Ciudad de México, a 23 de mayo de 2017.
"Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos".

VISTO: El estado que guarda el procedimiento de acceso a la información, derivado de la solicitud presentada el 21 de abril de 2017, a través de la Plataforma Nacional de Transparencia, a la que corresponde el número de folio 0002700094717, y

RESULTANDO

I.- Que mediante la referida solicitud, se requirió la información siguiente:

Descripción clara de la solicitud de información
Solicito una versión pública de toda la documentación generada en el taller "Hacia la Estrategia Nacional de Ciberseguridad" que dio inició el 19 de abril del 2017. Se solicita que entre la información se incluya, mas no se limite a, listas de asistencia, discursos, versiones estenográficas, minutas, presentaciones, anotaciones, memorias, y demás registros presentados y generados en la reunión.

Otros datos para facilitar su localización
La reunión a la que se hace referencia se encuentra comunicada en el post "Hacia la Estrategia Nacional de Ciberseguridad" que se puede encontrar en la siguiente dirección: http://www.gob.mx/mexicodigital/articulos/hacia-la-estrategia-nacional-de-ciberseguridad?idiom=eshttps" (sic)

II.- Que la Unidad de Transparencia turnó, por medios electrónicos, dicha solicitud a la Unidad de Gobierno Digital, unidad administrativa que consideró competente para contar con la información.

III.- Que por comunicado electrónico de 10 de mayo de 2017, la Unidad de Gobierno Digital manifestó a este Comité, que es incompetente para proporcionar la información solicitada por el particular, toda vez que dicho taller fue encabezado por el Gobierno de la República y con el acompañamiento técnico del Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA).

IV.- Que observando en lo conducente las disposiciones vigentes en materia de Archivos, se ha formado el expediente en que se actúa, con las constancias antes enunciadas.

V.- Que de conformidad con lo previsto en el Reglamento del Comité de Información de la Secretaría de la Función Pública, encontrándose en sesión permanente para, entre otros, resolver los procedimientos de su competencia, es de procederse al estudio y análisis de la información aludida en los resultandos precedentes.

CONSIDERANDO

PRIMERO.- Este Comité de Transparencia de la Secretaría de la Función Pública es competente para conocer, dictar los acuerdos que sean necesarios y resolver el presente procedimiento de acceso a la información, de conformidad con los artículos 6o. y 8o. de la Constitución Política de los Estados Unidos Mexicanos; 64, 65, fracción II, 108, 131 y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública; y 6, fracción II, del Reglamento del Comité de Transparencia de la Secretaría de la Función Pública, en relación con el Tercero Transitorio del Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública, publicado en el Diario Oficial de la Federación el 9 de mayo de 2016 y el Segundo Transitorio, segundo párrafo del Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicado en el citado órgano oficial de difusión el 26 de enero de 2017.

SEGUNDO.- En el folio que nos ocupa, se requiere obtener la información señalada en el Resultando I, del presente fallo, misma que se tiene por reproducida para los efectos conducentes.

Al respecto, la Unidad de Gobierno Digital se declaró **incompetente** para proporcionar la información requerida en la solicitud con número de folio 0002700094717.

TERCERO.- Expuesto lo anterior, es importante indicar que si bien es cierto, uno de los objetivos de la Ley Federal de Transparencia y Acceso a la Información Pública, es permitir que toda persona tenga acceso a la información en poder de los sujetos obligados de conformidad con las facultades que les correspondan; también lo es que en términos de lo previsto en el artículo 131, de la Ley Federal de Transparencia y Acceso a la Información Pública, cuando las Unidades de Transparencia determinen la incompetencia por parte de los sujetos obligados, dentro del ámbito de su aplicación, para atender la solicitud de acceso a la información, deberán comunicarlo al solicitante, y señalar al solicitante el o los sujetos obligados competentes.

Lo anterior, en relación con el diverso numeral 65, que en su fracción II, establece que los Comités de Transparencia tendrán, entre otras, la facultad y atribución, de confirmar, modificar o revocar las determinaciones que en materia de incompetencia realicen los titulares de las Áreas de los sujetos obligados.

Expuesto lo anterior, es importante indicar que la Unidad de Gobierno digital de esta Secretaría de la Función Pública, se declaró incompetente para atender la solicitud de información con número de folio 0002700094717, señalando que el taller fue encabezado por el Gobierno de la República, con el acompañamiento del Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA).

En ese contexto, es importante indicar que en el vínculo electrónico:http://www.gob.mx/mexicodigital/articulos/hacia-la-estrategia-nacional-de-ciberseguridad?idiom=eshttps, en el cual se contiene el comunicado oficial que lleva por título "Hacia la Estrategia Nacional de Ciberseguridad", se lee literalmente lo siguiente:

Hacia la Estrategia Nacional de Ciberseguridad

Los días 19 y 20 de abril se llevó a cabo un taller para avanzar en la definición de la Estrategia Nacional de Ciberseguridad de nuestro país. Participaron expertos y representantes de la industria, gobierno, comunidad técnica, entre otros.

El día de hoy concluyó el taller "Hacia la Estrategia Nacional de Ciberseguridad", encabezado por el Gobierno de la República y con el acompañamiento técnico del Programa de Seguridad Cibernética de la Organización de los Estados Americanos (OEA). En esta reunión, que dio inició el 19 de abril, participaron expertos nacionales e internacionales, así como representantes del sector privado, de la industria, sociedad civil, gobierno, órganos autónomos constitucionales, comunidad técnica y academia.

De la imagen arriba inserta, se advierte que quien pudiera tener información respecto del taller titulado "Hacia la Estrategia Nacional de Ciberseguridad", es el sujeto obligado "Presidencia de la República", a través de la Coordinadora de Estrategia Digital Nacional, en razón de que es quien elabora, da seguimiento y evalúa periódicamente la Estrategia Digital Nacional; fomenta la adopción y el desarrollo de tecnologías de la información y comunicación; impulsa el gobierno digital; promueve la innovación, apertura, transparencia, colaboración y participación ciudadana para insertar a México a la sociedad del conocimiento.

Asimismo, esta Dirección General de Transparencia localizó en materia de ciberseguridad, los siguientes vínculos electrónicos, en los cuales puede localizar información de su interés:

https://www.gob.mx/policiafederal/articulos/policia-federal-impulsa-la-campana-ciberseguridad-mexico-2017

De la consulta que se sirva realizar al vínculo electrónico en cita, localizará la siguiente información:

Policía Federal impulsa la campaña Ciberseguridad México 2017

Policía Federal implementa la campaña Ciberseguridad México 2017, con el propósito de fortalecer las capacidades de prevención, reacción y gestión de los problemas vinculados con la seguridad de las redes y la información

La estrategia de seguridad se basa en los ejes de prevención y atención ciudadana; la detección oportuna de amenazas y ataques cibernéticos; así como el fortalecimiento de las capacidades para la investigación de delitos y abusos cibernéticos.

Asimismo, se localizó el siguiente vínculo electrónico:

https://www.sites.oas.org/cyber/Documents/OAS-FIRST%202015%20Report%20SPA.pdf

En el citado vínculo electrónico, localizará información relacionada con el "Taller de Seguridad Cibernética de la OEA", del cual se desprende que en dicho taller participó la Policía Federal, participó en los Grupos de Trabajo, tal y como se advierte de la información que a continuación se inserta:

Grupos de Trabajo

En el segundo y tercer día, los asistentes participaron en tres líneas de trabajo paralelas centradas en temas cibernéticos específicos:

Respuesta a Incidentes

Los Equipos de Respuesta ante Incidentes de Seguridad Cibernética son actores clave en la respuesta nacional a los ataques cibernéticos e incidentes cibernéticos. Son responsables de una serie de tareas, incluyendo el análisis de amenazas, la respuesta y mitigación de ataques, la ayuda a restaurar los sistemas caídos, la emisión de alertas y la investigación de las tendencias de los ataques cibernéticos. Además, los CSIRT suelen compartir información y mejores prácticas entre ellos a través de redes, tales como el Foro de Equipos de Respuesta a Incidentes y la Red Hemisférica de la OEA de CSIRT.

La línea de trabajo de Respuesta a Incidentes abordó temas como las amenazas persistentes avanzadas (APT), el intercambio de información y el Protocolo de Semáforo (TLP), metodologías para la evaluación de la seguridad en el equipo local del cliente, la relación entre los CSIRT y las fuerzas del orden, Robo de Información Personalmente Identificable a granel, ingeniería social, participación del sector privado y estudios de caso de las experiencias de cada país relacionados con la respuesta a incidentes. Las sesiones contaron con la participación de Klaid Mägi, Jefe del CERT-EE, Autoridad del Sistema de Información de Estonia (RIA); Jeimy J. Cano M., Ph.D., Profesor e Investigador de la Universidad de los Andes; Patrick Cain del Grupo de Trabajo Anti-Phishing (APWG); Oliver González, Director General de CERTMX, Policía Federal de México; el Director del CERT Polska, Piotr Kijewski; Rajendra Sigh del Banco Mundial; Fernando Nikitin del Banco Interamericano de Desarrollo (BID); Sean Fouche, Gerente de Tecnología de la Información para la Agencia de Implementación de la Comunidad del Caribe sobre el Crimen y la Seguridad (CARICOM-IMPACS); David Van Duren, Jefe de la oficina del Foro Global sobre Experiencia cibernética; y el Gerente del Programa de Seguridad Cibernética de la OEA, Belisario Contreras.

Los debates evidenciaron que los ataques cibernéticos continuarán aumentando; por lo tanto, es importante que el personal de respuesta a incidentes pueda realizar el triage y priorice las mayores amenazas. Esto requiere un cierto nivel de capacidad analítica. Una forma en que un CSIRT puede mejorar su capacidad de análisis es disponer a mitad del equipo en respuesta a incidentes 24/7 y a la otra mitad en estudio e investigación.

Ciertos ataques cibernéticos, como las campañas de suplantación de identidad (phishing), son cada vez más difíciles de distinguir de los sitios web normales. Una vez que se descarga el malware a un computador, a menudo puede darles a los usuarios una falsa sensación de seguridad,

Por otra parte, también se localizaron los siguientes vínculos electrónicos:

http://www.gob.mx/policiafederal/prensa/impulsan-cns-sector-industrial-estrategia-en-materia-de-ciberseguridad

http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk;jsessionid=0y2xYCJHdQr5wT2s7MQJLpNZ4qCsmn3Tnv8cdh5jH7v1pkWhScP7!1638189857?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1418518

De la consulta que se sirva realizar a los vínculos electrónicos antes citados, localizará la siguiente información, que se estima podría ser de su interés:

Primer vínculo

Impulsan CNS - sector industrial estrategia en materia de ciberseguridad

En el marco de la *XXXVII Convención Anual*, organizada por la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), la Comisión Nacional de Seguridad, a través de la División Científica de la Policía Federal, participó en un coloquio enfocado "Hacia una Estrategia Nacional de Ciberseguridad y Protección de Datos".

El evento estuvo presidido por el Mtro. Víctor Lagunes Soto Ruiz, Jefe de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República, quien contó con especialistas de los sectores público y privado, mismos que expusieron el intercambio de conocimientos, experiencias y buenas prácticas en el combate al cibercrimen.

Por parte de la Policía Federal, participó el Titular de la Coordinación para la Prevención de Delitos Electrónicos, de la División Científica, quien resaltó la importancia de ampliar la colaboración con la industria para que, desde el Gobierno de la República, se dé puntual atención a una creciente demanda ciudadana. "Se trata de un reto compartido", señaló.

Segundo vínculo

IMPULSAN CNS- SECTOR INDUSTRIAL ESTRATEGIA EN MATERIA DE CIBERSEGURIDAD

Comunicado de Prensa No. 479 — Ciudad de México, a 8 de Septiembre de 2016

En el marco de la *XXXVII Convención Anual*, organizada por la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), la Comisión Nacional de Seguridad, a través de la División Científica de la Policía Federal, participó en un coloquio enfocado "Hacia una Estrategia Nacional de Ciberseguridad y Protección de Datos".

El evento estuvo presidido por el Mtro. Víctor Lagunes Soto Ruiz, Jefe de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República, quien contó con especialistas de los sectores público y privado, mismos que expusieron el intercambio de conocimientos, experiencias y buenas prácticas en el combate al cibercrimen.

De todo lo antes expuesto es posible advertir que los sujetos obligados que podrían contar con la información de su interés son: la Policía Federal, Presidencia de la República y la Secretaría de Gobernación a través de la Comisión Nacional de Seguridad, por lo que se sugiere dirija su requerimiento de información a dichos sujetos obligados a través de los siguientes vínculos electrónicos:

https://www.infomex.org.mx/gobiernofederal/home.action

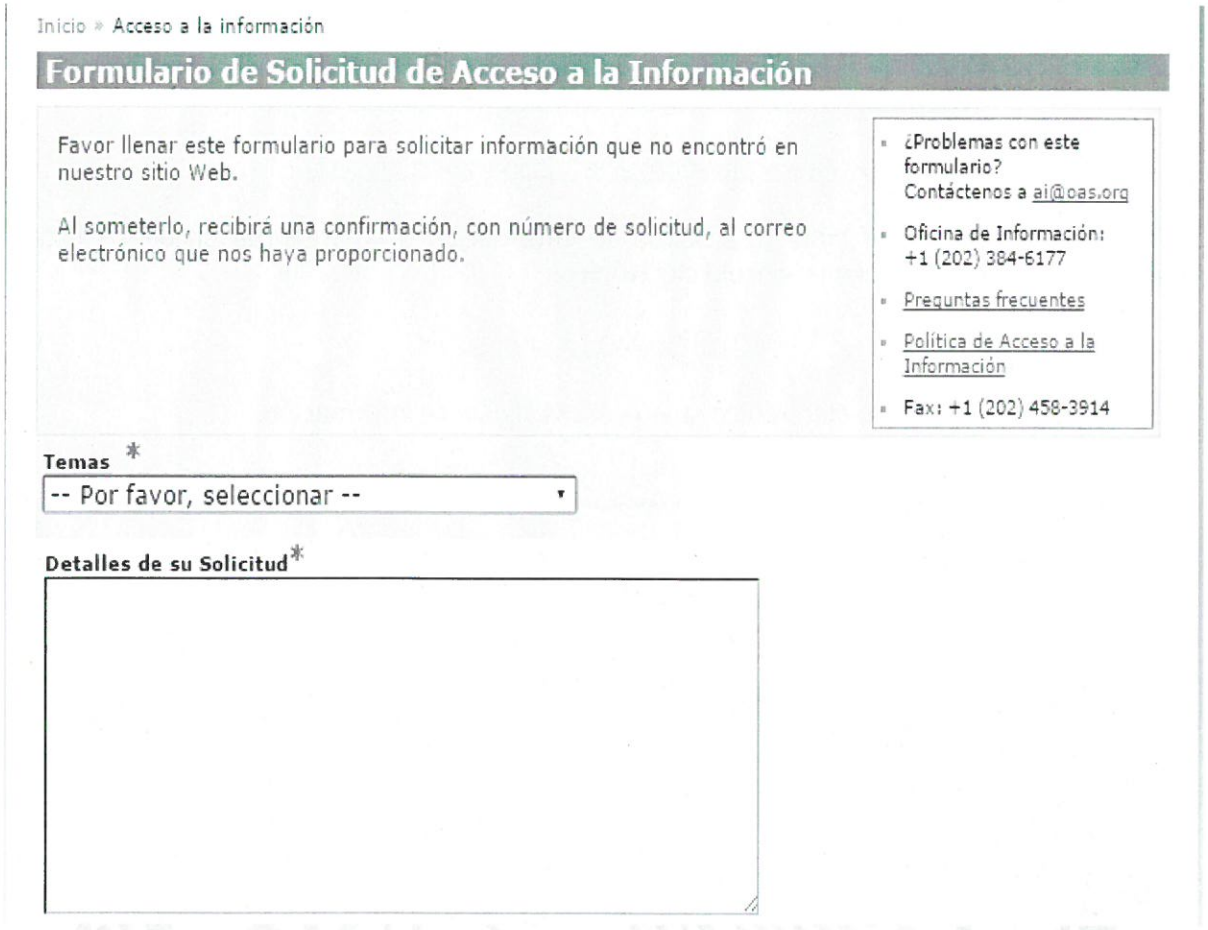
http://www.plataformadetransparencia.org.mx/

Inclusive, se sugiere dirija su solicitud de información a la Organización de los Estados Americanos, a través del siguiente vínculo electrónico:

http://www.oas.org/es/

Al abrir dicho vínculo electrónico, aparecerá la siguiente información:

Al dar click en el rubro "Temas", se desplegará dicha información, posteriormente deberá dar click en el rubro "Acceso a la Información", en la cual se advierte lo siguiente:



Inicio » Acceso a la información

Formulario de Solicitud de Acceso a la Información

Favor llenar este formulario para solicitar información que no encontró en nuestro sitio Web.

Al someterlo, recibirá una confirmación, con número de solicitud, al correo electrónico que nos haya proporcionado.

- ¿Problemas con este formulario? Contáctenos a ai@oas.org
- Oficina de Información: +1 (202) 384-6177
- Preguntas frecuentes
- Política de Acceso a la Información
- Fax: +1 (202) 458-3914

Temas *

-- Por favor, seleccionar --

Detalles de su Solicitud*

En dicha página, deberá llenar los rubros que ahí aparecen a efecto de solicitar la información de su interés.

Finalmente, no se omite mencionar que de conformidad con el "*ACUERDO que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias*", en su artículo 30, establece literalmente lo siguiente:

"**Artículo 30.-** La interpretación del presente Acuerdo, como de su Anexo Único, para efectos administrativos, así como la resolución de los casos no previstos en el mismo, corresponderá:

(. . .)

II. **En materia de seguridad de la información considerada de seguridad nacional, a la Secretaría de Gobernación, a través del Centro**."

En relación con lo anterior, el artículo 2 del citado acuerdo, es del tenor literal siguiente:

Artículo 2.- Para los efectos del presente Acuerdo, se entiende por:

(. . .)

VII. **Centro**: el Centro de Investigación y Seguridad Nacional, **órgano desconcentrado de la Secretaría de Gobernación**;

Con lo anterior se corrobora que los sujetos obligados referidos podrían contener la información requerida en la solicitud identificada con el número de folio 0002700094717.

Por lo expuesto y fundado, es de resolverse y se

RESUELVE

PRIMERO.- **Se confirma** la **incompetencia** de este sujeto obligado, para atender el requerimiento de información formulado por el particular en la solicitud con número de folio 0002700094717.

SEGUNDO.- Asimismo, se informa al solicitante de acceso a la información, que se encuentra a su disposición el teléfono 01-800-TELINAI (835-4324) y el correo electrónico vigilancia@inai.org.mx para que en su caso, comunique cualquier incumplimiento a la resolución de mérito.

No obstante lo anterior, es de señalar que se encuentran expeditos sus derechos para hacerlos valer ante el Poder Judicial de la Federación, si subsistiera algún aspecto no resuelto por el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos respecto a su recurso de revisión, o si en el caso, el cumplimiento que se otorga a través de la presente resolución le irroga detrimento a sus derechos.

TERCERO.- Notifíquese por conducto de la Dirección General de Transparencia de esta Secretaría de la Función Pública, para los efectos conducentes, como fue señalado en el Considerando Tercero, al solicitante y a la unidad administrativa señalada en esta resolución.

Así, por unanimidad de votos lo acordaron los integrantes del Comité de Transparencia de la Secretaría de la Función Pública, Tanya Marlenne Magallanes López, Directora General de Transparencia y Presidenta del Comité y Roberto Carlos Corral Veale, Director General Adjunto de Control y Evaluación, como suplente del Contralor Interno y Miembro de este Comité.

Mtra. Tanya Marlenne Magallanes López
PRESIDENTA

Lic. Roberto Carlos Corral Veale
REPRESENTANTE DE LA CONTRALORÍA INTERNA

Elaboró NAMU
Revisó: SADB