COMITÉ DE TRANSPARENCIA

DÉCIMA NOVENA SESIÓN EXTRAORDINARIA
26 de agosto de 2024

ACUERDO CT/19SE/066ACDO/2024

Requerimiento de la Unidad de Tecnologías Operacionales y de Información (UTOI), para que el Comité de Transparencia del Centro Nacional de Control del Gas Natural (CENAGAS), analice (confirmar, modificar o revocar) la **clasificación de la información como reservada**, total por un periodo de **5 años**, respecto al "*contrato "CENAGAS/SERV/074/2023-P" que tiene por nombre (Continuidad en el servicio de ciberseguridad SCADA para el CENAGAS)*", lo anterior de conformidad con lo establecido en los artículos 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública (Ley General); y 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), derivado de la solicitud de acceso a información con número de folio **330005724000218**.

ACUERDO CT/19SE/066ACDO/2024

Con fundamento en los artículos 43, 44, fracciones I, II, IV, 100, 101, 104, 106, fracción I, 108, 113, fracciones I, 137 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 64, 65, fracciones I, II, IV, 97, 98, fracción I, 99, 100, 102, 110 fracciones I, 140 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Sexto, Séptimo, Décimo séptimo fracción VIII, Trigésimo Tercero, Trigésimo Cuarto y Quincuagésimo quinto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos Generales), y en el numeral 3.1, fracción VII de los Criterios de funcionamiento del Comité de Transparencia del CENAGAS, este Comité **CONFIRMA** la propuesta de clasificación total de la información como **reservada**, realizada por la Unidad de Tecnologías Operacionales y de Información (UTOI), por un periodo de cinco (5) años, referente al "*contrato "CENAGAS/SERV/074/2023-P" que tiene por nombre (Continuidad en el servicio de ciberseguridad SCADA para el CENAGAS)*", así como sus anexos técnicos y entregables, derivada de la solicitud de acceso a información con número de folio **330005724000218**.

Toda vez que la información solicitada contiene información clasificada como reservada, por lo que se colige lo siguiente:

El 07 de febrero del año 2023 el CENTRO NACIONAL DE INTELIGENCIA (CNI) otorgó el carácter de SEGURIDAD NACIONAL al proyecto de contratación denominado "CONTINUIDAD EN EL SERVICIO DE CIBERSEGURIDAD SCADA PARA EL CENAGAS", proyecto que en el mes de julio de ese mismo año finalmente se estableció bajo el contrato CENAGAS/SERV/074/2023-P, utilizando la misma denominación del proyecto en comento.

Toda vez que su difusión expondría características técnicas, operativas y de infraestructura de la Ciberseguridad estratégica que se utiliza para el Transporte del Gas Natural por ducto, revelando ubicación y características del equipo, lo que vulneraría la Ciberseguridad del CENAGAS y compromete la infraestructura de Seguridad Nacional del país, además de poner en riesgo los sistemas de tecnologías de información que respaldan todos los datos del sistema de transporte de la molécula de gas, así como las características técnicas de las ubicaciones estratégicas del Centro en el perímetro operacional más que administrativo.

La Ciberseguridad es una prioridad para el Gobierno Federal, por ello el CENAGAS, cuenta con una protección de información y datos a nivel industrial, a través de software de análisis de vulnerabilidades especializado, firewalls para proteger contra ataques al Sistema SCADA, detección de entradas no autorizadas, detección de malware y otras amenazas digitales, el cual detecta posibles incidentes que son reportados y revisados por el Centro de Operaciones de Seguridad (SOC) y el Centro de Operaciones de Red (NOC),. servicios que monitorean la red industrial 24X7X365, de esa forma el Centro mantiene los más altos niveles de seguridad digital para proteger la información de todos el sistema informático que da soporte al Transporte de Gas Natural. Cualquier incidente informático es atendido a la brevedad y con respuesta inmediata, por ello la Seguridad Cibernética no sólo es a nivel software, hardware, reportes, sino también de protocolos para accionar el plan de recuperación, el plan de continuidad y equipo de respuestas ante incidentes en caso de un ataque a la seguridad del perímetro industrial del CENAGAS, es decir, es una estrategia integral. La pérdida de información por un ataque cibernético a este sistema sería catastrófico para el Centro y pondría en riesgo no sólo la red industrial, sino podría en caso extremo, comprometer la red administrativa, que aunque esta, se mantiene protegida por su propias Seguridad Informática, podría exponer otros sistema de información esenciales para la operación del CENAGAS como el SAP- GRP, aplicativos del Centro, nóminas, correos electrónicos, archivos de los usuarios o un ataque de malware o de virus, que podría dañar los datos almacenados.

Por lo que, atendiendo las responsabilidades de contar con el carácter de Seguridad Nacional resulta necesario reservar la información del contrato por al menos cinco años, como lo determina la normatividad en la materia, a fin de asegurar que las configuraciones de ciberseguridad, así como todo el hardware destinado a este fin, sean protegidos con la finalidad de blindar el sistema informático que da la seguridad a la red industrial, ya que revelar sus características técnicas y operativas hace vulnerable a la red.

El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

Si bien el procedimiento de contratación derivó en una adjudicación directa, la información intrínseca del proceso de contratación requirió de información técnica relevante que parte de una Base Instalada que se originó desde la implementación del sistema SCADA. A fin de poder llevar a cabo una investigación de mercado y demás consideraciones necesarias para obtener el carácter de Seguridad Nacional, dictamen de la Coordinación de Estrategia Digital Nacional y procedimiento de contratación bajo el mismo numeral de seguridad nacional.

La infraestructura existente, la cual es la base del contrato vigente, se expresa a través del contrato per se y sus anexos, así como la información que se genera mensualmente como entregable del servicio de NOC (Centro de Operaciones de Red) y SOC (Centro de Operaciones de Seguridad), objeto de la contraprestación a favor del proveedor que administra los servicios en comento. En

cuanto a los entregables mensuales, estos contienen información sensible de cada una de las aplicaciones que operan para salvaguardar la integridad de las redes, el perímetro y la seguridad del sistema SCADA en las capas de conexión con las interfaces institucionales y de servicios periféricos como Nominaciones, GRP, SGRIIGD y accesos remotos, por lo que es de alta importancia, reservar el acceso al contenido de los reportes que se emiten mensualmente, pare evitar que se pueda configurar una ruta que comprometa las operaciones industriales.

Por lo anterior, es importante reservar totalmente el contrato, anexos y entregables, con la finalidad de evitar un Ciberataque que comprometa la infraestructura del Sistema SCADA, el cual es el centro tecnológico para la vigilancia y monitorio del transporte de Gas Natural, con la pérdida de esta herramienta se vulnera la seguridad de la información y se expondrían datos sobre ubicaciones, presiones, cantidades y demás variables relevantes para la operación de los gasoductos. Por lo que se incumpliría el Marco de Gestión de Seguridad de la Información que mandata la Coordinación de Estrategia Digital Nacional para sistemas informáticos.

El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

Salvaguardar información de hardware y software de Ciberseguridad para no marcar vectores de ataque. Si bien ya se mencionó en el punto anterior la importancia de salvaguardar la información del contrato y los reportes mensuales con información sensible con respecto al mes que se brindó el servicio. Es aún más importante no comprometer las arquitecturas en lo que respecta a hardware, software y su licenciamiento, toda vez que, de exponer la información de la arquitectura integral de la solución de Ciberseguridad SCADA, se estarían marcando los vectores de ataque para toda persona que pueda entender de infraestructura de Ciberseguridad. Ya que podría comprender el nivel de protección con el que el Centro cuenta y no cuenta. Por lo que, de exponerse, intrínsecamente ingresamos a un nivel de vulnerabilidad sin capacidad de contener ningún ataque más allá de la infraestructura instalada.

Cabe comprender que la divulgación de la información trasciende hasta el punto de que la persona que posea esta información puede conocer la marca de la infraestructura e instalaciones que tenemos para contener un ataque cibernético, eso se concatena con poner en riesgo la operación del transporte de gas natural, así como el sistema de monitorio SCADA del cual es responsabilidad de esta Dirección Ejecutiva de Tecnologías Operacionales. Ya que si la delincuencia realiza un ciberataque a los dispositivos electrónicos así como una penetración al sistema, la información sensible quedaría expuesta y sería una pérdida económica significativa en caso de detrimento de esta, aparte de poner en riesgo la integridad de los gasoductos por posibles interrupciones del servicio lo que podría ser un pérdida incuantificable para el estado, aparte del peligro que significa una explosión en cualquier parte de los gasoductos, por no tener el control de la información durante un ataque cibernético.

En consecuencia, se **notifica** a la Unidad de Tecnologías Operacionales y de Información (UTOI), el presente Acuerdo, **requiriendo** dé cabal cumplimiento, y a su vez remitan a la Unidad de Transparencia, la respuesta correspondiente a la solicitud de acceso a información con número de folio **330005724000218**, a más tardar el día dos de octubre de dos mil veinticuatro, para con ello entregarla al particular en tiempo y forma, a través del del Sistema de Solicitudes de Acceso a la Información (SISAI 2.0) de la Plataforma Nacional de Transparencia (PNT).

NOMBRE	CARGO	FIRMA
Dr. Jerjes Giovanni Sánchez Reyes	Presidente Suplente del Comité de Transparencia	
Mtra. María Emma Villar González	Titular del Órgano Interno de Control Específico en el CENAGAS	
Arq. Jorge Arturo Mendoza Rodríguez	Suplente del Coordinador de Archivos del CENAGAS	

Estas firmas corresponden al Acuerdo CT/19SE/066ACDO/2024 de la Décima Novena Sesión Extraordinaria del Comité de Transparencia, celebrada el veintiséis de septiembre de dos mil veinticuatro.