

Ficha técnica base

Estatus ficha técnica **Revisión finalizada**

Resolución **Aprobado**

Clasificación del proyecto

Año POTIC **2022**

Categoría **Operativo**

Tipo de proyecto **Ordinario**

¿Requiere contratación? **Sí**

¿Cuántas? **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? **Sí**
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-2022-O-000397**

Nombre del proyecto **Servicio Integral de Seguridad de la Información**

Antecedentes **La Secretaría de Energía cuanta actualmente con el contrato SE-23/2019 para el**

Servicio Administrado de Seguridad de la Información (SASI), mismo que tiene una vigencia al 31 de mayo de 2022, contando con los siguientes servicios: 1. Sistema de Gestión de Seguridad de la Información 2. Servicio de BIA 3. Servicio Administrado de Centro de Operaciones de Seguridad (SOC) 7x24 durante la vigencia del contrato 4. Servicio de correlación de eventos y administración de bitácoras. 5. Servicio de DNS seguro 6. Servicio de protección perimetral 7. Servicio de navegación segura 8. Servicio de antispam para el correo electrónico 9. Servicio de antivirus a estaciones locales.

Planteamiento del problema La Secretaría de Energía requiere seguir contando con un servicio de seguridad que permita mantener la integridad y confiabilidad de la información que es procesada al interior de la misma, así como generar la base normativa interna para el cumplimiento de las políticas internas en esta materia.

Justificación Este servicio se requiere para contar con una estrategia integral de seguridad de la información, que permitan mitigar los riesgos y amenazas, presentes y futuras que comprometan la integridad, disponibilidad y confidencialidad de la información dentro de la Secretaría de Energía. La estrategia debe proporcionar los elementos técnicos, documentales y administrativos que permitan la operación, revisión y mejora del Sistema de Gestión de la Seguridad de la Información con el que cuenta la Secretaría de Energía, así como apearse en todo momento a los requerimientos técnicos y operativos establecidos, los cuales resultan imperativos para contar con elementos preventivos y correctivos en caso de presentarse una posible amenaza.

Objetivo Proporcionar a la Secretaría de Energía de la Infraestructura de Seguridad Informática (hardware, software y servicios) necesaria para asegurar el flujo de su información, mismo que incluye el suministro, instalación y configuración inicial (con afinación y puesta a punto) de la solución propuesta. El Servicio Administrado de Seguridad de la Información (SASI) deberá basarse totalmente en las mejores prácticas documentadas formalmente, tales como ITIL v3; así como en estándares internacionales como ISO/IEC 27001.

Impacto Este servicio permitirá contar con herramientas para salvaguardar la seguridad de la Secretaría de Energía de manera perimetral, así como al interior de la misma, considerando los servicios esenciales con los que se cuentan, garantizando la integridad y confidencialidad de la información de cualquier amenaza interna y externa que se presente, por lo cual no contar con este servicio pondría a la Secretaría de Energía en un estado de indefensión ante estas amenazas.

Alcance Si bien la contratación de este servicio ya no contará con el servicio de Firewall (se pretende contratar por contrato marco), el Servicio Integral de Seguridad de la Información requerido por la Secretaría de Energía considerará los siguientes elementos: 1. Servicio de Centro de Operaciones de Seguridad -Administración y Gestión de los Servicios -Ciberseguridad -Análisis de Vulnerabilidades -Pruebas de Penetración -Incidentes de Seguridad -Análisis Forense -Threat Hunting -Ciberpatrullaje 2. Servicio de Seguridad Perimetral -IPS -Sandboxing -AntiDDoS 3. Servicio de Navegación Segura -Filtrado de Contenido (Alta disponibilidad) 4. Servicio de Seguridad en Correo Electrónico -Filtrado de correo (Alta disponibilidad) 5. Servicio de Correlación de Eventos -SIEM 6. Servicio de Seguridad Endpoint -Antivirus -ATP -DLP Endpoint -DNS Seguro -EDR 7.

**Servicio de Inteligencia contra Ataques -SOAR o Machine Learning IA 8.
Servicio de SGSI y BIA**

Unidad solicitante **Dirección General de Tecnologías de Información y Comunicaciones**

Líder de proyecto

Nombre **Juan Pablo Jaimes Mendoza**

Teléfono **5550006000**

Ext. **1315**

Correo institucional **jjaimes@energia.gob.mx**

Criterios de evaluación

Nombre	Descripción	Unidad de medida	Línea base	Resultado esperado
Certificaciones	El proveedor deberá presentar todas las certificaciones del personal requeridas	Puntos y porcentajes	Cumplimiento de la totalidad de las certificaciones requeridas	Que el proveedor demuestre evidencia a través de la certificación de su personal

Cronograma e información presupuestal

Duración del proyecto

Fecha inicio **03/01/2022**

Fecha término **30/09/2025**

Fecha evaluación **27/10/2025**

Presupuesto contrataciones **\$40,000,000**

Presupuesto total estimado **\$40,000,000**

Cronograma de hitos del proyecto

	Fecha de cumplimiento	Porcentaje de avance
Planeación	03/01/2022	15%
Inicio	01/10/2022	35%
Ejecución	31/12/2022	35%
Cierre	30/09/2025	15%

Contrataciones

Nombre de la contratación

Servicio Integral de Seguridad de la Información

Descripción

Proporcionar a la Secretaría de Energía de la Infraestructura de Seguridad Informática (hardware, software y servicios) necesaria para asegurar el flujo de su información, mismo que incluye el suministro, instalación y configuración inicial (con afinación y puesta a

Dictaminación técnica

Fecha de cumplimiento: 01/06/2022
Porcentaje: 75%

Firma de contrato

Fecha de cumplimiento: 26/09/2022
Porcentaje: 25%

Periodo de contratación

punto) de la solución propuesta. El Servicio Administrado de Seguridad de la Información (SASI) deberá basarse totalmente en las mejores prácticas documentadas formalmente, tales como ITIL v3; así como en estándares internacionales como ISO/IEC 27001.

Fecha de inicio:
01/10/2022

Fecha de fin:
30/09/2025

	Cuentas gasto	Presupuesto estimado
	33903 - Servicios integrales	\$40,000,000
	Total	\$40,000,000

Arquitectura tecnológica

Seguridad **1. Servicio de Centro de Operaciones de Seguridad (SOC) 2. Servicio de Seguridad Perimetral 3. Servicio de Navegación Segura 4. Servicio de Seguridad en Correo Electrónico 5. Servicio de Correlación de Eventos 6. Servicio de Seguridad Endpoint 7. Servicio de Inteligencia contra Ataques 8. Servicio de SGSI y BIA**

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 **Agilizar las funciones de las dependencias y entidades de la Administración Pública Federal, así como su coordinación y vinculación, mediante el uso de TIC**

Acción puntual **Robustecer la seguridad de los sistemas implementando esquemas de gestión y validación de las operaciones en los mismos a fin de que a través de la segregación de funciones se transparente y evite actos de corrupción en el manejo de los recursos financieros**

¿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:

|| DANIEL SEGOVIA IBARRA | Director General de Tecnologías de Información y Comunicaciones | Secretaría de Energía | Servicio Integral de Seguridad de la Información | SENER-2022-O-000397 | 66a4102f28b29abb1201891b81c4e210 | SEID7211019R4 | 2021-10-29T21:24:44 ||

FIRMA ELECTRÓNICA UTIC:

<UPpwzxN+F9k5izSkuU4kam/TnZwBi/Sxxc4aajsBICW8tzzN2vejdB2tQgNjEQM83kQkvB28lix/GlWmlXjguM6dOO6/3aAIBVS0i0VynaDdR9Q3r44tx6l8tXxcVD1Hznl68ivAd382Y6GWYEMlsFbcjz12ZmeEMVQ8facwxZ1+ymOvBmpfEY/oprDmDTQH/O7+WJs+TxOIK+M8yxVxhFMrEtH/cIj3e0XImzF9uXDD00rCN2KKpfYeNLuPhCCoYhV241By5WT1xUqBXRQvdPb5yR1vDuPFc8JUzqBapbtle/mz+S7bIEMLQj+HLMBd7nCeSoJYepHmve2/OQXA==>

