Superintendencia de Electricidad

PROYECTO

PROYECTO DE SEGURIDAD GESTIONADA, DETECCIÓN Y RESPUESTA AVANZADA SOC Y XDR

REQUERIMIENTOS TÉCNICOS

JUNIO, 2026

1 Introducción

Los riesgos de seguridad aumentan en complejidad y alcance, a medida que la tecnología evoluciona. El sector energético no está exento; ha sido históricamente un objetivo de alto interés para actores malintencionados.

Con base en esta realidad, la Superintendencia de Electricidad (SIE) gestiona un proceso continuo de fortalecimiento de su infraestructura tecnológica, destacando la implementación de un Centro de Operaciones de Seguridad (SOC) y una plataforma de Detección y Respuesta de Endpoint (XDR) en 2024. Esta iniciativa ha permitido mejorar significativamente la postura de ciberseguridad institucional, optimizando la detección y respuesta ante incidentes, logrando cumplimiento con normativas de seguridad, mayor eficiencia operativa y una reducción sustancial del riesgo cibernético.

Como parte de esta evolución y alineado con la mejora continua de su Sistema de Gestión de Seguridad de la Información, la SIE continúa avanzando en la consolidación de un ecosistema de ciberseguridad robusto, alineado con las mejores prácticas del sector y con un enfoque proactivo en la protección de la infraestructura crítica del sistema eléctrico nacional. Este proyecto se enmarca en el Eje Estratégico 2: Fortalecimiento y Desarrollo de las Capacidades Institucionales, cuyo objetivo es incrementar los niveles de calidad, eficiencia y operatividad de la institución, garantizando la seguridad y confiabilidad del servicio eléctrico.

1.1 Acerca de la Superintendencia de Electricidad

La Superintendencia de Electricidad es el ente regulador del subsector eléctrico dominicano. Tiene la obligación de fiscalizar y supervisar el cumplimiento de las disposiciones legales, reglamentarias y la normativa técnica aplicables al subsector, en relación con el desarrollo de las actividades de generación, transmisión, distribución y comercialización de electricidad. Así mismo es responsable de establecer las tarifas y peajes sujetos a regulación de precios.

Por su lado la oficina de Protección al Consumidor de electricidad (Protecom), fue creada por la Ley 125-01, artículo 121, de fecha 26 de julio del 2001. Tiene como función atender y dirimir sobre los reclamos de los consumidores de servicio público frente a las facturaciones, mala calidad de los servicios o cualquier queja motivada por exceso o actuaciones indebidas de las empresas distribuidoras de electricidad. Existen 37 motivos de reclamaciones y descripción de cada uno, para garantizar el funcionamiento homogéneo de las instancias a cargo de dar respuestas a las reclamaciones. Protecom es una dependencia de la Superintendencia de Electricidad.

2 Objeto de la convocatoria

2.1 Situación actual

En 2024, la SIE implementó un Centro de Operaciones de Seguridad (SOC) y una plataforma de Detección y Respuesta de Endpoints (XDR), logrando una mejora significativa en la postura de ciberseguridad institucional. Estas soluciones han permitido fortalecer la detección y respuesta ante amenazas, optimizar la gestión de incidentes y avanzar en el cumplimiento de estándares de seguridad.

Sin embargo, la naturaleza dinámica de las amenazas cibernéticas y la especialización del sector eléctrico exigen dar continuidad y evolución a lo construido, estableciendo una línea base de madurez en ciberseguridad que abarque aspectos de identificación, protección, detección, respuesta y recuperación ante incidentes.

Para alcanzar este objetivo, es necesario consolidar una postura de seguridad más robusta, con medidas formalizadas, mejores prácticas y un modelo de gestión optimizado. Este proyecto busca fortalecer y expandir las capacidades del SOC y EDR/XDR, asegurando su integración efectiva con nuevas herramientas, procesos y estrategias de protección.

Bajo un enfoque de diseño e implementación llave en mano, el proyecto incluirá la configuración, capacitación y puesta en servicio de las soluciones requeridas, alineadas con los objetivos estratégicos de la SIE. Su implementación garantizará que la infraestructura de seguridad evolucione de manera escalable y resiliente, respondiendo eficazmente a los desafíos actuales y futuros del entorno cibernético.

2.2 Descripción de proyecto

Para consolidar y optimizar la postura institucional de ciberseguridad, se requiere una reestructuración estratégica que fortalezca las capacidades existentes mediante nuevas adquisiciones e implementación de mejores prácticas.

El objetivo del proyecto es seleccionar un único proveedor que garantice la evolución y optimización de las soluciones de seguridad actuales, asegurando una gestión integral, alineada con los requerimientos funcionales y estratégicos de la SIE. Esta iniciativa busca no solo mejorar la protección y resiliencia de la infraestructura tecnológica, sino también maximizar la eficiencia operativa y el cumplimiento normativo en un entorno de amenazas en constante cambio evolutivo.

2.3 Criterios de selección

Los oferentes serán evaluados en función del cumplimiento técnico, ponderaciones cualitativas y cuantitativas de los productos y servicios ofertados.

El Oferente deberá detallar claramente, a lo largo de toda su propuesta, de qué manera alcanzará los objetivos establecidos por la Superintendencia de Electricidad.

Experiencia en este tipo de servicio

La Superintendencia de Electricidad desea contar con Proveedores que demuestren solidez mediante experiencias previas en la prestación de este tipo de servicio, en el mercado nacional, con empleados (certificados) dispuestos a ser asignado al proyecto, en particular, y que sean capaces de adaptarse a la dinámica de trabajo y de la operativa de la organización.

Metodología de Gestión

El Proveedor deberá basarse en una metodología de gestión de los servicios, fundamentando en forma concreta la prestación de un servicio de excelencia, de acuerdo con los requerimientos del presente pliego.

Responsabilidad por los resultados

Con su estructura, el proveedor debe asumir la responsabilidad por los resultados, comprometiéndose a cumplir las metas definidas en la Especificación del Servicio.

2.4 Factores condicionantes

En caso de no cumplimiento de alguno de los puntos detallados en este documento, la Superintendencia de Electricidad podrá desestimar la oferta y no continuar con su evaluación.

Debe estar incluido dentro del servicio los siguientes ítems:

- Objetivos y alcance.
- El equipo de trabajo propuesto por el oferente, deben hablar y escribir en idioma español.
- Deben cumplir con la experiencia y certificaciones requeridas en esa ficha técnica.
- Deben cubrir los acuerdos a los que se llegue con la SIE en la fase de descubrimiento y los tópicos ya señalados en esta ficha técnica.
- El oferente debe cubrir todos los gastos que sean necesario para la ejecución de un proyecto exitoso.

3 Alcance del proyecto

3.1 Funcionalidades mínimas

Indistintamente de los productos y servicios que pueda tener la solución ofertada, se espera que esta considere los siguientes:

CANT.	DESCRIPCIÓN
500	**Seguridad avanzada.** **Protección Seguridad – Dispositivos Finales que incluya detección y respuesta extendidas.** Protección de Seguridad Avanzada para Dispositivos de usuarios Finales – Implementación de una solución de detección y respuesta Respuesta de Endpoints (EDR/XDR, por sus siglas en inglés) que brinde protección integral a los computadores de usuario final, garantizando monitoreo continuo, análisis avanzado de amenazas y mitigación proactiva de incidentes.
70	**Seguridad avanzada** **Protección Seguridad – Servidores.** Implementación de soluciones de seguridad avanzadas para la protección de servidores críticos, asegurando detección de vulnerabilidades, monitoreo de integridad y respuesta automatizada ante incidentes.
1	**Centro de Operaciones de Ciberseguridad** Servicios de seguridad administrada contemplando un alcance para 570 objetos (Servidores + Estaciones), que incluya: • Disponibilidad 24x7x365. • MTTA 15 min (incidentes críticos). • MTTR contención 4h / erradicación 24h. • Escalamiento L1→L2→L3 en 15/30/60 min. • Estados del caso: nuevo, en análisis, contenido, erradicado, cerrado. • Implementar indicadores de riesgo. • Adoptar el protocolo de respuesta rápida a incidentes integrando al Centro Nacional de Ciberseguridad de la Republica Dominicana.

3.2 Centro de Operaciones de Seguridad (Security Operations Center, SOC)

La SIE ha fortalecido la capacidad de monitoreo estratégico, análisis cibernético y respuesta a incidentes en tiempo real; para garantizar la continuidad y evolución de este servicio, el proyecto busca ampliar y optimizar las capacidades en materia de preservas las Integridad, Disponibilidad e integridad de la información, asegurando una gestión integral de la ciberseguridad alineada con los desafíos actuales y futuros.

El servicio deberá proporcionar inteligencia proactiva ante amenazas, detección avanzada de anomalías y toma de decisiones basada en datos, reforzando su integración con el Centro Nacional de Ciberseguridad (CNCS) y CSIRT-RD[1] para una respuesta rápida y coordinada ante incidentes críticos.

Esta iniciativa garantizará una operación 24/7 con cobertura completa de eventos de seguridad, mejorando la resiliencia cibernética de la SIE y permitiendo un modelo de seguridad adaptable y escalable según las necesidades institucionales.

3.3 Equipo de respuesta ante incidentes

La SIE debe contar con un equipo de respuesta ante incidentes integrado en el Centro de Operaciones de Seguridad, el cual opera de manera continua las 24 horas del día, los 7 días de la semana, 365 días del año para detectar, contener y remediar cualquier evento de ciberseguridad que pueda impactar la organización.

Buscamos robustecer las capacidades de detección temprana y respuesta rápida, evaluar amenazas en tiempo real y aplicar medidas correctivas oportunas. Mediante reportes de monitoreo, tenemos como objetivo identificar intentos de acceso no autorizado, detección de *malware* en dispositivos internos y vulnerabilidades en la infraestructura digital, asegurando una gestión proactiva de riesgos y una mejora continua en la postura de seguridad institucional.

El equipo de respuesta ante incidentes ha de tener un enfoque basado en la inteligencia de amenazas, utilizando herramientas avanzadas de monitoreo y correlación de eventos para priorizar alertas y minimizar tiempos de respuesta. Además, se integra con el Centro Nacional de CNCS y CSIRT-RD para garantizar una respuesta coordinada en caso de incidentes de alto impacto.

Este modelo de gestión ha demostrado su efectividad en la mitigación de riesgos cibernéticos y en la protección de los activos críticos de la SIE, permitiendo una mayor resiliencia frente a las amenazas emergentes y asegurando la continuidad operativa de la organización.

3.4 Generación de informes

La generación de informes es un componente imprescindible en la gestión del SOC y del equipo de respuesta ante incidentes. Además de los informes predeterminados generados por cada solución de seguridad, durante la prestación del servicio se deberá

[1] CSIRT-RD: Por sus siglas en inglés, Security Incident Response Team - RD

proporcionar documentación detallada que permita una supervisión efectiva y la toma de decisiones basada en datos.

Los informes incluirán:

- Reportes periódicos de avances, con análisis detallados sobre la evolución del proyecto y cumplimiento de hitos.
- Presentaciones ejecutivas, diseñadas para comunicar hallazgos pertinentes a la alta dirección y equipos operativos.
- Boletines de inteligencia de amenazas, proporcionando información actualizada sobre tendencias y riesgos emergentes.
- Notificaciones y alertas de seguridad, asegurando la divulgación oportuna de riesgos críticos que puedan impactar la organización.
- Documentación técnica y operativa, incluyendo cartas, planillas y copias impresas de informes relevantes.
- Recomendaciones estratégicas, orientadas a mejorar la postura de ciberseguridad y garantizar el cumplimiento de los objetivos del proyecto hasta su salida a producción.
- Logs y telemetría retenidos mínimo 12 meses en línea.
- Exportación a formato abierto cuando la SIE lo requiera.
- Evidencias con hash y bitácora para auditoría/forense.

Esta estrategia de generación de informes garantiza una visión integral de la seguridad cibernética en la SIE, facilitando la respuesta rápida ante incidentes, la mejora continua y la optimización de los procesos de monitoreo y protección.

3.5 Entregables del proyecto

Los siguientes son los entregables que se recibirán como parte de los servicios ofrecidos, los cuales deben ser formalmente revisados y aceptados. Al comenzar cada fase del proyecto, se definirán en conjunto los criterios de aceptación para cada entregable.

- **Plan de Integración y Evolución del SOC y XDR/EDR** – Documento detallado que establece el itinerario del proyecto, las fases de implementación y los hitos relevantes para la mejora continua de los servicios de seguridad gestionada.
- **Documento de Alcance.**
- **Transferencia de conocimiento de cada solución ofertada**. Para tres (3) personas.
- **Documento del Plan de Soporte y acuerdo de cumplimiento**. En el cual contemple el detalle de las acciones que están bajo su responsabilidad, para

garantizar su correcto funcionamiento y la continuidad de los servicios de la SIE. Además, debe especificar el modo de respuesta a incidentes que se reporten desde la organización y los tiempos de respuesta para brindar la solución.

4 Requerimientos preliminares

4.1 Calificación del proveedor

El oferente, además de cumplir en cuanto a cantidad, debe proporcionar productos de reconocido éxito y calidad, verificables en portales de firmas de evaluación reputadas, por ejemplo, Forrester Wave[2] y Gartner Magic Quadrant[3], asimismo, cumplir los requisitos siguientes:

- El Oferente debe ser un canal autorizado de parte del fabricante de la solución ofertada.

- Integrar en el proyecto a implementadores certificados en los productos ofertados.

- El proveedor debe ofertar todos los ítems presentados en la ficha técnica, por lo que serán adjudicados por todos los ítems.

4.2 Mantenimiento y soporte

- Incluir en el proyecto soporte técnico a través de varios canales y que este sea renovable más allá del periodo inicial, especificando el fin de vida de las diferentes soluciones.

- Acceso a actualizaciones de los softwares del proyecto.

4.3 Capacitación

Se requiere que la propuesta incluya la capacitación técnica y funcional de la solución (puede ser intensivo) para 3 personas.

---

[2] La metodología Forrester Wave™ es una representación gráfica de análisis que se crea con la ayuda de un analista interno y un investigador asociado que llevan a cabo el análisis y recopilan datos, un equipo de respuesta del proveedor que proporciona información detallada sobre productos y servicios.

[3] Un Magic Quadrant de Gartner (literalmente, "cuadrante mágico" en español) recoge la culminación de la investigación de un mercado específico, y te proporciona una visión panorámica de las posiciones relativas de sus competidores.

4.4 Adopción de controles de la ISO/IEC 27001:2022

- Garantizar Monitoreo Continuo
- Como proveedores, poder ser evaluados en términos de Confidencialidad, Integridad y Disponibilidad.
- Firma de acuerdo de confidencialidad (NDA).

4.5 Experiencia del proveedor

- El oferente debe proporcionar referencia de al menos tres (3) proyectos previos de soluciones y productos de seguridad tecnológica.
- Tener un mínimo de 5 años de presencia en el mercado local.

4.6 Cronograma

El Oferente deberá proveer el Cronograma de Implementación de los servicios.

4.7 Soporte técnico

El Oferente deberá proporcionar soporte y garantías del fabricante para la solución ofertada y todos sus módulos, y asegurar que los soportes y garantías de los fabricantes sean válidas hasta el final del Período de Responsabilidad por Defectos después de finalizar el proyecto o según se identifica a continuación:

Tipo	Comenzando desde	Duración
Soporte y garantías del fabricante	Salida a producción	Al menos 12 meses
Soporte del canal (Partner)	Salida a producción	Al menos 12 meses
Soporte posproducción y garantía de los trabajos realizados	Finalización práctica	Al menos 3 meses

4.8 Personal clave y certificaciones

El Oferente deberá proveer personal calificado con certificaciones vigentes y experiencia relacionada en las tecnologías a operar. Las credenciales podrán cumplirse por equivalencia aceptada y con plazo de regularización, según se detalla.

4.8.1 Dotación mínima por rol

Líder de Seguridad / Gobierno (1 persona)

Certificaciones:

- CISM o CISSP;
- e ISO/IEC 27001 Lead Implementer o, Lead Auditor.

Auditoría / Cumplimiento (1 persona)

Certificaciones:

- CISA (aceptable ISO/IEC 27001 Lead Auditor como equivalente).

Operación SOC 24/7 (mín. 2 analistas por turno)

Certificaciones:

- Certified SOC Analyst (CSA) o equivalente (CompTIA CySA+, Microsoft SC-200).
- Al menos 1 analista por turno con CEH o equivalente ofensivo (CompTIA PenTest+, OSCP "Associate/Junior").
- Security+ deseable para perfiles junior/rotación.

Respuesta a Incidentes – IR Lead (1 persona)

Certificaciones:

- Certified Incident Handler (ECIH o GCIH) o equivalente ISO/IEC 27035 Lead Incident Manager.

Gestión de servicios (1 persona)

Certificación:

- ITIL® 4 Foundation.

Nota de cobertura: La dotación debe garantizar **operación 24/7** con reemplazos, vacaciones y ausencias, sin degradar el nivel certificado por turno.

4.8.2 Equivalencias aceptadas

- CSA: CompTIA CySA+, Microsoft SC-200, GIAC GCIA/GCED, o certificación oficial de analista en SIEM/XDR de fabricante (p. ej., Splunk/Elastic/QRadar).
- CEH: PenTest+, OSCP (nivel inicial), GIAC GPEN/GWAPT.
- CISA: ISO/IEC 27001 Lead Auditor con experiencia demostrable en auditorías TI.
- CISM/CISSP: si no estuviera vigente, se admite CRISC o CCISO como puente, junto a ISO 27001 LI/LA y experiencia de gobierno.
- Incident Handler (ECIH/GCIH): GCIRT/GCFA o SC-200 cuando el stack sea Microsoft y se presenten runbooks/post-mortems que evidencien experiencia.
- ISO/IEC 27035 Lead Incident Manager: implementación documentada de NIST SP 800-61 (procedimientos, RACI, métricas MTTA/MTTR, tabletop ejecutado en 12 meses), con compromiso de certificación en plazo.

4.8.3 Evidencia, verificación y vigencia

- Presentar copia de certificados y/o ID de verificación en línea; indicar fecha de emisión/vencimiento.
- La Entidad podrá verificar en los portales de los emisores cuando aplique.
- Mantener vigentes las credenciales durante toda la ejecución del contrato; notificar con 30 días cualquier expiración y su plan de renovación.

4.8.4 Matriz resumen de credenciales y equivalencias

Rol	Cantidad mínima	Certificaciones requeridas	Equivalencias aceptadas (si aplica)	Cobertura por turno	Evidencia requerida
Líder de Seguridad / Gobierno	1	CISM o CISSP; y ISO/IEC 27001 Lead Implementer o Lead Auditor	CRISC o CCISO (como puente) + ISO 27001 LI/LA + experiencia de gobierno	Horario hábil / guardia; no 24/7	Certificados vigentes + ID de verificación + CV con proyectos relevantes

Auditoría / Cumplimiento	1	CISA (aceptable ISO/IEC 27001 Lead Auditor como equivalente)	ISO 27001 Lead Auditor + experiencia demostrable en auditorías TI	Según demanda / auditorías	Certificados + informes/actas de auditoría
Operación SOC 24/7 - Analistas	2 por turno	Certified SOC Analyst (CSA)	CompTIA CySA+, Microsoft SC-200, GIAC GCIA/GCED, o analista SIEM/XDR (Splunk/Elastic/QRadar)	24/7	Certificados + plan de turnos + runbooks
Operación SOC 24/7 - Perfil ofensivo por turno	1 por turno	CEH (deseable CompTIA Security + para perfiles junior/rotación)	CompTIA PenTest+, OSCP (nivel inicial), GIAC GPEN/GWAPT	24/7 (validación de detecciones / emulación ATT&CK)	Certificados + evidencias de emulación ATT&CK
Respuesta a Incidentes – IR Lead	1	Certified Incident Handler (ECIH o GCIH) y ISO/IEC 27035 Lead Incident Manager	GCIRT/GCFA; o SC-200 (stack MS) + runbooks/post-mortems; NIST 800-61 implementado como puente a 27035	On-call 24/7	Certificados + post-mortems + métricas MTTA/MTTR + tabletop
Gestión de servicios (ITSM)	1	ITIL® 4 Foundation	Experiencia ITSM demostrable (complementa, NO sustituye)	Horario hábil / coordinación	Certificado + flujos ITSM + SLAs/OLAs

4.9 Duración del servicio, licenciamiento, soporte técnico y soporte funcional

La duración de los servicios requeridos es por doce (12) meses. El esquema de licenciamiento y soporte técnico durante el tiempo de servicio deberá ser propuesto por el oferente en función de las características de la solución presentada.

5 Requerimientos técnicos

La presente sección establece los requerimientos técnicos mínimos para la consolidación del Centro de Operaciones de Seguridad (SOC) y la plataforma de Detección y Respuesta Extendida (XDR) de la SIE. Estos abarcan tanto los dispositivos de usuario final como los servidores y cargas de trabajo críticas, garantizando la prevención, detección y respuesta rápida ante incidentes. Se exige que las soluciones cuenten con capacidades de analítica y correlación de eventos, investigación de causa raíz, telemetría avanzada y generación de reportes consolidados, además de integrarse con procesos de gestión y marcos normativos internacionales. En este sentido, los oferentes deberán proponer herramientas escalables, interoperables y probadas en entornos de misión crítica, que contribuyan a la resiliencia institucional y a la coordinación con los organismos nacionales de ciberseguridad.

Área	Requisito	Cumple / No Cumple
Detección/Prevención	Machine learning estático y dinámico, operación offline	
Ransomware	Detección de cifrado y rollback de archivos	
Control de aplicaciones	Allow/deny por hash, ruta, certificado; inventario y whitelisting	
Control de dispositivos	Políticas sobre USB y medios: permitir, solo lectura o bloquear	
Protección de vulnerabilidades	Virtual patching a nivel driver de red (CVE y 0-day)	
EDR/XDR – IOC sweep	Búsqueda de IoC en todos los endpoints	
EDR/XDR – RCA	Análisis de causa raíz (timeline/causalidad)	
EDR/XDR – Live response	Investigación en vivo y acciones remotas en endpoint	
EDR/XDR – Ingesta	Colector/correlación de endpoint, red, correo y cargas	

EDR/XDR – Analítica	Modelos avanzados de detección y correlación	
EDR/XDR – Triage	Vista única de alertas con priorización y estado	
EDR/XDR – Attack story	Visualización del ataque (grafo/timeline, análisis red)	
Threat hunting	Constructor de consultas, búsquedas guardadas, acciones	
API/automatización	API para orquestación y automatización	
Gestión/seguridad	RBAC/AD para control de accesos y roles	
Reporting	Informes operativos y ejecutivos, trazabilidad y CVE	
Rendimiento	Control de CPU en escaneos y operación	
MDR	MDR opcional integrado en el agente	

5.1 Respuesta a Incidentes

	Respuesta a Incidentes	Cumple / No Cumple
1	El oferente deberá suministrar un servicio de evaluación inicial del plan de respuesta a incidentes de la entidad y proporcionar un informe del nivel de madurez, los resultados de la evaluación y un conjunto de recomendaciones.	
2	Se deben desarrollar con la entidad al menos un (1) manual de estrategias de respuesta a Incidentes (playbooks) en caso de que un incidente de ciberseguridad tenga impacto en la red. El manual de estrategias guiará a los analistas de la entidad en la detección, contención, erradicación y recuperación.	
3	Se deben probar (ejercicios de simulación) con la entidad usando el manual de estrategias de respuesta a incidentes desarrollados a fin de	

	que la entidad cuente con un plan de acción de respuesta a incidentes claro y conciso.	
4	El servicio debe incluir la capacidad de brindar ayuda inicial a la entidad (4 horas) si un incidente de seguridad se presenta y de ofrecer bolsas de horas adicionales de acuerdo con el soporte requerido para la detección, análisis, contención, reducción del impacto del incidente y recuperación de las operaciones.	
5	El servicio debe permitir realizar una evaluación final del plan de respuesta a incidentes de la entidad y proporcionar un informe del nivel de madurez, los resultados de la evaluación y un conjunto de recomendaciones.	

6 Evaluación de la propuesta técnica

Las propuestas presentadas por los oferentes serán evaluadas mediante la utilización de los siguientes criterios:

- Evaluación técnica Cumple / No Cumple.
- Evaluación económica.

Los Oferentes deben incluir contratos y/o cartas de clientes donde se evidencie su experiencia en proyectos similares. Solo las propuestas que CUMPLAN en la Evaluación Técnica pasan a la evaluación de la Oferta Económica. Por lo tanto, deben indicar en su propuesta en que página o en que enlace se encuentra la evidencia de cumplimiento de cada requerimiento técnico solicitado.

6.1 Oferta técnica

El contenido y extensión y formato de presentación de la Oferta Técnica debe ser de acuerdo con lo siguiente:

Ítem	Contenido	Extensión Formato de Presentación
OT1	<u>Presentación de la Empresa o Consorcio</u>	
	- Breve presentación de la empresa y su capacidad instalada para ofrecer y	Tres (3) paginas máximo.

	respaldar los servicios descritos en estos TDRs.	
OT2	<u>Experiencia de la Empresa o Consorcio</u>	
	- Breve reseña de la experiencia del personal que se asignara al proyecto.	Tres (3) páginas máximo, más anexos relevantes que fueran pertinentes.
	- Detalle de la experiencia relevante los últimos tres (3) años en proyectos similares en dimensión y/o comparables en alcance, monto y cantidad de usuarios.	Tres (3) páginas máximo por cada experiencia referenciada, más los anexos relevantes que fueran pertinentes.
	- Cartas de certificación y satisfacción por parte de los clientes de los proyectos citados como experiencia relevante. - Evidencias y referencias del alcance de los proyectos citados en relación con la naturaleza cada proyecto citado, sus componentes, los recursos involucrados, etc.	N/A
	NOTA: Los proyectos citados como referencia para los que no se presenten las cartas de certificación y las evidencias correspondiente no serán consideradas. De igual manera el personal propuesto que será asignado al proyecto y del cual no se presenten sus hojas de vida, certificaciones y evidencias correspondientes no serán considerados.	N/A
OT3	<u>Alcance de la solución</u>	
	- Descripción de cómo la solución propuesta cubre o compensa las funcionalidades requeridas tomando como base mínima las especificaciones descritas en estos TDRs.	Treinta (30) páginas máximo, más anexos relevantes que fueran pertinentes.
OT4	<u>Esquema de licenciamiento</u>	
	- Definición del esquema de licenciamiento propuesto sobre la base de la estimación de la cantidad de usuarios, las facilidades incluidas y el nivel de almacenamiento/procesamiento previsto. - El esquema de licenciamiento debe considerar el escalamiento de las	Diez (10) páginas máximo, más anexos relevantes que fueran pertinentes.

	facilidades, cantidad de usuarios, nivel de acceso etc.... Para la descripción del esquema de licenciamiento se debe tomar como base mínima las especificaciones descritas en estos TDRs.	
OT5	<u>Estrategia de Implementación</u>	
	- Descripción de la estrategia de implementación propuesta, considerando como mínimo las especificaciones descritas en estos TDR. Detallando claramente los siguientes aspectos: - Metodología propuesta de implementación. - Cronograma detallado del proceso de implementación y puesta en marcha de las soluciones indicando claramente los hitos de avance y el programa de formación para el personal de la SIE durante el proceso. - Composición del equipo de proyecto provisto por la empresa oferente, incluyendo: alcance de las responsabilidades de sus miembros, hojas de vida, nivel de dedicación, referencias profesionales, etc.... - Consideraciones relevantes sobre: manejo de contingencias, instalación de servicios, parametrización y ajustes, así como, requerimientos de HW y conectividad que debe cumplir la SIE, para llevar a cabo la estrategia de implementación en los tiempos descritos.	Diez (10) páginas máximo, más los anexos relevantes que fueran pertinentes.
OT6	<u>Soporte técnico y SOC</u>	
	- Descripción detallada del alcance del soporte técnico y del SOC a ser provisto por la empresa, diferenciando claramente el primer año de implementación y puesta en marcha de los años subsiguientes considerados en el servicio.	Veinte (20) páginas máximo, más los anexos relevantes que fueran pertinentes.

	- Para la descripción del esquema de soporte técnico se debe tomar como base mínima las especificaciones descritas en estos TDRs.	
OT7	**Estrategia de transferencia de conocimiento**	
	- La propuesta debe contener la descripción de la estrategia de transferencia de conocimiento, considerando como mínimo las especificaciones descritas en estos TDRs.	Dos (2) páginas máximo, más los anexos relevantes que fueran pertinentes.

6.2 Oferta económica

En la Oferta Económica deben ser considerados todos los costos asociados a la puesta en cuanto a, operación, servicios, licenciamientos y adecuaciones de la solución, tanto durante el proceso de implementación como durante el tiempo establecido de servicio.

7 Tiempo de entrega y Condiciones de pago

7.1 Tiempo y lugar de entrega.

El tiempo de entrega es de 30 días laborables en la Superintendencia de Electricidad, en la Av. John F. Kennedy No.3, Esq. Erik Leonard Ekman, Arroyo Hondo I, Santo Domingo, República Dominicana.

7.2 Condiciones de pago.

La Entidad Contratante procederá a realizar un primer pago por concepto de avance, por un porcentaje del 20% del valor del Contrato a partir de la firma y la Certificación de Contrato por la Contraloría General de la República y el restante 80% con la entrega y puesta en marcha del servicio.

7.3 Supervisor o responsable del contrato

La SUPERINTENDENCIA DE ELECTRICIDAD ha designado como supervisores o responsables del contrato a los representantes, Joel Agustin Jimenez de la dirección del Despacho y Yuset Guerrero. de la dirección de Tecnología.

8 Vigencia del Contrato

La vigencia del Contrato será por un (1) año, a partir de la fecha de la suscripción de este y hasta su fiel cumplimiento y liquidación.

9 Responsables del Informe

Joel Agustin Jimenez Francisco

Gerente De Ciberseguridad

Yuset Guerrero Cueto

Encargado de Proyectos
Interoperabilidad de Datos

SIE | Superintendencia de Electricidad

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACION Y COMUNICACION

Santo Domingo, R.D