INSTITUTO NACIONAL ELECTORAL

INE-CT-R-0122-2024

Resolución del Comité de Transparencia (CT) del Instituto Nacional Electoral (INE) en atención a la solicitud de acceso a la información 330031424000969 (UT/24/00912).

Apreciable persona solicitante:

La presente resolución da respuesta a su solicitud de acceso a la información. A efecto de explicarla con mayor facilidad, se divide conforme al siguiente índice.

Contenido

INE-CT-R-0122-2024

2. Atención de la solicitud
A. Cuáles son los datos de su solicitud

a. **Nombre de la persona solicitante:** C. Ernesto Aroche
b. **Fecha de ingreso de la solicitud de información:** 26 de febrero de 2024
c. **Medio de ingreso:** Plataforma Nacional de Transparencia (PNT)
d. **Folio de la PNT:** 330031424000969
e. **Folio interno asignado:** UT/24/00912
f. **Información solicitada:**

> "1. *Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2014 a la fecha.*
> *2. Solicito que se me informe la fecha exacta de cada uno de los ataques, su lugar de origen detectado y tipo de ataque (denegación de servicio, fuerza bruta, etc).*" **(sic)**
>
> **[Numeración propia]**

B. Qué hicimos para atenderla

La Unidad de Transparencia **(UT)** analizó su solicitud y la turnó a la Unidad Técnica de Servicios de Informática **(UTSI)** y a la Unidad Técnica de Transparencia y Protección de Datos Personales – Dirección de Políticas de Transparencia **(UTTyPDP - DPT)**, quienes respondieron conforme a sus competencias.

Las gestiones se describen en el siguiente cuadro y las respuestas de las áreas forman parte integral de este documento.

ÓRGANOS CENTRALES					
Con-sec.	**Áreas**	**Fechas de turno**	**Fecha(s) de respuesta**	**Medio de respuesta (Infomex-INE, correo electrónico, oficio)**	**Tipo de información**
1.	**UTSI**	26/02/2024 Dentro del plazo 06/03/2024 Reasignación de turno	04/03/2024 (Solicitud de ampliación de plazo) Dentro del plazo 13/03/2024 Dentro del plazo	Infomex-INE y oficio de respuesta sin número	**Información pública (punto 1)** **Reserva temporal total (punto 2)**

ÓRGANOS CENTRALES					
Con-sec.	**Áreas**	**Fechas de turno**	**Fecha(s) de respuesta**	**Medio de respuesta (Infomex-INE, correo electrónico, oficio)**	**Tipo de información**
2.	**UTTyPDP - DPT**	26/02/2024 Dentro del plazo	28/02/2024 Dentro del plazo	Infomex-INE y oficio de respuesta sin número	**Incompetencia (totalidad de la solicitud)**
					Máxima publicidad (totalidad de la solicitud)
					Orientación (totalidad de la solicitud)
Fecha de gestión más reciente: 13/03/2024					

* Las áreas solo se pronuncian por los puntos para los que detentan atribuciones.

C. Ampliación de plazo

El 14 de marzo de 2024, la UT notificó a la persona solicitante, a través de la PNT y correo electrónico, el acuerdo INE-CT-ACAM-0009-2024, mediante el cual, el CT aprobó la ampliación del plazo previsto en los artículos 132 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), 135 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) y 30 del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública (Reglamento), aprobado por el Consejo General del INE el 26 de agosto de 2020.

D. Suspensión de plazos

De conformidad con el Estatuto del Servicio Profesional Electoral Nacional y del Personal de la Rama Administrativa del Instituto Nacional Electoral, el acuerdo INE-CT-ACG-0002-2023 y la circular INE/DEA/8/2024, se suspendieron los plazos en materia de Transparencia, Acceso a la Información y Protección de Datos Personales el día 18 de marzo de 2024, reanudándose el 19 de marzo de la presente anualidad.

3. Acciones del CT

El 22 de marzo de 2024, la Secretaría Técnica (ST) del CT, por instrucciones del Presidente de dicho órgano convocó a sus integrantes y a las áreas que respondieron, para discutir, entre otros asuntos la presente resolución.

A. Competencia

El CT es competente para confirmar, modificar o revocar las manifestaciones de incompetencia, ampliaciones de plazo, declaratorias de inexistencia y clasificaciones de información de las áreas, en términos de lo dispuesto en los artículos 44 fracciones II y III, y 137 de la LGTAIP; 65 fracciones II y III, 135 y 140 de la LFTAIP; y 24 párrafo 1, fracción II del Reglamento.

B. Análisis de la clasificación y de la manifestación

Las áreas responsables de atender la solicitud precisaron que parte de la información debe ser protegida por alguna razón **(reserva temporal total)** y que no detentan atribuciones para contar con ella **(incompetencia),** por lo que el CT verificó que la **clasificación y manifestación** contengan los elementos para confirmar, modificar o revocar el sentido.

A fin de facilitar el análisis, se realiza la precisión correspondiente respecto de lo requerido por la persona solicitante.

Punto 1 "*Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2014 a la fecha."* **(sic)**			
Qué área respondió	**Cómo respondió**	**El área explicó por qué respondió en ese sentido (motivación)**	**El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)**
UTSI	**Información pública**	Sí, el área precisa que por lo que hace al presente cuestionamiento, se precisa que por "ataque" se entenderá un **intento** (deliberado o no) por vulnerar la integridad, disponibilidad o confidencialidad de los sistemas informáticos del INE. Cabe precisar que, en todos los casos, los intentos fueron detectados y contenidos por los distintos mecanismos de seguridad de la Red Nacional	Sí, de conformidad con lo establecido en los artículos: "*6, tercer párrafo de la Constitución Política de los Estados Unidos Mexicanos; 30 de la Ley General de Instituciones y Procedimientos Electorales; 1, 4, 19, 20, 101 segundo párrafo, 108 último párrafo, 113 fracción VII y 129 de la Ley General de Transparencia y Acceso a la Información Pública 110 fracción VII y 130, cuarto párrafo de la Ley Federal de*

INE-CT-R-0122-2024

<table>
<tr><td colspan="4">Punto 1

“Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2014 a la fecha.” (sic)</td></tr>
<tr><td>Qué área respondió</td><td>Cómo respondió</td><td>El área explicó por qué respondió en ese sentido (motivación)</td><td>El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)</td></tr>
<tr><td></td><td></td><td>de Informática del Instituto (RedINE), por lo que ninguno de ellos fue exitoso. En este sentido, se entrega la información con la que se cuenta, es decir, el número de intentos de ataques durante el periodo comprendido entre el 1 de enero de 2014 al 26 de febrero de 2024.

A continuación, se presenta una tabla de las cantidades por año.

<table><tr><th>Año</th><th>Número de intentos de ataques</th></tr><tr><td>2014</td><td>51</td></tr><tr><td>2015</td><td>471</td></tr><tr><td>2016</td><td>226</td></tr><tr><td>2017</td><td>1,018</td></tr><tr><td>2018</td><td>1,792,743</td></tr><tr><td>2019</td><td>2,583,631</td></tr><tr><td>2020</td><td>3,779,721</td></tr><tr><td>2021</td><td>2,970,477</td></tr><tr><td>2022</td><td>2,309,631</td></tr><tr><td>2023</td><td>3,078,035</td></tr><tr><td>1 de enero al 26 de febrero de 2024</td><td>2,616,121</td></tr><tr><td>Total</td><td>19,132,125</td></tr></table></td><td>Transparencia y Acceso a la Información Pública; 211 bis 1 y 211 bis 2 del Código Penal Federal; 1; 2, párrafo 1, fracción XXXI; 20, fracción V; 24, párrafos 1 y 2, fracciones I y III; 27, párrafo 1; 28, párrafo 3; 29, párrafo 1; 32; 35 y 36 del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública; Lineamientos vigésimo sexto y trigésimo tercero de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.” (sic)</td></tr>
<tr><td>UTTyPDP</td><td>Incompetencia**</td><td>Sí, el área informa que el área es incompetente para atender la solicitud que nos ocupa, toda vez que, de acuerdo con el artículo 22, numeral 2, del</td><td>Sí, de conformidad con lo establecido en los siguientes artículos:</td></tr>
</table>

INE-CT-R-0122-2024

Punto 1 "*Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2014 a la fecha."* **(sic)**			
Qué área respondió	**Cómo respondió**	**El área explicó por qué respondió en ese sentido (motivación)**	**El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)**
		Reglamento, la información solicitada no se genera al desarrollar las atribuciones de dicha Dirección.	"*22, numeral 2 y 28, numeral 10, del Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública*." **(sic)**
	Máxima publicidad	Sí, el área atendiendo al principio de máxima publicidad establecido en los artículos 6, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), y 4 del Reglamento de Transparencia, hace del conocimiento que, en la página denominada NormaINE (https://norma.ine.mx/) del Instituto se pueden consultar contenidos que aluden a seguridad informática en el Instituto que podrían ser de interés a la persona peticionaria.	
	Orientación	Sí, el área sugiere turnar la solicitud a la UTSI, quien pudiera tener la información, ya que entre sus funciones esta, establecer y aplicar reglas, procedimientos y estándares en materia de seguridad informática, así como coordinar la aplicación de auditorías en la materia.	

INE-CT-R-0122-2024

Punto 2 "*Solicito que se me informe la fecha exacta de cada uno de los ataques, su lugar de origen detectado y tipo de ataque (denegación de servicio, fuerza bruta, etc).*" **(sic)**			
Qué área respondió	**Cómo respondió**	**El área explicó por qué respondió en ese sentido (motivación)**	**El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)**
UTSI	**Reserva temporal total***	Sí, el área señala que la información requerida sobre los detalles **como lo son la fecha exacta, lugar de origen y tipo de ataque**, no pueden ser proporcionados, ya que de ser otorgados pondría en riesgo la seguridad Nacional Informática de los sistemas del INE.	Sí, de conformidad con lo establecido en los artículos: "*6 de la Constitución Política de los Estados Unidos Mexicanos; 106, fracción I, 113 fracción VIII de la Ley General de Transparencia y Acceso a la Información Pública.; 98 fracción I, 110 fracción VIII de la Ley Federal de Transparencia y Acceso a la Información Pública; 305, numeral 1 de la Ley General de Instituciones y Procedimientos Electorales; 18; 28; 29 del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública; 338, numeral 2 inciso a) y 340, numeral 1 del Reglamento de Elecciones del Instituto Nacional Electoral; 66 numeral 1 del Reglamento Interior del Instituto Nacional Electoral.; Lineamiento vigésimo séptimo, fracciones I, II, III y IV de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la información Pública y Protección de Datos Personales*." **(sic)**

INE-CT-R-0122-2024

Punto 2 "*Solicito que se me informe la fecha exacta de cada uno de los ataques, su lugar de origen detectado y tipo de ataque (denegación de servicio, fuerza bruta, etc).*" **(sic)**			
Qué área respondió	**Cómo respondió**	**El área explicó por qué respondió en ese sentido (motivación)**	**El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)**
UTTyPDP	**Incompetencia****	Sí, el área informa que el área es incompetente para atender la solicitud que nos ocupa, toda vez que, de acuerdo con el artículo 22, numeral 2, del Reglamento, la información solicitada no se genera al desarrollar las atribuciones de dicha Dirección.	Sí, de conformidad con lo establecido en los siguientes artículos: "*28, numeral 10 y 29, párrafo 3, fracción VII, del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública y 68, del Reglamento Interior de este Instituto y 44, numeral 1, inciso d) del Reglamento Interior del Instituto Nacional Electoral*." **(sic)**
	Máxima publicidad	Sí, el área atendiendo al principio de máxima publicidad establecido en los artículos 6, de la Constitución Política de los Estados Unidos Mexicanos, y 4 del Reglamento de Transparencia, hace del conocimiento que, en la página denominada NormaINE (https://norma.ine.mx/) del Instituto se pueden consultar contenidos que aluden a seguridad informática en el Instituto que podrían ser de interés a la persona peticionaria.	
	Orientación	Sí, el área sugiere turnar la solicitud a la UTSI, quien pudiera tener la información, ya que entre sus funciones esta, establecer y aplicar reglas, procedimientos y estándares en materia de seguridad informática, así como coordinar la aplicación de auditorías en la materia.	

* Toda vez que el área **UTSI** clasificó como reserva temporal total, respecto del punto 2 de la solicitud, dicha clasificación será analizada por el CT en el apartado siguiente.

Debido a que la manifestación de incompetencia sustentada por el área **UTTyPDP-DPT, no invoca la participación de un sujeto obligado distinto al INE, no existe materia para el análisis.

Consideraciones del CT

Reserva temporal total

El área **UTSI**, clasificó como **reserva temporal total los detalles de los ataques digitales como lo son la fecha exacta, lugar de origen y tipo de ataque**.

Lo anterior, en virtud de que la información solicitada referente a los detalles de los ataques digitales, de ser otorgados pondría en riesgo la seguridad Nacional Informática de los sistemas del INE.

Por tales motivos se considera como reserva temporal total, de conformidad con los artículos 113 fracción VII de la LGTAIP; y 110 fracción VII de la LFTAIP.

Para obtener mayores elementos, el CT a través de la ST, revisó la respuesta enviada por el área, cuyos resultados, se comparten a continuación:

Revisión de la información

<table>
<tr><td>Conclusión de la Secretaría Técnica del Comité de Transparencia:</td><td colspan="5">Es factible confirmar la clasificación.</td></tr>
<tr><td rowspan="2">Propuesta de clasificación del área:</td><td rowspan="2">Reserva temporal total</td><td rowspan="2">Plazo de clasificación</td><td>5</td><td>0</td><td>0</td></tr>
<tr><td>Años</td><td>Meses</td><td>Días</td></tr>
<tr><td>Folios PNT:</td><td>330031424000969</td><td>Medio de envío de la información clasificada:</td><td colspan="3">INFOMEX-INE</td></tr>
<tr><td>Folios internos:</td><td>UT/24/00912</td><td>¿El área envió la totalidad de la información o una muestra?</td><td colspan="3">El área envía explicación</td></tr>
<tr><td>Área que envía la información clasificada:</td><td>UTSI</td><td rowspan="2">Volumen de la totalidad o muestra:</td><td colspan="3" rowspan="2">El área envía explicación</td></tr>
<tr><td>Fecha de recepción de</td><td>13/03/2024</td></tr>
</table>

la información clasificada en la UT:			
Número de RA[1] formulados:	N/A[2]	**Número de RII[3] formulados:**	N/A

1. Descripción general de la información

El área **UTSI** señaló lo siguiente:

> *"Ahora bien, con relación al presente cuestionamiento, se informa a la persona solicitante que la información correspondiente a **todos** los **detalles** de los intentos de ataques es información que, previamente ha sido clasificada como temporalmente reservada mediante las resoluciones emitidas por el Comité de Transparencia (CT) del Instituto Nacional Electoral, como a continuación se precisa:*

Resolución del CT	*Periodo de la información que se reservo*	*Fecha de inicio de clasificación*	*La clasificación se encuentra vigente hasta.*
INE-CT-R-0072-2021	*La presente resolución deriva del RRA 12927/20, mediante la cual se determina reservar la información relativa a los intentos de ataques cibernéticos como lo es: el país detectado, fecha y hora de detección, dirección IP origen detectada, dirección IP/equipo/servicio destinado detectado y tipo de patrón identificado, correspondiente a la información relativa a los intentos de ataques cibernéticos del 1 de enero de 2015 al 1 de octubre de 2020.*	*25 de marzo de 2021.*	*25 de marzo de 2026.*

[1] Requerimiento de Aclaración (RA).
[2] No Aplica (NA).
[3] Requerimiento Intermedio de Información (RII).

Resolución del CT	*Periodo de la información que se reservo*	*Fecha de inicio de clasificación*	*La clasificación se encuentra vigente hasta.*
INE-CT-R-0225-2021	*Información relativa a los intentos de ataques cibernéticos del 2 de octubre de 2020 al 7 de julio de 2021.*	*5 de agosto de 2021.*	*5 de agosto de 2026.*
INE-CT-R-0325-2021	*Información relativa a los intentos de ataques cibernéticos del 8 de julio de 2021 al 19 de noviembre de 2021.*	*2 de diciembre de 2021.*	*2 de diciembre de 2026.*

En este sentido, la información requerida por la persona solicitante y correspondiente a los periodos antes descritos se encuentra reservada, por lo tanto, no puede ser proporcionada, ya que los motivos que dieron origen a su clasificación subsisten actualmente, y las temporalidades por las que fueron aprobadas las clasificaciones por el Comité de Transparencia del Instituto, siguen vigentes.

*En este orden de ideas, por cuanto hace a la información solicitada respecto de los periodos del **01 de enero al 31 de diciembre de 2014 y del 20 de noviembre de 2021 al 26 de febrero de 2024**, fecha en la que se recibió la presente solicitud, y considerando la clasificación de los meses y años previos, resulta necesario clasificar dicha información en los periodos señalados como temporalmente reservada.*

*Debido a lo anterior, se hace del conocimiento de la persona solicitante que la información requerida sobre los detalles **como lo son la fecha exacta, lugar de origen y tipo de ataque**, no le pueden ser proporcionados, ya que de ser otorgados pondría en riesgo la seguridad Nacional Informática de los sistemas del Instituto Nacional Electoral. Al respecto, dicha información requerida por la persona solicitante ya ha sido clasificada previamente como reservada y está relacionada con el detalle de los pormenores de los intentos de ataques como a continuación se ejemplifica:*

País detectado	*Fecha y hora de detección*	*Dirección IP Origen detectada*	*Dirección IP/Equipo/Servicio destino detectado* *(IP/Equipo/Servicio que pretendió ser afectado)*	*Tipo de Patrón Identificado*

Se refiere a la posible ubicación geográfica desde dónde se identifica la IP de Origen detectada.	*Estampa de tiempo asociada con algún evento.*	*Dirección IP detectada desde dónde se identifica el origen de algún evento.*	*Dirección IP/equipo/servicio identificado como el objetivo de algún evento.*	*Sucesión de términos para la identificación de algún evento.*

Glosario

IP: *Acrónimo en inglés de Internet Protocol (Protocolo de Internet). Método por el cual la información es enviada de una computadora a otra en el Internet.*[4]
Internet*: Es una red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP.*[5]
TCP/IP*: También conocido como Conjunto de Protocolos de Internet en el cual el Protocolo de Control de Transferencia y el Protocolo de Internet son importantes. Es el protocolo básico de comunicación de Internet y también para redes privadas.*[6]
Evento[7]*: Acontecimiento observable de un sistema informático. Lo anterior, de acuerdo con el estándar estadounidense NIST IR 7298 Revisión 3 publicada por el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) de los Estados Unidos de Norteamérica.*

Por otra parte, cabe precisar que, de acuerdo con el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés), un "ciberataque" se define como:

Intento *de obtener acceso no autorizado a servicios, recursos o información del sistema, o un* ***intento*** *de comprometer la integridad, disponibilidad o confidencialidad del sistema, a través del ciberespacio, con el fin de:*

- *Interrumpir, deshabilitar, destruir, o controlar un entorno/infraestructura informática; o*
- *Destruir la integridad de los datos; o*
- *Robar información controlada*[1]*.*

Cada ataque se traduce en un intento (deliberado o no) por vulnerar la integridad, disponibilidad o confidencialidad de los sistemas informáticos del Instituto

[4] Fuente: https://www.cert.org.mx/diccionario/

[5] ídem
[6] ibidem
[7] https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final
[1] Computer Security Resource Center. Glossary. National Institute of Standars and Technology. Disponible en: https://csrc.nist.gov/Glossary/?term=3015#AlphaIndexDiv

Nacional Electoral, y no de los servidores que los albergan. Cabe señalar que, en todos los casos, los intentos fueron detectados y contenidos por los distintos mecanismos de seguridad de la Red Nacional de Informática del Instituto (RedINE), por lo que ninguno de ellos fue exitoso.

En este sentido, a continuación, se exponen las razones y motivos de la reserva en comento:

Prueba de daño

Como lo señala el artículo 108, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública se requiere de la aplicación de la prueba de daño, cuyos elementos, en correlación con el numeral Trigésimo tercero de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, se exponen a continuación:

I. Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;

La causal de reserva encuadra en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el numeral Vigésimo sexto, de los mencionados Lineamientos generales.

Vigésimo sexto. *De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que* ***obstruya la prevención de delitos*** *al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*

Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:

- **I.** *La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;*
- **II.** *Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y*
- **III.** *Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal.*

II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría

un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;

Como lo establece el artículo 30 de la Ley General de Instituciones y Procedimientos Electorales (LGIPE), son fines de este Instituto, entre otros: contribuir al desarrollo de la vida democrática, asegurar a la ciudadanía el ejercicio de los derechos políticos-electorales y vigilar el cumplimiento de sus obligaciones, garantizar la celebración periódica y pacífica de las elecciones para renovar a los integrantes de los Poderes Legislativo y Ejecutivo de la Unión, así como ejercer las funciones que la Constitución le otorga en los procesos electorales locales.

De lo anterior se desprende que las funciones que, tanto constitucional como legalmente, le han sido conferidas a este Instituto, le son exclusivas, es decir, no hay algún otro organismo en el país que ejecute dichas funciones, mismas que se desarrollan cotidianamente y que no necesariamente se circunscriben a los procesos electorales federales o locales, sino que se desarrollan día con día con motivo de sus funciones.

Por ello, el INE se ha dado a la tarea de desarrollar diversos sistemas informáticos que dan soporte al ejercicio de sus funciones, por lo que brindar la información solicitada colocaría en estado de riesgo la operatividad del INE y con ello el ejercicio de las mencionadas funciones.

*Por un lado, se encuentra el derecho de acceso a la información de la persona solicitante; por otro, la seguridad informática de los sistemas del INE con los que cumple sus fines, así como prevenir o evitar la conducta criminal, toda vez que, de otorgar la información relativa a los **todos los detalles** de los intentos de ataques cibernéticos como lo es la **fecha exacta, lugar de origen detectado y tipo de ataque**, se estaría potencializando el riesgo de que se lleven ataques cibernéticos, así como el acceso ilícito a sistemas y equipos informáticos. Como se ha señalado, dar a conocer información como la que se solicita, implica otorgar elementos que podrían eventualmente hacer vulnerables los sistemas con que cuenta este Instituto y sobre los cuales se apoya para el ejercicio de sus funciones.*

En ese sentido, se considera que la necesidad de restringir temporalmente el acceso a la información que se pide es mayor al interés de la persona solicitante en conocer los datos que requirió. Con ello se ponderan los fines del INE en el desarrollo de la vida democrática del país, por encima del derecho de acceso a la información de una sola persona; desde luego, ambos derechos son importantes y deben ser respetados, sin embargo, dadas las características de la información que se solicita, se considera necesario velar temporal y particularmente uno, por encima del otro, pues este Instituto debe proteger el interés público por encima del particular.

*En caso de otorgar la información referente a **todos los detalles** de los intentos de ataques cibernéticos ocurridos en cualquiera de sus plataformas o sistemas, específicamente lo relacionado a la **fecha exacta, lugar de origen detectado y***

tipo de ataque, *se estarían exponiendo a los mecanismos, herramientas y sistemas con los que este Instituto cuenta para garantizar la seguridad informática de todos los procesos sistematizados que implementa y ejecuta, así como su funcionamiento, situación que pondría en riesgo la capacidad del INE para cumplir con sus funciones, lo que al ponderarlo frente el derecho a la información del solicitante, lo supera en las consecuencias que se puedan generar.*

En consecuencia, se considera que el riesgo al que se expondrían la totalidad de los sistemas informáticos del INE y, por ende, la propia capacidad del Instituto para llevar a cabo sus funciones rebasa los intereses jurídicos tutelados de acceso a la información, pues se hace hincapié en que la información relativa a ***todos los detalles*** *de los intentos de ataques como lo son la* ***fecha exacta, el lugar de origen detectado y el tipo de ataque****, guardan relación con los mismos y, en ese sentido, se pondrían en riesgo las funciones del INE, pues son parte de la base con la que lleva a cabo sus tareas cotidianas. Asimismo, el otorgar dicha información puede obstruir en la prevención de delitos como lo es el* ***acceso ilícito a sistemas y equipos de informática*** *establecido en el título noveno del Código Penal Federal, en el cual se señala lo siguiente:*

TITULO NOVENO
Revelación de secretos y acceso ilícito a sistemas y equipos de informática
…
Capitulo II
Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
(…)

Por lo que, de otorgarse la información, se estarían proporcionando elementos que facilitarían a un potencial atacante el identificar la ruta de menor resistencia en un hipotético caso de que se buscará vulnerar la seguridad de los activos informáticos del INE y con ello acceder de manera ilícita a sistemas y equipos de informática.

III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate;

Como se ha manifestado, la difusión de la información solicitada pone en riesgo evidente la estabilidad de los sistemas informáticos del Instituto, y con ello la operación institucional de este organismo, así como propiciar el delito de acceso ilícito a sistemas y equipos de informática. En consecuencia, para cumplir y salvaguardar los fines de este Instituto se considera necesario reservar la información con el objeto de contribuir a la vida democrática del país y asegurar a los ciudadanos el ejercicio de sus derechos políticos electorales.

En este sentido, las soluciones para llevar a cabo la mitigación de ataques de denegación de servicio cuentan con una capacidad finita en los recursos de cómputo y de ancho de banda requeridos para realizar las actividades de revisión y depuración del tráfico de red.

De esta manera, al realizar el dimensionamiento de las soluciones de protección contra ataques volumétricos, se realizan las estimaciones necesarias para contar con el software y el hardware que permita identificar y detener un posible ataque de una volumetría estimada; pero también se debe considerar una solución que tenga un costo – beneficio operativo y económico aceptable, lo que implica necesariamente contar con límites definidos por la marca y el modelo de la solución seleccionada.

En este sentido, se considera que tener acceso a esta información facilitaría a un potencial atacante el identificar la ruta de menor resistencia en un hipotético caso de que se buscara vulnerar la seguridad de los activos informáticos del INE.

*Por lo que, difundir la información solicitada provocaría un **riesgo real** de recibir intentos de ataques cibernéticos directamente enfocados en tratar de evitar las medidas de seguridad informática que se hubieran descrito al hacer pública la información solicitada, es decir, la información que se solicita puede ser utilizada para desarrollar ataques específicamente diseñados para intentar vulnerar los mecanismos, herramientas, infraestructura y sistemas con los que cuenta el INE, afectando así las actividades cotidianas del Instituto, sean éstas relacionadas o no, con los procesos electorales; por lo tanto, se considera que esas agresiones serían potencialmente más riesgosas que aquellas que se pudieran generar sin el conocimiento exacto de las características de los mecanismos, herramientas y sistemas de protección y defensa con los que cuenta el INE. Asimismo, de conformidad con lo establecido en la resolución recaída el Recurso de Revisión **RRA 12927/20** desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es por ello que después del análisis realizado por esta*

Unidad, el dar a conocer información relativa a los intentos de ataques cibernéticos como lo es la fecha exacta, lugar de origen detectado y tipo de ataque, se estaría potencializando el riesgo de que se lleven ataques cibernéticos, así como el acceso ilícito a sistemas y equipos informáticos, por lo que con la reserva de la información se pretende prevenir esta conducta criminal.

Asimismo, el recibir intentos de ataques directamente enfocados podrían comprometer la estabilidad de los sistemas informáticos, la operatividad del propio Instituto, e incluso, se podría comprometer el cumplimiento de los principios que rigen las actividades del INE, es decir, la certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, así como propiciar el acceso ilícito a sistemas y equipos de informática.

IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;

Otorgar la información solicitada podría implicar colocar en un estado de vulnerabilidad permanente a los sistemas informáticos del INE, ya que se trata de información sensible que podría brindar elementos para una posible amenaza o vulneración de los propios sistemas, lo que desencadenaría propiciar el delito de acceso ilícito a sistemas y equipos de informática, por lo que con la reserva de la información se pretende prevenir esta conducta criminal.

*Asimismo, resulta importante destacar que el riesgo **real** antes descrito, mismo que surgiría a partir de la divulgación de información solicitada, es **demostrable**, ya que además de los ataques que ha sufrido el INE y que gracias a las medidas de seguridad con las que se cuenta y de las que de entregarse la información se pondrían en estado de vulnerabilidad y riesgo real, existen numerosos ejemplos de acciones de este tipo (intentos de ataques cibernéticos) que han causado estragos a diversos sistemas informáticos en todo el mundo, y al mismo tiempo **identificable**, ya que de antemano se conocen algunos de los principales tipos en los que se pueden clasificar los referidos ataques cibernéticos. Si bien es cierto que los daños provocados varían en función de la complejidad del ataque y la intención con la que son desarrollados, se considera relevante destacar que cualquier amenaza a la que se encuentre expuesto el INE, se potencializa si se da a conocer el origen de estos y, las características técnicas y de funcionamiento de los mecanismos y herramientas diseñados e implementados para garantizar la seguridad informática del mismo.*

De manera tal que, compartir esta información con un tercero pone en riesgo real la seguridad institucional, ya que coloca al INE en un riesgo latente de sufrir intentos de ataques o accesos no autorizados e ilícitos a la red institucional y a los sistemas de este órgano nacional, ya que – en términos de seguridad informática– todos los intentos de ataques dan inicio con una etapa de reconocimiento durante la cual el atacante hace uso de diversas técnicas que tienen como propósito recopilar y consolidar información técnica acerca de los sistemas que se pretenden atacar, así como de la infraestructura tecnológica subyacente.

Así, se puede decir que, a partir de la ejecución de técnicas de reconocimiento, el atacante, entre otros, está en posibilidad de reconstruir los planos arquitectónicos de la red de datos, así como los componentes de software que coexiste en dicha red de datos y documentar las versiones de dichos componentes. Esta información permite al atacante buscar componentes que presenten vulnerabilidades a partir en bases de datos especializadas (ejemplo: National Vulnerability Database, https://nvd.nist.gov/) así como hacerse de herramientas de ataque (exploits) que permiten aprovechar dichas vulnerabilidades para afectar la seguridad de los activos informáticos afectados.

Por lo anterior, revelar esa información materializaría el riesgo real de afectaciones a la integridad, estabilidad y permanencia de las actividades de este órgano electoral y potencializaría las posibilidades de propiciar el delito de acceso ilícito a sistemas y equipos de informática.

En este orden de ideas, el artículo 30 de la LGIPE establece los fines de este Instituto, a saber:

Artículo 30.

1. *Son fines del Instituto:*
    a) *Contribuir al desarrollo de la vida democrática;*
    b) *Preservar el fortalecimiento del régimen de partidos políticos;*
    c) *Integrar el Registro Federal de Electores;*
    d) *Asegurar a los ciudadanos el ejercicio de los derechos político-electorales y vigilar el cumplimiento de sus obligaciones;*
    e) *Garantizar la celebración periódica y pacífica de las elecciones para renovar a los integrantes de los Poderes Legislativo y Ejecutivo de la Unión, así como ejercer las funciones que la Constitución le otorga en los procesos electorales locales;*
    f) *Velar por la autenticidad y efectividad del sufragio;*
    g) *Llevar a cabo la promoción del voto y coadyuvar a la difusión de la educación cívica y la cultura democrática;*
    h) *Garantizar la paridad de género y el respeto de los derechos humanos de las mujeres en el ámbito político y electoral, y*
    i) *Fungir como autoridad única para la administración del tiempo que corresponda al Estado en radio y televisión destinado a los objetivos propios del Instituto, a los de otras autoridades electorales y a garantizar el ejercicio de los derechos que la Constitución otorga a los partidos políticos en la materia.*

2. *Todas las actividades del Instituto se regirán por los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad, objetividad, paridad, y se realizarán con perspectiva de género.*

*En este orden de ideas, el riesgo que pudiera surgir a partir de la divulgación de la información es **real y tangible**, tan es así que el propio Código Penal Federal,*

establece delitos específicos en materia de acceso ilícito a sistemas y equipos de informática, en los cuales se prevén precisamente este tipo de circunstancias:

TITULO NOVENO
Revelación de secretos y acceso ilícito a sistemas y equipos de informática
…
Capitulo II
Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
(…)

Con base en lo anterior, se acredita el daño específico que tendría lugar en caso de que la información fuera pública, ya que se trata de información de gran relevancia, pues como ya se comentó, se encuentra relacionada con aspectos básicos de seguridad informática de los sistemas, y su publicación o divulgación podría ocasionar incluso la destrucción o inhabilitación de la red informática y sistemas del INE.

V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y

Los riesgos que podría conllevar la divulgación de la información, no se limitan a lo relacionado con el desarrollo de los procesos electorales, ya que como se mencionó anteriormente, los sistemas informáticos apoyan la ejecución de las diversas funciones del Instituto, que no necesariamente se desarrollan con motivo de estos. Por lo tanto, los diferentes riesgos a los que se enfrentaría el INE pueden suscitarse en cualquier momento causando afectaciones generales a su funcionamiento institucional.

Aunado a lo anterior, así como al cúmulo de razones establecidas a lo largo del presente documento, se atienden las circunstancias requeridas en el tenor siguiente:

***Modo**.- Cualquier tipo de ataque mediante el acceso o intento de **acceso ilícito** a los sistemas e infraestructura institucionales que sirven de sustento a las actividades propias del INE, que por su propia naturaleza, y tal y como ha quedado precisado, son el conjunto de actos ordenados por la Constitución Federal y la Ley General de Instituciones y Procedimientos Electorales, realizados por las autoridades electorales, los partidos políticos, así como la ciudadanía, que tiene por objeto la renovación periódica de los integrantes de los Poderes Legislativo y Ejecutivo, tanto federal como de las entidades federativas, los integrantes de los ayuntamientos en los estados de la República y de la Ciudad de México.*

***Tiempo**.- Tomando como base los criterios establecidos en el derecho penal, se corre el riesgo de que los ataques se presenten en cualquier momento, es decir, una circunstancia de riesgo permanente y continuo. Como se ha manifestado, el riesgo que representa otorgar la información no sólo se limita a los procesos electorales, sino que se extiende a lo largo del tiempo ya que la infraestructura que da soporte a los sistemas informáticos del INE se utiliza para las actividades cotidianas de la institución.*

***Lugar**.- Al tratarse de elementos de tecnologías de la información y comunicaciones, los ataques pueden ser perpetrados desde cualquier lugar del mundo, causando daño en la infraestructura, redes y/o sistemas del INE, en cualquier parte del territorio nacional.*

VI. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.

Conforme a lo establecido en las fracciones que anteceden, clasificar como reservada la información detallada con anterioridad, constituye una necesidad del INE de salvaguardar los derechos político electorales; así como para seguir cumpliendo con los fines instituciones, por lo que, se debe de proteger la seguridad de los sistemas informáticos, redes e infraestructura que emplea, por lo que otorgar la información implica un riesgo que coloca en estado de vulnerabilidad a la seguridad informática institucional, y con ello, el cumplimiento de las atribuciones y fines del Instituto en preservar el desarrollo de la vida democrática.

Temporalidad de la reserva

*Habiendo considerado la prueba de daño realizada y la naturaleza de la información que se clasifica como temporalmente reservada, se estima que **todos los detalles** de los pormenores de los ataques intentados de, particularmente por lo que hace a la fecha exacta, lugar de origen detectado y*

tipo de ataque, es información que debe permanecer con carácter de reservada de acuerdo con lo siguiente:

Información	*Temporalidad de reserva*
El detalle de los pormenores de los ataques intentados de enero a diciembre de 2014.	*5 años a partir de la aprobación por parte del Comité de Transparencia.*
El detalle de los pormenores de los ataques intentados del 20 de noviembre de 2021 al 26 de febrero de 2024.	*5 años a partir de la aprobación por parte del Comité de Transparencia.*

Lo anterior, debido a que reservar la información por un periodo menor al establecido implica poner en riesgo la seguridad informática del Instituto, para el cumplimiento de sus funciones constituciones y legales, de conformidad con los artículos 101, segundo párrafo, 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Finalmente, se tomaron en cuenta las siguientes consideraciones de modo, tiempo y lugar:

Circunstancias	*Descripción*
Modo	*La solicitud fue turnada a la Dirección de Seguridad y Control Informático, perteneciente a la UTSI.*
Tiempo	*Se realizó la búsqueda de la información en el periodo señalado por la persona solicitante.*
Lugar	*Se realizó la búsqueda exhaustiva en los archivos físicos y electrónicos de la UTSI, específicamente en los de la Dirección de Seguridad y Control Informático.*

(…)." (sic)

2. Detalles de la revisión de la ST del CT

De la respuesta del área **UTSI** se observa que la información es clasificada como reserva temporal total, ya que los detalles **como lo son la fecha exacta, lugar de origen y tipo de ataque**, no pueden ser proporcionados, toda vez que de ser otorgados pondría en riesgo la seguridad Nacional Informática de los sistemas del INE.

Ahora bien, una vez señalado lo anterior el INE tiene el deber de apegarse en todo momento a las disposiciones legales, tal como se aprecia acontinuación:

La LGTAIP y la LFTAIP, reconocen, entre otras causales de reserva, las siguientes:

> **LGTAIP**
>
> *"**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación (…)*
>
> *VII. Obstruya la prevención o persecución de los delitos." (sic)*
>
> **LFTAIP**
>
> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General,como información reservada podrá clasificarse aquella cuya publicación (…)*
>
> *VII. Obstruya la prevención o persecución de los delitos. (sic)*
>
> **Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la Elaboración de Versiones Públicas (Lineamientos generales en materia de clasificación y desclasificación)**
>
> ***"Vigésimo sexto.** De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que **obstruya la prevención de delitos** al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*
>
> *Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:*
>
> **I.** *La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;*
> **II.** *Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y*
> **III.** *Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal." (sic)*

Máxime que la naturaleza de la información de reserva atiende a la existencia de elementos objetivos que permitan determinar que, de entregar dicha información se causaría un daño presente, probable y específico (prueba de daño) a los intereses jurídicos protegidos por la LGTAIP y la LFTAIP, en el entendido que dichos preceptos legales tienen el siguiente alcance:

Prueba de daño:

Los artículos 104, 113 fracción VII y 114 de la LGTAIP; 102, 110 fracción VII y 111 de la LFTAIP; y su correlativo 14 apartado 3 del Reglamento, disponen que, en la aplicación de la prueba de daño, el sujeto obligado deberá justificar los siguientes elementos:

***Por daño presente**: La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*

El área **UTSI**, señaló que:

"*(…) la difusión de la información solicitada pone en riesgo evidente la estabilidad de los sistemas informáticos del Instituto, y con ello la operación institucional de este organismo, así como propiciar el delito de acceso ilícito a sistemas y equipos de informática. En consecuencia, para cumplir y salvaguardar los fines de este Instituto se considera necesario reservar la información con el objeto de contribuir a la vida democrática del país y asegurar a los ciudadanos el ejercicio de sus derechos políticos electorales.*

En este sentido, las soluciones para llevar a cabo la mitigación de ataques de denegación de servicio cuentan con una capacidad finita en los recursos de cómputo y de ancho de banda requeridos para realizar las actividades de revisión y depuración del tráfico de red.

De esta manera, al realizar el dimensionamiento de las soluciones de protección contra ataques volumétricos, se realizan las estimaciones necesarias para contar con el software y el hardware que permita identificar y detener un posible ataque de una volumetría estimada; pero también se debe considerar una solución que tenga un costo – beneficio operativo y económico aceptable, lo que implica necesariamente contar con límites definidos por la marca y el modelo de la solución seleccionada.

En este sentido, se considera que tener acceso a esta información facilitaría a un potencial atacante el identificar la ruta de menor resistencia en un hipotético caso de que se buscara vulnerar la seguridad de los activos informáticos del INE.

*Por lo que, difundir la información solicitada provocaría un **riesgo real** de recibir intentos de ataques cibernéticos directamente enfocados en tratar de evitar las medidas de seguridad informática que se hubieran descrito al hacer pública la información solicitada, es decir, la información que se solicita puede ser utilizada para desarrollar ataques específicamente diseñados para intentar vulnerar los mecanismos, herramientas, infraestructura y sistemas con los que cuenta el INE, afectando así las actividades cotidianas del Instituto, sean éstas relacionadas o no, con los procesos electorales; por lo tanto, se considera que esas agresiones serían potencialmente más riesgosas que aquellas que se pudieran generar sin el conocimiento exacto de las características de los mecanismos, herramientas y sistemas de protección y defensa con los que cuenta el INE. Asimismo, de conformidad con lo establecido*

*en la resolución recaída el Recurso de Revisión **RRA 12927/20** desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es por ello que después del análisis realizado por esta Unidad, el dar a conocer información relativa a los intentos de ataques cibernéticos como lo es la fecha exacta, lugar de origen detectado y tipo de ataque, se estaría potencializando el riesgo de que se lleven ataques cibernéticos, así como el acceso ilícito a sistemas y equipos informáticos, por lo que con la reserva de la información se pretende prevenir esta conducta criminal.*

Asimismo, el recibir intentos de ataques directamente enfocados podrían comprometer la estabilidad de los sistemas informáticos, la operatividad del propio Instituto, e incluso, se podría comprometer el cumplimiento de los principios que rigen las actividades del INE, es decir, la certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, así como propiciar el acceso ilícito a sistemas y equipos de informática." **(sic)**

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

El área **UTSI**, señaló que:

"(…) *Otorgar la información solicitada podría implicar colocar en un estado de vulnerabilidad permanente a los sistemas informáticos del INE, ya que se trata de información sensible que podría brindar elementos para una posible amenaza o vulneración de los propios sistemas, lo que desencadenaría propiciar el delito de acceso ilícito a sistemas y equipos de informática, por lo que con la reserva de la información se pretende prevenir esta conducta criminal.*

*Asimismo, resulta importante destacar que el riesgo **real** antes descrito, mismo que surgiría a partir de la divulgación de información solicitada, es **demostrable**, ya que además de los ataques que ha sufrido el INE y que gracias a las medidas de seguridad con las que se cuenta y de las que de entregarse la información se pondrían en estado de vulnerabilidad y riesgo real, existen numerosos ejemplos de acciones de este tipo (intentos de ataques cibernéticos) que han causado estragos a diversos sistemas informáticos en todo el mundo, y al mismo tiempo **identificable**, ya que de antemano se conocen algunos de los principales tipos en los que se pueden clasificar los referidos ataques cibernéticos. Si bien es cierto que los daños provocados varían en función de la complejidad del ataque y la intención con la que son desarrollados, se considera relevante destacar que cualquier amenaza a la que se encuentre expuesto el INE, se potencializa si se da a conocer el origen de estos y, las características técnicas y de funcionamiento de los mecanismos y herramientas diseñados e implementados para garantizar la seguridad informática del mismo.*

De manera tal que, compartir esta información con un tercero pone en riesgo real la seguridad institucional, ya que coloca al INE en un riesgo latente de sufrir intentos de ataques o accesos no autorizados e ilícitos a la red institucional y a los sistemas de este órgano nacional, ya que – en términos de seguridad informática– todos los intentos de ataques dan inicio con una etapa de reconocimiento durante la cual el atacante hace uso de diversas técnicas que tienen como propósito recopilar y consolidar información técnica acerca de los sistemas que se pretenden atacar, así como de la infraestructura tecnológica subyacente.

Así, se puede decir que, a partir de la ejecución de técnicas de reconocimiento, el atacante, entre otros, está en posibilidad de reconstruir los planos arquitectónicos de la red de datos, así como los componentes de software que coexiste en dicha red de datos y documentar las versiones de dichos componentes. Esta información permite al atacante buscar componentes que presenten vulnerabilidades a partir en bases de datos especializadas (ejemplo: National Vulnerability Database, https://nvd.nist.gov/) así como hacerse de herramientas de ataque (exploits) que permiten aprovechar dichas vulnerabilidades para afectar la seguridad de los activos informáticos afectados.

Por lo anterior, revelar esa información materializaría el riesgo real de afectaciones a la integridad, estabilidad y permanencia de las actividades de este órgano electoral y potencializaría las posibilidades de propiciar el delito de acceso ilícito a sistemas y equipos de informática." **(sic)**

Daño específico: *La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.*

El área **UTSI**, compartió el siguiente cuadro:

"*Conforme a lo establecido en las fracciones que anteceden, clasificar como reservada la información detallada con anterioridad, constituye una necesidad del INE de salvaguardar los derechos político electorales; así como para seguir cumpliendo con los fines instituciones, por lo que, se debe de proteger la seguridad de los sistemas informáticos, redes e infraestructura que emplea, por lo que otorgar la información implica un riesgo que coloca en estado de vulnerabilidad a la seguridad informática institucional, y con ello, el cumplimiento de las atribuciones y fines del Instituto en preservar el desarrollo de la vida democrática.*" **(sic)**

Plazo de reserva: El área **UTSI**, indicó que de conformidad con los artículos 113 fracción VIII de la LGTAIP y 110 fracción VIII de la LFTAIP, se clasifica como reserva temporal total por un **plazo de 5 años**, **los detalles de los ataques digitales como lo son la fecha exacta, lugar de origen y tipo de ataque**.

Conclusión: En virtud de lo anterior el CT, **confirma** la clasificación de **reserva temporal total** propuesta por el área de **UTSI**, respecto **los detalles de los ataques digitales como lo son la fecha exacta, lugar de origen y tipo de ataque.**

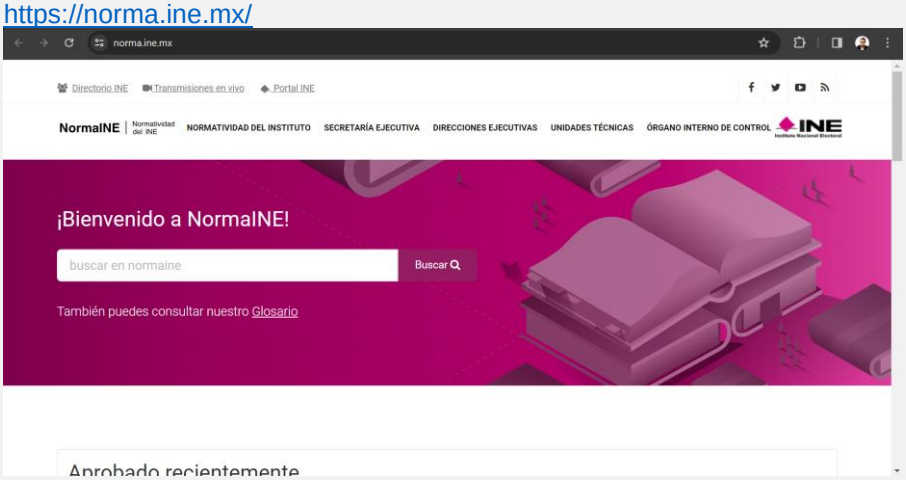
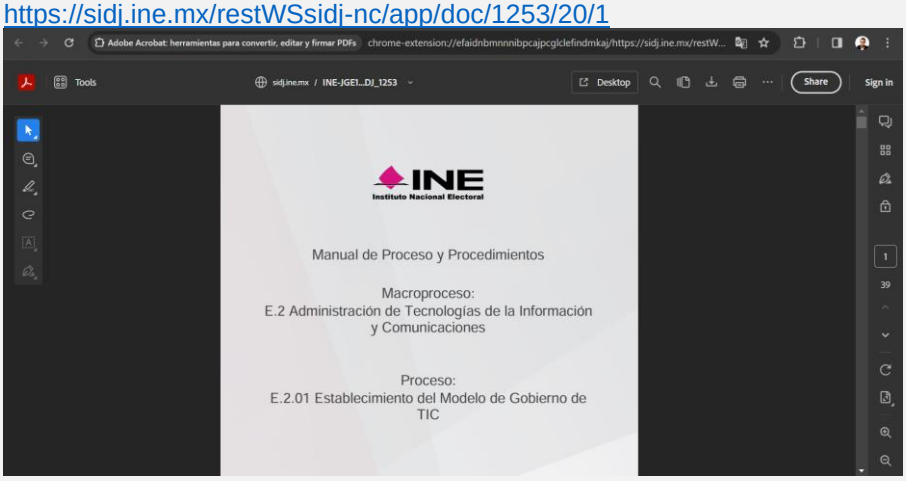
C. Modalidad de entrega de la información

La modalidad de entrega elegida por la persona solicitante es mediante la PNT y correo electrónico.

Por lo tanto, los archivos señalados en los puntos **1** a **6,** serán remitidos por medio de la PNT y correo electrónico.

INE-CT-R-0122-2024

En el siguiente cuadro se lista la información que las áreas ponen a disposición:

CUADRO DE DISPOSICIÓN DE LA INFORMACIÓN	
Tipo de la Información	**<u>Información pública (oficios de respuesta)</u>** **UTSI** **1.** Oficio sin número, mediante 1 archivo electrónico. **UTTyPDP - DPT** **2.** Oficio sin número, mediante 1 archivo electrónico. **3.** NormaINE, mediante 1 liga electrónica. https://norma.ine.mx/  **4.** Manual de proceso y procedimientos de establecimiento del modelo de gobierno de TIC, mediante 1 liga electrónica. https://sidj.ine.mx/restWSsidj-nc/app/doc/1253/20/1  **5.** Manual de proceso y procedimientos de gestión de TIC, mediante 1 liga electrónica. https://sidj.ine.mx/restWSsidj-nc/app/doc/1255/20/1

	 **6.** Manual de proceso y procedimientos de mejora continua de TIC, mediante 1 liga electrónica. https://sidj.ine.mx/restWSsidj-nc/app/doc/1252/20/1 
Formato disponible	• 2 archivos electrónicos • 4 ligas electrónicas
Modalidad de entrega	La modalidad de entrega elegida por la persona solicitante es mediante la PNT y correo electrónico. **Archivos electrónicos. -** La información puesta a disposición en los puntos **1** a **6**, será remitida por medio de la PNT y correo electrónico. **Modalidad en CD. -** Cabe señalar que la información señalada en los puntos **1** a **6**, **no supera** la capacidad de 10 MB en correo electrónico y 20 MB en PNT, no obstante, si lo requiere, se pone a su disposición la información, en 1 CD, previo pago por concepto de recuperación, mismo que le será entregado en el domicilio que para tal efecto señale, una vez que efectúen el pago por concepto de cuota de recuperación.

Modalidad de entrega alternativa. - No obstante, pueden proporcionar a esta UT, 1 CD DE 80 Min. 700 MB que se requiere para la reproducción de la información o una memoria USB (disco duro) con capacidad similar, mismos que serán enviados al área responsable, una vez reproducidos se le hará llegar dentro de los 10 días hábiles siguientes, al domicilio señalado para recibir notificaciones.

No se omite manifestar, que dicho CD contendrá la misma información que le será remitida mediante la PNT y correo electrónico.

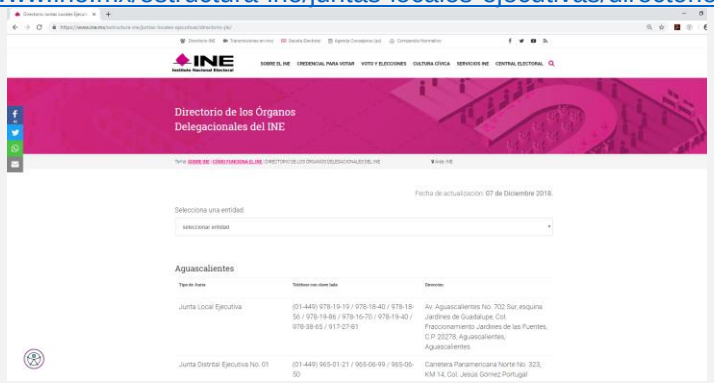
En caso de radicar en la Ciudad de México, se proporciona la dirección para la entrega del material (CD, DVD, disco duro externo, etc.):

Viaducto Tlalpan No. 100, Edificio "C" primer piso, Col. Arenal Tepepan. Del. Tlalpan, C.P. 14610 Ciudad de México, en horario de lunes a viernes (días hábiles) de 9:00 a 18:00 horas, con atención del Lic. Miriam Acosta Rosey y Alan Rodrigo Flores Álvarez, mediante los correos electrónicos miriam.acosta@ine.mx y alan.floresa@ine.mx.

Ahora bien, si usted radica fuera de la Ciudad de México, deberá seguir los siguientes pasos para entrega de material:

1. Se pone a disposición la liga electrónica donde podrán consultar el Directorio Institucional a fin de que pueda ubicar el domicilio de la Junta Local o Distrital Ejecutiva más cercana a su domicilio:

https://www.ine.mx/estructura-ine/juntas-locales-ejecutivas/directorio-jle/



2. Una vez que hayan ubicado la Junta Local o Distrital Ejecutiva más cercana a su domicilio, deberá proporcionar los datos de la Junta Local o Distrital Ejecutiva que haya elegido, a esta UT a través de los correos electrónicos miriam.acosta@ine.mx y alan.floresa@ine.mx.

3. Llevado a cabo lo anterior, se le notificará mediante correo electrónico el día y horario en el que podrán acudir para hacer entrega del material; así

	como los datos del personal de la Junta Local o Distrital Ejecutiva que le otorgará la atención correspondiente.
Cuota de recuperación	$11.00 (ONCE PESOS 00/100 M.N.), por 1 CD con las respuestas proporcionadas por las áreas. [Precio unitario por CD $11.00 (ONCE PESOS 00/100 M.N.] **No se omite manifestar, que dicho CD contendrá la misma información que le será remitida mediante la PNT y correo electrónico.** El envío de la información no tiene costo alguno, por lo que las cuotas de recuperación corresponden al medio de reproducción o en su caso certificación.
Especificaciones de pago	Depósitos entre cuentas BBVA: Se debe realizar el alta en la banca móvil el convenio CIE: 001741667, para realizar la transferencia. Transferencias desde otros bancos: Se realiza a la Cuenta CLABE INTERBANCARIA: 012914002017416675. En ambos casos, es obligatorio poner como referencia: **18COPIAS7** (espacio) y el concepto de pago, por ejemplo: **18COPIAS7 pago cd** **Nota: Es importante el espacio entre la referencia y el concepto, ya que servirá para identificar el pago y para que el mismo no sea rechazado.** Es indispensable proporcionar la ficha de depósito a esta UT, por correo electrónico a más tardar al día siguiente hábil de haber realizado el mismo, a fin de comprobar que se ha cubierto el pago de la cuota antes mencionada y se genere la información. Si bien la PNT ofrece opciones para genera formatos de pago, el INE –por ser un organismo autónomo- tiene un mecanismo propio y una cuenta bancaria especifica distinta a la de la Administración Pública Federal (APF). Los costos están previstos en el Acuerdo del CT INE-CT-ACG-0001-2024.
Plazo para reproducir la información	Una vez que la UT reciba le comprobante de pago por correo electrónico, el área responsable contará con 5 días hábiles para remitir la información y la UT con 5 días más para su entrega.
Plazo para disponer de la información	Una vez generada la información y notificada su disposición a la persona solicitante, contará con un plazo de 60 días para recogerla. El pago deberá efectuarse en un plazo no mayor de 30 días hábiles. Transcurrido el plazo referido y de no recoger la información, los particulares deberán realizar una nueva solicitud de acceso a la información.

Fundamento legal	Artículos 6 de la CPEUM; 6 de la LFTAIP; 4, 32 y 34 párrafos 2 y 3 del Reglamento; y el Acuerdo del CT INE-CT-ACG-0001-2024.

D. Qué hacer en caso de inconformidad

En caso de inconformidad con esta resolución, podrán impugnarla a través del recurso de revisión dentro de los quince días hábiles siguientes a la fecha de la notificación de la presente, conforme lo establecen los artículos 142, 144 y 145 de la LGTAIP; 146 a 149 de la LFTAIP y 38 del Reglamento.

E. Fundamento legal

Por lo antes expuesto y con fundamento en los artículos: 6, tercer párrafo de la CPEUM; 30 de la Ley General de Instituciones y Procedimientos Electorales; 1, 4, 19, 20, 101 segundo párrafo, 108 último párrafo, 113 fracción VII y 129 de la LGTAIP; 110 fracción VII y 130, cuarto párrafo de la LFTAIP; 211 bis 1 y 211 bis 2 del Código Penal Federal; 1; 2, párrafo 1, fracción XXXI; 20, fracción V; 22, numeral 2, 24, párrafos 1 y 2, fracciones I y III; 27, párrafo 1; 28, párrafo 3 y numeral 10; 29, párrafo 1; 32; 35 y 36 del Reglamento; lineamientos vigésimo sexto y trigésimo tercero de los Lineamientos generales en materia de clasificación y desclasificación; se emite la siguiente:

F. Determinación

Conforme al apartado anterior, se presenta el concentrado de decisiones del CT:

> **Primero. Información pública.** Se pone a disposición la información considerada como pública.
>
> **Segundo. Reserva temporal total.** Se confirma la clasificación de reserva temporal total formulada por el área **UTSI respecto de los detalles de los ataques digitales como lo son la fecha exacta, lugar de origen y tipo de ataque.**
>
> **Tercero. Incompetencia**. Debido a que la manifestación de incompetencia sustentada por el área **UTTyPDP - DPT**, no invoca la participación de un sujeto obligado ajeno al INE, no existe materia para el análisis.

Cuarto. Inconformidad. En caso de inconformidad con la presente resolución podrá interponer el medio de impugnación respectivo.

Notifíquese a la persona solicitante por la vía elegida y a las áreas **UTSI** y **UTTyPDP - DPT**, por la herramienta electrónica correspondiente.

Aviso de privacidad del Sistema INFOMEX-INE; y de la PNT (INAI).[8]

----------*Inclúyase la Hoja de Firmas debidamente formalizada*----------
---

Autorizó: SLMV Supervisó: MAAR Elaboró: ARFA

"Este documento ha sido firmado electrónicamente de conformidad con el criterio SO/007/2019 emitido por el Pleno del INAI el cual señala: "Documentos sin firma o membrete. Los documentos que son emitidos por la UT son válidos en el ámbito de la LFTAIP cuando se proporcionan a través de la PNT, aunque no se encuentren firmados y no contengan membrete."

Asimismo, se da cuenta del oficio INAI/SAI/DGEPPOEP/0547/2020 emitido por el INAI, en el cual señaló que las respuestas otorgadas por la UT del INE en el que el CT del INE utilice la Firma Electrónica Avanzada (que expide el propio INE) puede realizarse en el ámbito de la Ley de la materia, cuando se proporciona a través de la PNT, considerando que cuando un particular presenta una solicitud por medios electrónicos a través de la PNT, se entenderá que acepta que las notificaciones le sean efectuadas por dicho sistema.

---

[8] **¿Quién es el responsable de tus datos personales?** El Instituto Nacional Electoral (INE), a través de la Unidad Técnica de Transparencia y Protección de Datos Personales (UTTyPDP) es el responsable del tratamiento de los datos personales que nos proporciones.

¿Para qué finalidad o finalidades utilizamos tus datos personales? Los datos personales serán utilizados para las siguientes finalidades: Finalidad primaria: registrar y gestionar internamente las solicitudes de acceso a la información y para el ejercicio de los derechos de acceso, rectificación, cancelación oposición y portabilidad de datos personales (derechos ARCOP), así como los recursos de revisión. Realizar notificaciones a las personas solicitantes, así como llevar un registro de estas gestiones para efectos de rendición de cuentas; finalidad secundaria: Generar información estadística, para integrar los informes en materia de transparencia, acceso a la información pública y protección de datos personales, que presenta la UTTyPDP ante diversos órganos colegiados del INE y ante el organismo garante en materia de transparencia, acceso a la información y protección de datos personales. Para las finalidades antes descritas no requerimos de tu consentimiento, ya se actualizan las causales de excepción previstas en el artículo 22, fracciones IV y IX, de la LGPDPPSO.

¿A quién transferimos tus datos personales? Solo realizaremos transferencias de tus datos personales para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados, para las cuales no requerimos de tu consentimiento, de conformidad con lo previsto en los artículos 22, fracciones II y III, y 70, fracciones II y VIII, de la LGPDPPSO. Adicionalmente, transferiremos tus datos personales al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de la Plataforma Nacional de Transparencia, con la finalidad de atender las solicitudes de información pública y para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, así como para atender los requerimientos del organismo garante para sustanciar los recursos de revisión.

¿Cómo y dónde puedes manifestar la negativa al tratamiento de tus datos personales? Podrás manifestar la negativa al tratamiento de tus datos personales a través del ejercicio de los derechos de cancelación u oposición ante la Unidad de Transparencia (UT) del INE, ubicada en Viaducto Tlalpan número 100, edificio "C", primer piso, colonia Arenal Tepepan, alcaldía Tlalpan, código postal 14610, Ciudad de México, de 9:00 a 18:00 horas, de lunes a viernes, en días hábiles o bien, a través de la Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx/).

¿Dónde puedes consultar el aviso de privacidad Integral?

El aviso de privacidad integral podrás consultarlo en el siguiente vínculo https://www.ine.mx/transparencia/listado-bases-datos-personales/ en el apartado correspondiente a la UTTyPDP.

INSTITUTO NACIONAL ELECTORAL

INE-CT-R-0122-2024

Resolución del Comité de Transparencia (CT) del Instituto Nacional Electoral (INE), respecto a la solicitud de acceso a la información **330031424000969 (UT/24/00912).**

La presente resolución fue aprobada por unanimidad de votos de los integrantes del CT, en Sesión Extraordinaria Especial celebrada el 26 de marzo de 2024.

Mtro. Juan Manuel Vázquez Barajas PRESIDENTE CON DERECHO A VOTO	Encargado del despacho de la Dirección Jurídica, en su carácter de Presidente del Comité de Transparencia.
Dr. Héctor Virgilio Esaú Jaramillo Rojas INTEGRANTE TITULAR CON DERECHO A VOTO	Asesor de la Secretaría Ejecutiva B, en su carácter de Integrante del Comité de Transparencia.
Mtra. María del Carmen Urías Palma INTEGRANTE TITULAR CON DERECHO A VOTO	Encargada del despacho de la Unidad Técnica de Transparencia y Protección de Datos Personales, en su carácter de Integrante del Comité de Transparencia.

Mtra. Sendy Lucia Murillo Vargas	Subdirectora de Acceso a la Información, en su carácter de Secretaria Técnica (suplente) del Comité de Transparencia.

"Este documento ha sido firmado electrónicamente, de conformidad con el artículo 22 del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Nacional Electoral."

FIRMADO POR: MURILLO VARGAS SENDY LUCIA
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2999291
HASH:
EA214C38016BFFC64D22E8D7D683C91A8A3CE162ADA2B0DF0D598D7229EF90F9

FIRMADO POR: VAZQUEZ BARAJAS JUAN MANUEL
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2999291
HASH:
EA214C38016BFFC64D22E8D7D683C91A8A3CE162ADA2B0DF0D598D7229EF90F9

FIRMADO POR: JARAMILLO ROJAS HECTOR VIRGILIO ESAU
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2999291
HASH:
EA214C38016BFFC64D22E8D7D683C91A8A3CE162ADA2B0DF0D598D7229EF90F9

FIRMADO POR: URIAS PALMA MARIA DEL CARMEN
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2999291
HASH:
EA214C38016BFFC64D22E8D7D683C91A8A3CE162ADA2B0DF0D598D7229EF90F9