una pérdida de información en 12 equipos de cómputo con Sistema Operativo Windows X, los eventos mencionados fueron en las siguientes fechas:

El primero se presentó en julio de 2022.

El segundo se presentó en octubre de 2023.

Anexo A

En el Anexo A se describe con mayor detalle el servicio integral de ciberseguridad solicitado.



ANEXO A

Objetivo

Definir a detalle los servicios de ciberseguridad requeridos por el Instituto Nacional para la Educación de los Adultos, en adelante **INEA**, a contratar, así como el alcance detallado de los mismo, sus entregables y términos en los cuales deberán ser entregados.

Descripción del servicio

Con la finalidad de dar cumplimiento a los controles de seguridad indicados en el proceso ASI y OPEC del acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la administración pública federal publicado en el diario oficial de la federación el 06 de septiembre de 2021 y las atribuciones de la **Subdirección de Recursos Tecnológicos** se requiere contratar los siguientes servicios en una solución integral para el Instituto:

- S1.- Servicio administrado de monitoreo y correlación de eventos de seguridad.
- S2.- Equipo de respuesta ante incidentes de seguridad computacional.
- S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR - Endpoint Detection and Response).
- S4.- Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.

Ciberseguridad es dar seguridad en el ciberespacio. El ciber espacio está integrado por los siguientes elementos: redes interconectadas, aplicaciones interconectadas, información, personas e Internet, de acuerdo con la definición de la norma ISO/IEC 27032.

Cabe señalar que se privilegiara el uso de herramientas de software libre para brindar el servicio, siempre y cuando no comprometa la integridad del mismo y no se ponga en riesgo la información del Instituto.

Los servicios deberán ser entregados con base en la descripción detallada en la sección siguiente. Estos deberán ser realizados durante la vigencia del contrato y con estricto apego a las políticas y procedimientos de seguridad de INEA, las cuales serán dadas a conocer únicamente al licitante adjudicado.

El alcance de la Infraestructura Tecnológica del INEA consta de:

Infraestructura tecnológica del INEA	Cantidad
Infraestructura de telecomunicaciones.	121
Servidores de Aplicaciones y base de datos	91
Sistemas de información	79
Equipos de cómputo de usuarios (escritorio y portátiles)	1000

En ninguna circunstancia la solución tecnológica de **EXECUDATA, S.A. DE C.V.** pondrá en riesgo la información o la infraestructura del INEA, por lo que mi representada monitoreará y remediará cualquier vulnerabilidad de su infraestructura de forma inmediata.

En caso de presentarse alguna vulnerabilidad se desconectará inmediatamente de la infraestructura del INEA durante el tiempo que remedie las vulnerabilidades, para evitar propagar el riesgo que esta implique, por lo que se sujetará a las deductivas y penas convencionales por no prestar el servicio durante este periodo.



En caso de que el INEA cambie o agregue algún o algunos equipos activos de su infraestructura, **EXECUDATA, S.A. DE C.V.** se compromete a actualizar los agentes para estos equipos en los sistemas correlacionadores de eventos para mantener el monitoreo y los registros correspondientes

3. Características técnicas

EL SERVICIO INTEGRAL DE CIBERSEGURIDAD, Requiere los siguientes servicios en un esquema 24 x 7 x 365 con operación remota y en caso de ser necesario en sitio bajo demanda con un equipo de especialistas en seguridad, los cuales no serán exclusivos para proporcionar este servicio para el INEA, a través de un Centro de Operación de Seguridad (SOC) ubicado dentro del territorio nacional.

El detalle de los servicios requeridos por el INEA se describe a continuación

3.1. S1 - Servicio administrado de monitoreo y correlación de eventos de seguridad.

3.1.1. Descripción:

Para el Servicio administrado de monitoreo y correlación de eventos de seguridad **EXECUDATA, S.A. DE C.V.** diseñará, implementará, configurará, afinará y operará una solución de correlación de eventos de seguridad (SIEM).

3.1.2. Hardware y software para la prestación del servicio

EXECUDATA, S.A. DE C.V. proporcionará el hardware y software necesarios para la prestación de los servicios y mantendrá actualizados sus equipos con las últimas actualizaciones de software y/o firmware, así como las que sean aplicables para la prestación del servicio sin costo adicional para el Servicio administrado de monitoreo y correlación de eventos de seguridad.

La solución propuesta **EXECUDATA, S.A. DE C.V.** podrá estar basada en software libre.

3.1.3. Actividades a realizar como parte del servicio

EXECUDATA, S.A. DE C.V. considerará dentro de las actividades del servicio lo siguiente:

- Diseño y definición de la arquitectura de la solución.
- Implementación de la solución tecnológica, así como de todos los componentes, agentes o elementos requeridos de acuerdo con la arquitectura actual de la Infraestructura del INEA.
- Puesta a punto y "fine tuning" de la configuración de monitoreo y reglas de correlación.
- La solución propuesta será implementada de acuerdo con la arquitectura propuesta, siendo en todo momento responsabilidad de **EXECUDATA, S.A. DE C.V.** proporcionar, configurar, operar y mantener los componentes de hardware y software de la solución, incluyendo aquellos que deban instalarse en la arquitectura del INEA, tales como los agentes de monitoreo.
- Será responsabilidad **EXECUDATA, S.A. DE C.V.** recolectar la información o requerimientos necesarios para la implementación, configuración y puesta en operación de la solución de monitoreo en un periodo no mayor a cuarenta y cinco (15) días naturales posteriores al fallo, durante este periodo, **EXECUDATA, S.A. DE C.V.** realizará la definición en conjunto con la Subdirección de Recursos

INEA Invitación a tres personas IA-11-MDA-011MDA001-N-60-2024"



Tecnológicos (SRT) de los umbrales iniciales que serán configurados para las diferentes capas de servicios tecnológicos, a fin de que se pueda obtener una medición de los niveles de servicios definidos para este servicio.

- Como parte su cotización de los servicios proporcionados, **EXECUDATA, S.A. DE C.V.** considerará el costo asociado al licenciamiento (en caso de aplicar), enlaces, entre otros, manteniendo actualizada toda la arquitectura de la solución.
- **EXECUDATA, S.A. DE C.V.** considerará como parte de su alcance todos los elementos de comunicación necesarios para realizar la conexión remota desde la ubicación de su Centro de Operaciones al INEA.
- **EXECUDATA, S.A. DE C.V.** asegurará que cualquier componente tecnológico, hardware y software de operación empleado para la entrega de servicio sea actualizado durante toda la vigencia del contrato, con base en la liberación de versiones y/o parches liberados por cada fabricante.
- En caso de que el Servicio administrado de monitoreo y correlación de eventos de seguridad sea auditado por cualquier entidad fiscalizadora, **EXECUDATA, S.A. DE C.V.** proporcionará la información de soporte necesaria (procedimientos, información de licenciamiento, estadísticas o cualquier otro documento que sea evidencia del servicio), incluyendo la visita a las instalaciones de así ser requerido, por parte del INEA o de terceros en su nombre.
- **EXECUDATA, S.A. DE C.V.** contemplará un agente no intrusivo que contemple tecnología Linux, Windows y Mac, que no entorpezca la funcionalidad del servidor y degradación de los servicios en productivo.
- **EXECUDATA, S.A. DE C.V.** se apegará a las políticas en materia de seguridad de la información vigentes en el INEA.

3.1.4. Características de la solución de correlación.

Para la entrega de este servicio, **EXECUDATA, S.A. DE C.V.** proporcionará una plataforma de detección/correlación de eventos que cubra los siguientes requerimientos:

- Modelo centralizado de insumos e interpretación de información originada por los componentes de la infraestructura tecnológica del INEA.
- Filtrado y análisis de la información generada por los diferentes componentes a monitorear.
- Colectar y analizar los diferentes indicadores de compromisos, comportamiento o pistas de auditoría por medio de tecnologías de correlación de eventos, "machine learning", inteligencia artificial o análisis de comportamiento.
- Detectar, validar, priorizar y reportar eventos o incidentes de seguridad que pongan en riesgo la disponibilidad, confidencialidad e integridad de los activos de información del INEA.
- Almacenamiento histórico local de información por el periodo de la vigencia del contrato.
- Permitir el análisis de información y la elaboración de reportes durante la vigencia del contrato mediante almacenamiento remoto.
- Monitoreo y visualización en tiempo real, mediante un Panel de control centralizado con indicadores operativos acerca de los eventos y riesgos identificados, con acceso para el INEA, mediante un protocolo seguro (ejemplo servicio web HTTPS) (Con al menos 3 cuentas de acceso). La solución propuesta colectará y monitoreará información originada de los dispositivos dentro del alcance definido.
- La solución propuesta podrá implementarse en la modalidad de cloud privada o la que **EXECUDATA, S.A. DE C.V.** determine, siendo en todo momento responsabilidad de mi representada proporcionar, configurar, operar y mantener los componentes de hardware y software de la solución propuesta, incluido cualquier tipo de licenciamiento necesario.
- La solución deberá contar con una arquitectura que permita brindar el nivel de disponibilidad descrito dentro de los Niveles de Servicio.

INEA Invitación a tres personas IA-11-MDA-011MDA001-N-60-2024"



- El Licitante deberá especificar los controles de seguridad implementados que permitan garantizar la disponibilidad, integridad y confidencialidad de la información almacenada.
- **EXECUDATA, S.A. DE C.V.** garantizará que la plataforma de monitoreo sea actualizada con base en las recomendaciones del fabricante, así mismo, que se aplican las acciones de remediación con base en las vulnerabilidades identificadas.

Será responsabilidad de **EXECUDATA, S.A. DE C.V.** recolectar la información o requerimientos necesarios para implementación, configuración y puesta en operación, de la solución de monitoreo de eventos de seguridad en un periodo no mayor a cuarenta y cinco (15) días naturales a partir del fallo, durante este periodo, **EXECUDATA, S.A. DE C.V.** realizará la definición en conjunto con el INEA, las fuentes, variables y alertas de seguridad iniciales que serán configurados para las diferentes capas de servicios tecnológicos, a fin de que se pueda obtener visibilidad de los eventos de seguridad que ocurran dentro de la infraestructura del servicio con el INEA.

- **EXECUDATA, S.A. DE C.V.** asegurará que cualquier componente tecnológico, hardware y software de operación empleado para la entrega del servicio será actualizado durante la vigencia del contrato, con base en la liberación de versiones y/o parches liberados por cada fabricante.
- **EXECUDATA, S.A. DE C.V.** se apegará a las políticas en materia de seguridad de la información que el INEA, proporcione a mi representada.

3.1.1. Monitoreo y gestión de eventos de seguridad

EXECUDATA, S.A. DE C.V. proporcionará un servicio de Monitoreo de Eventos de Seguridad de TI, basado en un marco de trabajo que permita centralizar, organizar y mejorar la capacidad de detección y visibilidad de eventos de seguridad que se puedan presentar dentro de la operación del servicio y que sean considerados como una actividad sospechosa considerando lo siguiente:

- El servicio se proporcionará en un esquema de operación 7x24x 365.
- **EXECUDATA, S.A. DE C.V.** basará su operación en metodologías y procesos basados en buenas prácticas aplicables, apegado a CIS-CONTROL V.8.0, MITRE ATT&CK, OWASP, OSSTMM, ISSAFF, NIST 800-115, ISO 27001, ISO 31000, ISO 27032 e ITIL, donde se consideren: proceso de identificación de eventos, plan de comunicación y procedimientos de escalabilidad y mejora continua.
- **EXECUDATA, S.A. DE C.V.** contará con un proceso definido e implementado para la gestión de toda actividad sospechosa identificada a través de las diferentes fuentes de información correlacionadas, realizando las actividades necesarias para descartar falsos positivos e iniciar actividades de atención de Incidentes de Seguridad cuando en conjunto con los contactos definidos por el servicio se determine la existencia, con base a criterios claramente definidos, un incidente de seguridad.
- El SOC realizará las actividades de notificación y escalamiento necesarias para garantizar la oportuna respuesta y atención en base a los niveles de servicio definidos.
- De forma semestral se definirá, revisará y actualizará los Indicadores de compromiso base para el servicio de monitoreo.

3.2. S2.- Equipo de respuesta ante incidentes de seguridad informática.

3.2.1. Descripción:

EXECUDATA, S.A. DE C.V. contará con un equipo de Respuesta ante Incidentes de Seguridad Informática conformado por especialistas en seguridad, los cuales no serán exclusivos para



proporcionar este servicio para el INEA, que tendrá la responsabilidad de Gestionar los Incidentes que se puedan presentar durante la operación diaria del servicio.

3.2.2 Actividades a realizar como parte del servicio

- **EXECUDATA, S.A. DE C.V.** presentará un proceso que considerará las siguientes actividades: Detección, Clasificación, Atención y Contención, investigación, Análisis, Diagnóstico, Solución y Erradicación, Recuperación y Mejora.
- Realizará las notificaciones a los contactos definidos en el servicio con base en los niveles de servicio definidos.
- Para todo incidente que sea clasificado como prioridad alta y/o crítica, realizará un análisis de causa raíz.
- Reportará los incidentes relacionados.
- Mantendrá la proactividad en la búsqueda de amenazas que pudiesen afectar la operación del servicio.
- **EXECUDATA, S.A. DE C.V.** se responsabiliza de tener una mesa de servicio, a fin de lograr la recuperación en el menor tiempo posible de cualquier afectación en la infraestructura de seguridad del servicio.
- Niveles de escalamiento con base en la prioridad asignada de acuerdo al tipo de afectación diagnosticado.
- **EXECUDATA, S.A. DE C.V.** brindará atención en sitio de ingeniería especializada en caso de que se requiera la atención de incidentes críticos o que, por el tipo de actividad desarrollada, no se puedan realizar de forma remota.
- Los tiempos de atención y solución se basarán en los Niveles de Servicio definidos, tomando como referencia la prioridad de atención del incidente.
- Como complemento de los requerimientos anteriores **EXECUDATA, S.A. DE C.V.** contará con un proceso definido para la categorización y análisis de riesgo sobre los incidentes requeridos, así como establecer canales de comunicación con el personal técnico que designe el servicio, tales como correo electrónico, teléfono, chat, etc.
- **EXECUDATA, S.A. DE C.V.** será el responsable de documentar todo el proceso de gestión de incidentes, de inicio a fin incluyendo y siendo posible la notificación a Guardia Nacional, previa autorización del INEA, contemplando la cadena de custodia de la evidencia para que, si fuera el caso, no sea desestimada por un inapropiado manejo de la evidencia.
- Definirá los SLA's con los que se estará trabajando.
- Aplicará los principios indicados en las normas ISO/IEC 27035-1 e ISO/IEC 27035-2

3.3 S3.- Servicio administrado de una solución de seguridad para equipos de cómputo (EDR - Endpoint Detection and Response).

3.3.1 Descripción:

Características de la de solución

Los detalles de la detección deberán contener en caso que aplique, al menos lo siguientes elementos:

- Conexiones de red, incluyendo direcciones IP y puertos utilizados.
- Actividades de disco, incluyendo carga, lectura, escritura, creación de ejecutables y eliminación.
- Consultas DNS realizadas



- Operaciones de registro de Windows realizadas
- Actividades, procesos y comandos ejecutados.
- **EXECUDATA, S.A. DE C.V.** realizará el monitoreo de actividades sospechosas y notificará al personal asignado por el INEA.
- La consola de administración permitirá extraer reportes de amenazas detectadas por equipos y mostrar el estado de conexión del agente con la consola.
- La solución debe ser implementada mediante un único agente por cada equipo y ser administrada desde una consola que puede estar ubicada en la nube privada de mi representada.
- Proveer protección y visibilidad a los equipos indicados por el INEA
- Proveer protección a equipos e Identificar de forma proactiva actividades de amenazas avanzadas.
- La consola de administración será accesible por los puntos finales en cualquier lugar e incluso cuando se encuentren conectados a redes públicas mediante VPN.
- La consola de administración tendrá la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, sistema operativo, unidad organizacional, versión del agente, tipo de equipo.
- La consola de administración tendrá la capacidad de contener el equipo de cómputo y ponerlo en una cuarentena de red bajo demanda
- Poseer visibilidad y gestión de los activos protegidos en tiempo real e información sobre las aplicaciones y procesos que se ejecutan en cualquier parte de su entorno para mitigar amenazas.
- El acceso a la consola de administración será seguro, es decir, mediante un canal de comunicación cifrado empleando HTTPS, mínimo mediante TLS v1.2 y entregará al menos una cuenta de auditor y una cuenta de administrador al personal designado por el INEA.
- La comunicación entre el agente y el servidor será segura.
- La solución propuesta mantendrá registros por un tiempo mínimo de 90 días a través de la consola de administración y mantener disponible toda la información fuera de línea para Eventos de Auditoría por la duración del contrato.
- El agente contará con una contraseña de protección para desinstalación.
- La solución propuesta tendrá la funcionalidad para agregar indicadores de compromiso bajo demanda.
- La consola de administración tendrá la funcionalidad de crear paneles de control personalizados.
- La solución propuesta integrará de manera transparente con la solución SIEM, también ofertadas por mi representada para el servicio S1.
- El agente de la solución propuesta será compatible a 32 y 64 bits, con:
 - Windows 7, 8, 10 y superiores
 - Windows Server 2003, 2008 y superiores
 - Linux y
 - Mac

EXECUDATA, S.A. DE C.V. administrará la solución propuesta debiendo:

- Describir la cantidad de reglas y/o funcionalidades del EDR.
- Realizar el despliegue de los agentes necesarios a todo el servicio contratado, así como lanzar el desinstalador de la solución en conjunto con personal que atienda este servicio.
- Proporcionar un servicio de monitoreo de eventos de seguridad y notificación oportuna en un esquema de operación 7x24x365.
- Basar su operación en metodologías y procesos basados en buenas prácticas, que de forma enunciativa mas no limitativa pueden ser: CIS-CONTROL V.8.0, MITRE ATT&CK, OWASP, OSSTMM, ISSAFF, NIST 800-115 , ISO 27001, ISO 31000, ISO 27032, ISO/IEC 27035-1, ISO/IEC 27035-2 e ITIL, donde se consideren: proceso de identificación de eventos, plan de comunicación y procedimientos de escalabilidad y mejora continua

INEA Invitación a tres personas IA-11-MDA-011MDA001-N-60-2024"

Página 15 de 21

**EXECUDATA SA DE CV, TEL 5552115779 DIR. RODRIGO CIFUENTES 34 INT 5,
COL. SAN JOSÉ INSURGENTES, 03900 BJ CDMX - MEXICO**



- Apegarse a las políticas en materia de seguridad de la información publicadas en el INEA.
- Contará con un proceso definido e implementado para la gestión de toda actividad sospechosa identificada a través de las diferentes fuentes de información correlacionadas, realizando las actividades necesarias para descartar falsos positivos y sus evidencias e iniciar actividades de atención de Incidentes de Seguridad cuando en conjunto con los contactos definidos por el INEA se determine la existencia, con base a criterios claramente definidos de un incidente de seguridad.
- El SOC realizará las actividades de notificación y escalamiento necesarias para garantizar la oportuna respuesta y atención en base a los niveles de servicio definidos
- Será responsable de las actualizaciones de la solución, necesarias para mantener la solución segura y vigente respecto al fabricante. Sin costo extra para la convocante.
- Dar soporte personalizado en caso de fallas en los agentes, según los niveles de servicio.
- Mantener comunicación vía telefónica, correo electrónico u otro medio previamente definido por el servicio.
- Al finalizar el contrato, entregará la información de todos los logs y respaldos de información y evidencias al INEA y ayudar en las tareas de migración como la desinstalación de los agentes.
- Al finalizar la prestación de los servicios, en el entendido que la información generada es propiedad del INEA, se realizará un procedimiento de borrado seguro de la herramienta y entregará evidencia y reporte del tratamiento correspondiente.

3.4. S4 - Servicio de ciberinteligencia, análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.

3.4.1. Descripción:

EXECUDATA, S.A. DE C.V. proporcionará un servicio de ciberinteligencia que incluye:

- Una base de conocimientos de mitigación de vulnerabilidades en código.
- Una base de conocimientos de mitigación de vulnerabilidades en infraestructura.
- análisis de vulnerabilidades semestrales a infraestructura
- pruebas de penetración y pentesting en ambiente productivo que considere: notificaciones de seguridad oportunas, así como notificación de vulnerabilidades,
- análisis de vulnerabilidades de código dinámico, estático y combinado bajo demanda de 40 eventos para liberación de aplicativos a producción, considerando una combinación como un evento y no de manera independiente.
- al menos un ejercicio anual de pruebas de penetración interna y externa,
- un evento de validación de remediaciones anual,
- un ejercicio de Ingeniería social semestral
- servicio de ciberpatrullaje durante la vigencia del contrato.

EXECUDATA, S.A. DE C.V. realizará el informe de un monitoreo proactivo de cualquier vulnerabilidad, notificación, alerta o bug que sea identificado y/o publicado por el fabricante de cada tecnología utilizada en el INEA o cualquier entidad acreditada y que sea indicio de un posible riesgo para el INEA, con el fin de generar una alerta temprana sobre esta condición para su remediación, siempre y cuando la infraestructura del INEA lo soporte.

3.4.2. Características:

- El servicio operará en un esquema de 7x24x365.
- Los análisis de vulnerabilidades serán bajo demanda y en el ambiente productivo.
- EXECUDATA, S.A. DE C.V.** contará con procesos y/o procedimientos documentados para las Notificaciones de Seguridad.
- EXECUDATA, S.A. DE C.V.** documentará las fuentes empleadas para realizar la identificación de vulnerabilidades, las cuales deberán ser medios informativos



especializados en seguridad o publicaciones de los fabricantes o centros especializados.

- La identificación de alguna vulnerabilidad será notificada a los contactos del INEA definidos en el servicio de acuerdo a los tiempos definidos en los Niveles de Servicio.

3.4.3. Servicio de red team

EXECUDATA, S.A. DE C.V. realizará:

- Análisis de vulnerabilidades semestrales,
- Pruebas de penetración y pentesting en ambiente productivo que considere: notificaciones de seguridad oportunas, así como notificación de vulnerabilidades,
- Análisis de vulnerabilidades de código dinámico, estático e interactivo bajo demanda de eventos para liberación de aplicativos a producción, considerando una combinación como un evento y no de manera independiente.
- Al menos un ejercicio de pruebas durante la vigencia del contrato de penetración interna y externa,
- Un evento de validación de remediaciones anual,
- Entrega de base de conocimientos de corrección de vulnerabilidades.
- un ejercicio de Ingeniería social durante la vigencia del contrato para un mínimo de 50 y un máximo de 100 usuarios, basados en un muestreo estratificado de acuerdo con la estructura organizacional del INEA

Lo anterior para identificar y clasificar las vulnerabilidades existentes en el ambiente operativo del servicio, con las cuales se apliquen planes de remediación que ayuden a tomar decisiones sobre las medidas correctivas o de mitigación en pro de aumentar el nivel de seguridad del INEA.

Los ejercicios de análisis de vulnerabilidades y pruebas de penetración deberán seguir los siguientes puntos:

- EXECUDATA, S.A. DE C.V. contará con procesos y/o procedimientos para la ejecución de análisis de vulnerabilidades, los cuales deben estar alineados a metodologías o buenas prácticas, que de forma enunciativa más no limitativas pueden ser: OWASP, OSSTMM, SANS, ISECOM, NIST entre otras,
- EXECUDATA, S.A. DE C.V. considerará pruebas de caja negra y gris para entornos de producción, externos e internos.
- Los ejercicios se ejecutará sólo dentro de los horarios y fechas estipulados en el plan de trabajo que se defina y apruebe en conjunto con el personal del INEA.
- Después de la ejecución de los servicios de análisis de vulnerabilidades y pruebas de penetración, se elaborará en conjunto con el INEA los planes de trabajo para la remediación de los hallazgos, y en el plan de trabajo se deberán acordar las fechas en que se realicen nuevamente los análisis de vulnerabilidades para validar que los hallazgos fueron remediados.
- Las pruebas no serán disruptivas, es decir, a través de la ejecución de pruebas de penetración no se deberá ver afectado algún servicio productivo del INEA.

En el caso de las pruebas de Ingeniería social seguirán los siguientes puntos:

- EXECUDATA, S.A. DE C.V. será responsable de determinar el escenario de ejecución y realizar la propuesta de este al personal asignado por el INEA, antes de su ejecución.
- EXECUDATA, S.A. DE C.V. considerará como mínimo pruebas de ingeniería social, tales como: Phishing, Vishing, Baiting y Acceso Físico.
- Las pruebas no serán disruptivas, es decir, a través de la ejecución de pruebas de ingeniería social no se deberá ver afectado algún servicio productivo del INEA.

Metodologías y estándares



EXECUDATA, S.A. DE C.V. proporcionará la metodología a utilizar, la cual estará basada en mejores prácticas y marcos de referencia de seguridad de la información como, CIS-CONTROL V.8.0, MITRE ATT&CK, OWASP, OSSTMM, ISSAFF, NIST 800-115, ISO 27001, ISO 31000, ISO/IEC 27032, ISO/IEC 27035, misma que deberán ser validada y aprobada por la SRT.

- Identificar los activos bajo prueba.
- Identificar la existencia de algunos controles detectivos de la actividad probada por parte del equipo AZUL.
- Definir los tiempos esperados de TTD (Tiempo de Detection) y TTR (Tiempo de Respuesta) aceptables, acordado con el representante de la Institución. En este caso, algún responsable del negocio o el CISO.
- Identificar la persona responsable de la seguridad de dichos activos.
- El responsable del equipo AZUL investigará y explicará la existencia de un conjunto de controles de seguridad que lograrán la detección y contención del evento simulado. El responsable del equipo azul comunicará los controles que se encuentren operativos y explicar los límites de efectividad de estos en relación con la misión bajo prueba. De otra forma, el equipo AZUL podrá declararse no preparado para cubrir este incidente o proponer la adecuación de los controles que hicieran falta, si fuera el caso.
- En cada misión, los elementos aleatorios que se agregaran será que no se revelara el momento exacto de la prueba ni las tácticas y procedimientos utilizados por parte del equipo ROJO, respetando los límites de la prueba.

Ciberpatrullaje

EXECUDATA, S.A. DE C.V. proporcionará un servicio de ciberpatrullaje que permita al INEA, tener visibilidad de eventos relacionados con la imagen, sitio web, reputación del servicio, perfiles críticos de la organización que se puedan encontrar en diferentes puntos de exposición y de esta manera, poder iniciar oportunamente acciones que permitan minimizar los riesgos identificados.

El servicio cubrirá las siguientes características:

- Realizarse en un esquema de 7x24x365.
 - El análisis realizado por **EXECUDATA, S.A. DE C.V.** considerará el panorama geopolítico, económico y social del entorno en el cual se encuentra el servicio Integral de ciberseguridad, para identificar comportamientos de ataques de acuerdo con el sector y ubicación.
 - **EXECUDATA, S.A. DE C.V.** contará con una metodología que permita coleccionar información de los diferentes puntos de exposición, identificar, analizar y reportar cualquier evento que constituya un ciberriesgo para el servicio de ciberseguridad, dentro de los cuales se encuentran: amenazas de ataques, fugas de información, sitios web apócrifos, campañas contra los servicios del INEA, o personal crítico, venta de información confidencial, detección de campañas de mercadotecnia fraudulenta, entre otros.
 - **EXECUDATA, S.A. DE C.V.** considerará diferentes puntos de exposición, tales como: Dark Web, Deep Web, Clear Web, redes sociales, portales web en internet, apps de dispositivos móviles, correo electrónico, entre otros.
 - Los ciberriesgos identificados serán comunicados a los contactos definidos por el INEA, con base en los niveles de servicio definidos.
 - **EXECUDATA, S.A. DE C.V.** incorporará los hallazgos del servicio de ciberinteligencia como fuente de información para el proceso de Respuesta de incidentes de Seguridad.
 - Si existen acciones de respuesta dentro de los alcances de los diferentes servicios que confirman este documento para mitigar los ciberriesgos identificados, **EXECUDATA, S.A. DE C.V.** iniciará las acciones de contención de acuerdo con los procedimientos definidos y niveles de servicio establecidos, previo acuerdo con los contactos definidos
- INEA Invitación a tres personas IA-11-MDA-011MDA001-N-60-2024"



por el INEA.

- **EXECUDATA, S.A. DE C.V.** documentará sus alcances de contención de eventos identificados, a fin de evaluar las capacidades de respuesta (ejemplo: solicitud de baja de sitios apócrifos) y los niveles de servicio asociados.

Mesa de Ayuda

EXECUDATA, S.A. DE C.V. pondrá a disposición del INEA el servicio de mesa de ayuda dentro de los 5 días hábiles posteriores a la fecha de adjudicación del contrato para que el INEA pueda reportar las fallas del servicio, para lo cual mi representada proporcionará números convencionales y celulares, además de correos electrónicos del representante designado por el Prestador de Servicios.

Medios para reportar fallas o deficiencia en la prestación del servicio

- **EXECUDATA, S.A. DE C.V.** entregará el procedimiento de recepción de reportes y atención de fallas, dentro de los 5 días hábiles posteriores a la fecha de adjudicación del contrato.
- Se proporcionará un correo electrónico y un número telefónico del centro de atención telefónica de **EXECUDATA, S.A. DE C.V.** como parte del servicio, sin costo de llamada para el usuario, como medios para reportar fallas o deficiencias del servicio.
- **EXECUDATA, S.A. DE C.V.** entregará una matriz de escalamiento que permita al INEA contactar al personal designado por el Prestador de Servicio para asegurar el cumplimiento conforme al presente documento.
- De igual manera, **EXECUDATA, S.A. DE C.V.** proporcionará un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.

Capacitación y/o transferencia de conocimientos

- **EXECUDATA, S.A. DE C.V.** incluirá la transferencia de conocimientos, para al menos tres personas, con una duración mínima de 40 horas para el INEA, para cada una de las herramientas que incorpore como parte de su solución.
- La transferencia de conocimientos incluirá la operación, administración y configuración de cada una de las herramientas que formen parte de la solución propuesta.
- La fecha en que se realizará la transferencia de conocimientos será definida entre **EXECUDATA, S.A. DE C.V.** y el INEA.

Perfil del prestador de servicios

EXECUDATA, S.A. DE C.V. cumple con los siguientes requisitos:

- Un especialista en Riesgo Cibernético
- Un especialista en Servicios de Ciberseguridad
- Un especialista en Servicios de Protección de Datos

Contar con especialistas en Ciberseguridad que desarrollen las siguientes actividades:

- Formular planes para salvaguardar archivos informáticos.
- Dar seguimiento de los informes sobre virus informáticos.
- Implementar protocolos criptográficos y herramientas de seguridad basadas en los mismos.
- Crear y desarrollar proyectos de seguridad informática y de las comunicaciones.
- Identificar posibles riesgos.
- Desarrollar técnicas de prevención.
- Análisis forense y análisis de malware.
- Hacking ético.



Para acreditar la especialización en Ciberseguridad, el personal asignado al servicio cuenta con alguna de las siguientes certificaciones:

- EC-Council Certificado Hacker Ético (CEH)
- CompTIA Security + (SY0-401)
- (ISC) 2 Certified Information Systems Security Professional (CISSP)
- eJPT (elearning Junior Penetration Tester)
- OSCP (Offensive Security Certified Professional)
- (Offensive Security Web Expert)
- ISO/IEC 27032
- ISO/IEC 27035

Para acreditar la especialización en Informática, el personal asignado al servicio tendrá alguna de las siguientes certificaciones:

- CISSP - (ISC) 2
- CISSP with concentration - (ISC) 2
- CCNA Security - Cisco.
- CCSP- (ISC) 2
- CCNP Security-Cisco.
- CIW - Certifications Partners.
- GSAE - SANS/GIAC - GIAC Security Audit Essentials.
- CCSK- CSA.
- CISA
- CISM
- CRISC
- ISO/IEC 27001 LA
- ISO/IEC 27001 LI

Confidencialidad

EXECUDATA, S.A. DE C.V. presenta en su propuesta técnica carta en papel membretado firmada por el representante legal, donde nos comprometemos a mantener absoluta confidencialidad de la información a la cual tengan acceso siendo responsable de cada uno de los integrantes del personal asignado para el desarrollo y operación del servicio, respetando el manejo correcto de la información.

Toda la información a que tenga acceso el personal que **EXECUDATA, S.A. DE C.V.** designe para el cumplimiento del contrato, es considerada de carácter confidencial.



**MANIFIESTO QUE MI ADMINISTRADA SE SUJETA AL CUMPLIMIENTO
DE LOS REQUERIMIENTOS ESTABLECIDOS EN ESTE DOCUMENTO
(ANEXO 1 ESPECIFICACIONES TÉCNICAS)**

**EXECUDATA, S.A. DE C.V.
FRANCISCO VALENTE RAMOS O'REILLY
ADMINISTRADOR ÚNICO**

T+WUD90m/+OaiJk50KAGhW3ntGBpNEPJVHU6CQyvBF3Ch2CZud0m1++hi/jjtXwdR0r/JytEzmla8Yb+UhZp260Rl24Yxz2XxoLzoJyhW7HN/OJAv/5DhrEVEcaIlgUgLKX5HKvj+441dE176AyFKs1/NhzmyS
6kahlmPdI9sXoHkUgfuUFWKT+Tdx+eyvZMH2v3rIwGogJRcu9al1rWRJz8pIVM1HQW3EXtS8nBpEvv0jspkzsRzCkLC27whoKCBgPaLLV65Yyw5wT5tZUTiLlGCWGFJFVZosuFILLU7pIfGesjmsJiefIhm
VCXTUz1lhbHuf5wZp3mBwHw==

Firmante: EXECUDATA SA DE CV
RFC: EXE0912089N5

Número de Serie: 0000100000702093151
Fecha de Firma: 26/06/2024 19:04

Certificado:

MIIGRCCBCyGAWIBAgIUMDAwMDEwMDA3MDIwOTMxNTExNDQyK0ZlhcNAQELBQAwgGVMtUwMwYDVQDDCxBQYBERUwU0VSVk1DSU8gREUGURNSU5JU1RSQUJNT04gVFJQ1VUQUJQTEuMCwGAlUECGwl
U0VSVk1DSU8gREUGURNSU5JU1RSQUJNT04gVFJQ1VUQUJQTEuMCwGAlUECGwlU0VSVk1DSU8gREUGURNSU5JU1RSQUJNT04gVFJQ1VUQUJQTEuMCwGAlUECGwl
JAYDVQJQDB1Bdi4gSglkYXNbyA3NywQ29sLjBhdWVycmVyb3EOMAwGAlUEEQwFMDAxZCzAjbGVBAYTAK1YMQ0wCwYDVQIDARDRE1YMRMwEQYDVQHDAdVUFVFRFTU9DMRUwEwYDVQQtEwxtQVQ5NzA3
MDFOTjMxXDBaBgkqhkiG9w0BCQITXJl3c3BvbnNhYmx1OibBRE1JTk1TFVFBQ01PTiBDRU5UUKFMIERFIENFU1JZQ01PUBUUK1CVVRBUK1FUYBBTCBDDT05UUK1CVV1FTLRFMB4XDTIZMDkMjEzMl
MDkMjEzMjYxMl0wGzAZBgnVBAEMTEkVYRUVNREPUQS8TQSBERSBDVjE1bMkGAlUEKRMSRVhFQ1VEQVRBIFNBIERFIENNMwRwGQYDVQKExJFWEVDVURBVEEgU0EgREUGQ1YxZCzAjbGVBAYTAK1YMSIwIA
KoZlhcNAQELBQADggIBAJ+z3Vt39vyipEzUfikiKftHmN+XWNJV2NVU7zqCjOJxgXyCRy1qnH2NB1IMu0FO2iCtVf1YgZufGssYUjEg0KXGSHD5D+uINesGk9COCse9K3cg01Iwz2/£UyVfgzDlhbIw6Scmls7Gg
A4IBDwAggEKAoIBAQCG3XyobMcEb3Yhx9ALJzuPA99z23kmyPHQQM2PAJnbc/rUd45Wflivqdbh3N2NF713UCU52FSYMDGLMpl1DNEvhadJot9cPyjvBHa/ietScv4HBEUI2H1ylEEEdWjwCDJIlb6FFwIrM
TfLw+npfeiOvyb/vl77tq9QH819C/0N2wdKn1WhYewztfXvMKTMML/1/dggDsmhUbs0JZDTRXBWgC+MT4JTuvDPvmg441lFpVhBhniEnWoKvInKf2VSJNmKGBaC+uRorCle6naOKOIzadnx9Wa8eweb6DdpyvX
VemamGcEbmeCfG6LNLWUVi08mpdyAVxEMieB0doloAgMBAAGJTzBNMAwGAlUdEwEB/wCMAAwCwYDVDR0PBAQDAGPMBEGCWSAGG+EIBAQQEAWIFoDAdBgNVHUSFjAUBggrBgeFBQcDBAYIKwYBBQUHAWIDQYJ
KoZlhcNAQELBQADggIBAJ+z3Vt39vyipEzUfikiKftHmN+XWNJV2NVU7zqCjOJxgXyCRy1qnH2NB1IMu0FO2iCtVf1YgZufGssYUjEg0KXGSHD5D+uINesGk9COCse9K3cg01Iwz2/£UyVfgzDlhbIw6Scmls7Gg
0EQUn4N1mV4ZmITDMQoyQnvV11zNMD1GHw8eR4b9ztj15hjp/Tdf4uV6j5AXGje7Edgn2o0Fs2ClOA2Mvmsm6T1IU2mlRysh4ZgK6eVN6Pyp0171a7qt0XR+ECf3RX1LHOJ3hQgB9K67e0LfiHgqTRq1HsmjDKX
VsJdBQC6g0b0AfYr6JgWgnol8YjuHjLBeoChP416Z2/I21BMUK3cn/g2xt+pKvtJLhxiH/VQ15n2TVrx+/3Qa9fOfWaxUe10yWGTy+tHsXC/BoecIE0XOHX7o+19cSSGtuShmWI0SOxfBd5I4qHjQkoZVos7KF
Ux7VsEsCpDSYcgMoTQPbLvsU2LshCBELHcMnemsu/teXT+FS1WJxk6hSNNLJR7r/vkhImBdqJWkBeV4Dn3UTp9hCNcisGum9f9cqamDrkQYVbWwGsLV/e1Kl0HSEnz7RI4pAsNs13azDkvebwnrYg7SKPP
qGQUXC/duIRzkr2R34NvQ42v9KYJWAlLLpb76bvcZu1R29Lm8X2+BUiVrKlH3UQ

Firma:

kIIMuAZnglXvXf7H3cUKwLj4NihAY7JMIUK1pjqPSRKWFNyZj/Varv0hENAgSZNl91xm5qGF6/yOhbQkHyZeDy1ZHtyaas65TXCPwO3tuEyF5ooRQBH6ozGo7hneIYsmu+mxBG6bP3goDJTYAsND5RPb+r69E8
OQ6za8uwec41zWqFYW/s6N9+v91bRHfz+G03jTliB2IhuvcmJx0HFGuzjCwDkydf8jV6dQ2eaaJnzisn8NNvS0L7p41twgZINhMQp7C5iRdwTvdAKiitcfBng8xCCkjqQ26OnCG8KXYV/bmHXWbFz8tgho4TBKS
zIRatq7LtepqWCrLE6MhkW==