# Ficha técnica base

| | |
|---|---|
| Número de versión | 2 |
| Estatus ficha técnica | **Revisión finalizada** |
| Resolución | **Aprobado** |

## Clasificación del proyecto

| | |
|---|---|
| Año POTIC | **2025** |
| Categoría | **Operativo** |
| Tipo de proyecto | **Anticipado** |
| ¿Requiere contratación? | **Sí** |
| ¿Cúantas? | **1 contratación(es)** |
| ¿Requiere un esfuerzo de implementación TIC y SI con recursos humanos internos? | **No** |

## Consideraciones estratégicas

| | |
|---|---|
| 1. ¿El proyecto contempla la realización de contrataciones consolidadas? | **No** |
| 2. ¿El proyecto contempla contrataciones que se realicen al amparo de contratos marco de TIC vigentes? | **No** |
| 3. ¿El proyecto prioriza el aprovechamiento de recursos tecnológicos disponibles con que cuentan las Instituciones? | **No** |
| 4. ¿El proyecto considera reutilizar software existente de la APF? | **No** |
| 5. ¿El proyecto implica el alojamiento de la información en territorio nacional? | **No** |
| 6. ¿El proyecto observa los Estándares Técnicos emitidos por la CEDN? | **Sí** |
| 7. ¿El proyecto considera la participación de los Centros Públicos de Investigación o Empresas Productivas del Estado en su desarrollo e implementación? | **No** |

## Información del proyecto

| | |
|---|---|
| Identificador del proyecto | **SENER-2025-O-000263** |
| Nombre del proyecto | **Fortalecimiento a la Seguridad de la Información** |
| Antecedentes | **La Secretaría de Energía tiene implementado mecanismos que garantizan la seguridad esencial, permitiendo la comunicación segura de información a través de canales de datos e internet. Estos mecanismos también protegen el correo electrónico institucional y permiten el acceso a sitios de internet a todas las personas servidoras públicas de la Secretaría de Energía. El pasado 5 de julio se dió el fallo del "Servicio Integral de Seguridad de la Información" (SISI), el cual se formalizará a través del contrato SE-28/2024, con una vigencia hasta el 31 de dicimbre de 2024.** |
| Planteamiento del problema | **La Secretaría de Energía requiere llevar a cabo la actualización tecnológica dela Seguridad de la Información, ya que los mecanismos con los que se cuenta si bien han sido efectivos, no garantizan la continuidad operación diaria, lo cual pone en riesgo el cumplimiento de las atribuciones y obligaciones establecidas en el artículo 30 del Reglamento Interior de la Secretaría de Energía para la Dirección General de Tecnologías de información y Comunicaciones, ya que no se contaría con herramientas que garanticen la integridad, confidencialidad y disponibilidad de esta información.** |
| Justificación | **La Secretaría de Energía tiene la responsabilidad de desarrollar y mantener ventajas competitivas a través de la innovación, la cual es un imperativo para las organizaciones contemporáneas. Lograr este objetivo supone un uso eficiente de la información y el conocimiento, para lo cual las tecnologías de información y comunicaciones (TIC) constituyen un recurso estratégico; para ello, es necesaria una infraestructura de TIC segura y confiable, que ayude a sus personas servidoras públicas avanzar en lugar de obstaculizar el desarrollo de sus actividades y proyectos. En la práctica, esto quiere decir que deben adoptarse esquemas de trabajo nuevos para apoyar las necesidades de desarrollo actuales y futuras de la Dependencia. Desde la infraestructura al usuario final, las TIC desempeñan un papel clave para dotar a los funcionarios públicos de recursos que permitan impulsar al Gobierno Federal y elevar su competitividad. Todos estos servicios tienen la intención principal de proporcionar a los funcionarios de la Secretaría de Energía con las Herramientas necesarias para el desempeño de sus actividades y atribuciones. Esto siempre buscando las mejores condiciones al estado.** |
| Objetivo | **El objetivo del servicio es proporcionar a la Secretaría de Energía una plataforma de Seguridad de la Información necesaria para asegurar la confidencialidad, integridad y disponibilidad de sus activos de información, garantizando que la información de las personas servidoras públicas y de la Dependencia serán protegidas, preveniendo cualquier modificación no autorizada de esta.** |
| Impacto | **Este proyecto integrará de manera inmediata los mecanismos de seguridad y telecomunicaciones que son necesarios al interior de la Secretaría de Energía para garantizar la continuidad operativa de los servicios que proporciona.** |
| Alcance | **Este proyecto beneficiará a todo el personal adscrito a la Secretaría de Energía, así como a los ciudadanos que utilizan sus recursos de información para el desempeño de sus actividades.** |
| Unidad solicitante | **Dirección General de Tecnologías de Información y Comunicaciones** |
| Líder de proyecto | Nombre **Juan Pablo Jaimes Mendoza**<br>Teléfono **5550006000**<br>Ext. **1315**<br>Correo institucional **jjaimes@energia.gob.mx** |

## Criterios de evaluación

| Nombre | Descripción | Unidad de medida | Línea base | Resultado esperado |
|---|---|---|---|---|
| Seguridad de la operación diaria | Activos de información que serán salv aguardados a través de la plataforma d e seguridad requerida | Equipos | 1000 | 1000 |
| Cobertura de seguridad | Cobertura de la Integridad, confidenci alidad y disponibilidad de la informac ión de los usuarios | Usuarios | 950 | 950 |
| Protección Perimetral | Cobertura de los inmuebles de la Secr etaría de energía de posibles ataques y/o amenazas de seguridad de la infor mación | Inmuebles | 4 | 4 |
| Madurez de seguridad de la informaci ón | Elevar el nivel de detección de brecha s de seguridad a través de análisis det allados de seguridad | Análisis realizados | 4 | 4 |

## Cronograma e información presupuestal

**Duración del proyecto**

Fecha inicio **03/06/2024**

Fecha término **31/01/2026**

Fecha evaluación **31/03/2026**

Presupuesto contrataciones **$ 26,050,260.00**

Presupuesto total estimado **$ 26,050,260.00**

## Cronograma de hitos del proyecto

| | Fecha de cumplimiento | Porcentaje de avance |
|---|---|---|
| Planeación | **27/09/2024** | **25%** |
| Inicio | **03/03/2025** | **25%** |
| Ejecución | **31/12/2025** | **25%** |
| Cierre | **31/01/2026** | **25%** |

## Contrataciones

**Nombre de la contratación**
Servicio Integral de Seguridad de la Información

**Descripción**
Proporcionar a la Secretaría de Energía los servicios de Seguridad de la Información necesarios para asegurar la disponibilidad, confidencialidad e integridad de la información, esto incluye el suministro, instalación, configuración inicial y puesta a punto de las soluciones propuestas, así como su gestión durante la vigencia del contrato. El “Servicio Integral de Seguridad de la Información” deberá basarse totalmente en las mejores prácticas documentadas formalmente tales como ITIL y en estándares internacionales como ISO 27001, esto con el propósito que, con una estrategia integral de seguridad de la información se logren mitigar los riesgos y amenazas presentes y futuras, que comprometan la integridad, disponibilidad y confidencialidad de la información; la estrategia debe proporcionar los elementos técnicos, documentales y administrativos que no solo cumplan con lo especificado, sino que permitan la operación, revisión y mejora de Sistema de Gestión de la Seguridad de la Información.

**Dictaminacion técnica**

| Fecha de cumplimiento: | Porcentaje: |
|---|---|
| 31/10/2024 | 50% |

**Firma de contrato**

| Fecha de cumplimiento: | Porcentaje: |
|---|---|
| 31/12/2024 | 50% |

**Periodo de contratación**

| Fecha de inicio: | Fecha de fin: |
|---|---|
| 01/03/2025 | 31/12/2025 |

| Cuentas gasto | Presupuesto estimado |
|---|---|
| 33901 - Servicios profesionales, científicos y técnicos integrales | $ 26,050,260.00 |
| **Total** | **$ 26,050,260.00** |

## Arquitectura tecnológica

---

Seguridad **Servicio de Centro de Operaciones de Seguridad (SOC) (Operación 7x24x365 durante la vigencia del contrato, infraestructura principal del servicio de SOC deberá estar hospedada en un centro de datos, Gestión de altas, bajas y cambios en configuraciones de las soluciones, Mantenimiento correctivo 7x24x365, Generación de reportes bajo demanda), Servicio de Seguridad Perimetral (Capacidad de identificar y controlar aplicaciones independientemente del puerto, protocolo, cifrado SSL o SSH, o táctica evasiva, políticas de uso positivo de aplicaciones, es decir, permitir, negar, habilitar políticas por horario, identificar usuarios a través de integración con Active Directory, LDAP, eDirectory, Syslog Listener y XML-API, incluir mecanismos de protección contra paquetes fragmentados, incluir mecanismos de protección contra ataques de reconocimiento (escaneo), permitir el control de trasferencia de archivos por aplicación, identificando más de 30 tipos de archivos (DLL, ZIP, EXE, etc.)), Servicio de Navegación Segura (Soportar conexiones de al menos 1200 usuarios, deberá ser conformada por (2) dos appliances con al menos 3 interfaces de red ethernet RJ-45/1 GB en alta disponibilidad, soportar protocolos de administración SNMPV2 y SNMPV3, deberá permitir políticas por categorías, generación y exportación de reportes a formato pdf, csv, doc, docx, o html, mecanismos de autenticación pueden estar basados en estándares abiertos como lo son NTLM, LDAP (Active Directory, eDirectory), Soportar el protocolo http sobre puertos 80 y 443, deberá contener descifrado de SSL/HTTPS para revisión del contenido y manejo de listas negras), Servicio de Seguridad en Correo Electrónico (soportar la conexión de al menos 800 correos electrónicos por hora, conformada por (2) dos appliances con al menos 3 interfaces de red ethernet RJ-45/1 GB, soportar protocolos de administración SNMPv2 y SNMPv3, Capacidad de reconocimiento y contención de amenazas día**

**cero con sospecha de virus, bloquear mensajes considerados como SPAM basado en la utilización de listas, Verificar el contenido de archivos anexos por lo menos para las extensiones Doc, Docx, Htm, Html, Txt, Wps, Xml, PDF, Rar, Zip), Servicio de Seguridad Endpoint (considerar protección contra amenazas de malware, exploits y día cero para al menos 1200 equipos, divididos en alrededor de 1000 estaciones de trabajo y 200 servidores físicos y virtuales, detectar y proteger contra malware, exploits y día cero a través de una consola de gestión, la cual, puede ser implementada en sistema operativo Windows, Linux o versión propietaria del fabricante, capaz de analizar archivos DLL y script JavaScript, poder analizar archivos comunes para usuarios como lo son documentos de Word, Excel, PDF, PowerPoint, HTML, entre otros, prevenir la desinstalación sin autorización de la herramienta e incluso poder utilizar una contraseña para su desinstalación o deshabilitación, deberá actualizar su contenido (firmas de detección de virus, firmas de detección de intrusos, listado de aplicaciones) desde la consola de administración, desde Internet, desde un equipo definido para la actualización local, inclusive en forma manual), Servicio de Detección y Respuesta en Red (protección contra amenazas para al menos 1200 equipos, divididos en alrededor de 1000 estaciones de trabajo y 200 servidores físicos y virtuales, permitir la compatibilidad de agentes con el protocolo de internet (IP) en las versiones 4 y 6, solución debe ser capaz de analizar archivos DLL y script JavaScript, detección y protección en las comunicaciones desde y hacia Internet, contra los ataques basados en Web de Malware día-cero, polimórfico, botnets y Ataques Persistentes Avanzados (APT), capaz de soportar reglas YARA), Servicio de Recuperación de Desastres, el cual, es un conjunto de medidas y procedimientos diseñados para proteger y restaurar la información y los sistemas de una organización ante eventos adversos como ransomware, desastres naturales, fallos técnicos o ataques cibernéticos.**

## Alineación del proyecto

---

Plan Nacional de Desarrollo **I. Política y Gobierno**

¿El proyecto está alineado a uno o más programas específicos? **No**

Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública (PNCCIMGP)
**Programa especial derivado del PNCCIMGP**

Objetivo prioritario **Promover la eficiencia y eficacia de la gestión pública**

Estrategia prioritaria **Potenciar la transformación de la Administración Pública Federal mediante el uso y aprovechamiento de las TIC, en beneficio directo de la población**

Acción puntual **Promover la interacción de las tecnologías entre la población y la APF para mejorar la comunicación entre sociedad y gobierno**

¿El proyecto está alineado a otro objetivo y estrategia del PNCCIMGP? **No**

Objetivos estratégicos de TIC **MEJORAR LA CAPACIDAD DE FLUJO DE INFORMACIÓN MEDIANTE UNA INFRAESTRUCTURA SÓLIDA Y SEGURA QUE PERMITA LA CONSOLIDACIÓN DE TODOS LOS ELEMENTOS TECNOLÓGICOS DE LAS SECRETARÍA.**

| | |
|---|---|
| Objetivos de la EDN | **Promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales** |
| Principios de la EDN | **Seguridad de la información** |

## Firma electrónica

---

**CADENA ORIGINAL UTIC:**
|| 5b2bb117b0352330c3bce102474b12ff | DANIEL SEGOVIA IBARRA | Director General de Tecnologías de Información y Comunicaciones | Secretaría de Energía | Fortalecimiento a la Seguridad de la Información | SENER-2025-O-000263 | SEID7211019R4 | 2024-09-26T19:50:14 ||

**FIRMA ELECTRÓNICA UTIC:**
meWQMxuDDEldlrQ50atu98+cCBZhOOgmOuOeb+NvdbqjTRrhpRsIjMxjFC2vj5MCW65LibDroh+jTj4bqAeB4I2mVf1tFg+mTurJSZKDZpNnthObtD/j2npKL1Yu5tbwrbX7FURRVlok2P9y1z4ne50bQFtm3EqpbRnrhJehf/inf5bdQB/SJCE23XdpbwO08UtfT7WlX845J5vHaRWhZFGld389yyrgnkGMs5wtozYPeil7JQyKUGC4VAaU7sUXsvnAes628eLgRqCUqP1BgbzZ97ozczuEn2B4Zu8C2741lqhvw7HZD5OEO+b+IYR8v8FTc3GqEG2HDJlUa/HJ4Q==