



INSTITUTO NACIONAL ELECTORAL

**INE-CT-R-0365-2024**

**Resolución del Comité de Transparencia (CT) del Instituto Nacional Electoral (INE) en atención a la solicitud de acceso a la información 330031424003367 (UT/24/03205).**

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

- 1. Atención de la solicitud ..... 2
  - A. Cuáles son los datos de su solicitud..... 2
  - B. Qué hicimos para atenderla ..... 2
  - C. Ampliación de plazo ..... 3
- 2. Acciones del CT ..... 4
  - A. Competencia ..... 4
  - B. Análisis de la clasificación y de la manifestación..... 4
  - C. Modalidad de entrega de la información..... 20
  - D. Qué hacer en caso de inconformidad..... 25
  - E. Fundamento legal..... 25
  - F. Determinación ..... 25



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

### 1. 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:** 25 de julio de 2024
- c. **Medio de ingreso:** Plataforma Nacional de Transparencia (PNT)
- d. **Folio de la PNT:** 330031424003367
- e. **Folio interno asignado:** UT/24/03205
- 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 2023 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	26/07/2024 Dentro del plazo	02/08/2024	Infomex-INE y oficio de	Información pública (punto 1)



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

ÓRGANOS CENTRALES					
Con-sec.	Áreas	Fechas de turno	Fecha(s) de respuesta	Medio de respuesta (Infomex-INE, correo electrónico, oficio)	Tipo de información
		Segundo turno 05/08/2024 Reasignación de turno	(Solicitud de ampliación de plazo) Dentro del plazo  Respuesta a segundo plazo 14/08/2024 Dentro del plazo	respuesta sin número	<b>Reserva temporal total (punto 2)</b>
2.	UTTyPDP - DPT	26/07/2024 Dentro del plazo	30/07/2024 Dentro del plazo	Infomex-INE y oficio de respuesta sin número	<b>Incompetencia (totalidad de la solicitud)</b>
		Requerimiento de aclaración 08/08/2024	Respuesta al RA 09/08/2024		<b>Máxima publicidad (totalidad de la solicitud)</b>
		Segundo turno 16/08/2024	Segundo turno 16/08/2024		<b>Orientación (totalidad de la solicitud)</b>
<b>Fecha de gestión más reciente: 16/08/2024</b>					

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

### C. Ampliación de plazo

El 13 de agosto de 2024, la UT notificó a la persona solicitante, a través de la PNT y correo electrónico, el acuerdo INE-CT-ACAM-0031-2024, 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.



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

### 2. Acciones del CT

El 23 de agosto 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			
1. "Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2023 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 <b>intento</b> (deliberado o no) por vulnerar la integridad, disponibilidad o confidencialidad de los sistemas informáticos del INE.	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



INSTITUTO NACIONAL ELECTORAL

**INE-CT-R-0365-2024**

<b>Punto 1</b>											
1. "Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2023 a la fecha. <b>(sic)</b> "											
<b>Qué área respondió</b>	<b>Cómo respondió</b>	<b>El área explicó por qué respondió en ese sentido (motivación)</b>	<b>El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)</b>								
		<p>En este sentido, se precisa que en el periodo comprendido entre el 1 de enero de 2023 al 31 de julio de 2024, no se ha materializado ningún intento de ataque en contra de los sistemas administrador por la UTSI por los motivos señalados en el párrafo que antecede, resultando en que el número de ataques que causaron afectaciones a dichos sistemas sea igual a cero.</p> <p>No obstante, los intentos de ataque que fueron identificados y registrados en los sistemas de esta Unidad Técnica a través de las herramientas con las que cuenta el Instituto en el periodo solicitado por la persona solicitante en los sistemas administrados por esta Unidad corresponden a los siguientes:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="background-color: #e91e63; color: white;">Año</th> <th style="background-color: #e91e63; color: white;">Número de intentos de ataques</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">2023</td> <td style="text-align: center;">3,078,035</td> </tr> <tr> <td style="text-align: center;">2024 (al 12 de agosto de 2024)</td> <td style="text-align: center;">3,599,277</td> </tr> <tr> <td style="text-align: center;"><b>Total</b></td> <td style="text-align: center;"><b>6,677,312</b></td> </tr> </tbody> </table>	Año	Número de intentos de ataques	2023	3,078,035	2024 (al 12 de agosto de 2024)	3,599,277	<b>Total</b>	<b>6,677,312</b>	<p><i>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 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." <b>(sic)</b></i></p>
Año	Número de intentos de ataques										
2023	3,078,035										
2024 (al 12 de agosto de 2024)	3,599,277										
<b>Total</b>	<b>6,677,312</b>										
<b>UTTyPDP</b>	<b>Incompetencia**</b>	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	Sí, de conformidad con lo establecido en los siguientes artículos:								



INSTITUTO NACIONAL ELECTORAL

**INE-CT-R-0365-2024**

**Punto 1**  
 1. "Solicito se me informe el número de ataques digitales a servidores y página electrónica han registrado por día desde el año 2023 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)
	<b>Máxima publicidad</b>	<p>Reglamento, la información solicitada no se genera al desarrollar las atribuciones de dicha Dirección.</p> <p>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 NormalNE (<a href="https://norma.ine.mx/">https://norma.ine.mx/</a>) del Instituto se pueden consultar contenidos que aluden a seguridad informática en el Instituto que podrían ser de interés a la persona peticionaria.</p>	<p>"22, numeral 2 y 28, numeral 10, del Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública." <b>(sic)</b></p>

**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)
<b>UTSI</b>	<b>Reserva temporal total*</b>	<p>Sí, el área señala que la información requerida sobre los detalles <b>como lo son la fecha exacta, lugar de origen y tipo de ataque</b>, no pueden ser proporcionados, ya que de ser otorgados pondría en riesgo la seguridad Nacional</p>	<p>Sí, de conformidad con lo establecido en los artículos:</p> <p>"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</p>



INSTITUTO NACIONAL ELECTORAL

**INE-CT-R-0365-2024**

<b>Punto 2</b>			
<i>“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)</i>			
<b>Qué área respondió</b>	<b>Cómo respondió</b>	<b>El área explicó por qué respondió en ese sentido (motivación)</b>	<b>El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)</b>
		Informática de los sistemas del INE.	<i>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)</i>
<b>UTTyPDP</b>	<b>Incompetencia**</b>	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:  <i>“28, numeral 10 y 29, párrafo 3, fracción VII, del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información</i>



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

<b>Punto 2</b>			
<i>“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)</i>			
<b>Qué área respondió</b>	<b>Cómo respondió</b>	<b>El área explicó por qué respondió en ese sentido (motivación)</b>	<b>El área detalló las normas en las que se basa para responder en ese sentido (fundamentación)</b>
	<b>Máxima publicidad</b>	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 NormalNE ( <a href="https://norma.ine.mx/">https://norma.ine.mx/</a> ) del Instituto se pueden consultar contenidos que aluden a seguridad informática en el Instituto que podrían ser de interés a la persona peticionaria.	<i>Pública y 68, del Reglamento Interior de este Instituto y 44, numeral 1, inciso d) del Reglamento Interior del Instituto Nacional Electoral.” (sic)</i>

\* 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 de los siguientes periodos:**

- ◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.
- ◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

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

<b>Conclusión de la Secretaría Técnica del Comité de Transparencia:</b>	Es factible confirmar la clasificación.				
<b>Propuesta de clasificación del área:</b>	Reserva temporal total	<b>Plazo de clasificación</b>	Periodo del 1 de enero de 2023 al 26 de febrero de 2024		
			4 años	5	29 días
			Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.		
			5	0	0
			Años	Meses	Días
<b>Folios PNT:</b>	330031424003367	<b>Medio de envío de la información clasificada:</b>	INFOMEX-INE		
<b>Folios internos:</b>	UT/24/03205	<b>¿El área envió la totalidad de la información o una muestra?</b>	El área envía explicación		
<b>Área que envía la información clasificada:</b>	UTSI	<b>Volumen de la totalidad o muestra:</b>	El área envía explicación		
<b>Fecha de recepción de la información clasificada en la UT:</b>	14/08/2024				



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

Número de RA <sup>1</sup> formulados:	N/A <sup>2</sup>	Número de RII <sup>3</sup> formulados:	N/A
---------------------------------------	------------------	--	-----

### 1. Descripción general de la información

Es importante señalar que el área **UTSI**, no remite muestra de la información sin embargo remite explicación de la clasificación de reserva temporal total, mediante su oficio de respuesta, señalando lo siguiente:

#### ◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.

*“Ahora bien, se hace de conocimiento de la persona solicitante que la información correspondiente a cada uno de los **detalles** de los pormenores presentados del, **1 de enero de 2023 al 26 de febrero de 2024**, se encuentra clasificada como temporalmente reservada, ya que dicha información fue requerida a través de la solicitud de acceso a la información UT/24/00912. Lo anterior, toda vez que los detalles como lo son; **la fecha exacta, lugar de origen y tipo de ataque** no pueden ser proporcionados, ya que de ser otorgados se pondría en riesgo la seguridad Nacional Informática de los sistemas del Instituto Nacional Electoral.*

*Asimismo, como se mencionó en líneas anteriores se informa que dicha información ya había sido previamente clasificada de manera parcial por contener información reservada, de conformidad con el siguiente cuadro:*

Solicitud de información	Información reservada	Resolución del CT	Temporalidad de la clasificación de la información	Fecha de inicio de clasificación	Fecha de término de clasificación
UT/24/00912	Información relativa al número de ataques digitales a servidores y página electrónica que se registraron del 1 de enero al 31	INE-CT-R-0122-2024	5 años	26 de marzo de 2024.	26 de marzo de 2029.

<sup>1</sup> Requerimiento de Aclaración (RA).

<sup>2</sup> No Aplica (NA).

<sup>3</sup> Requerimiento Intermedio de Información (RII).



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

Solicitud de información	Información reservada	Resolución del CT	Temporalidad de la clasificación de la información	Fecha de inicio de clasificación	Fecha de término de clasificación
	de diciembre de 2014 y del 20 de noviembre de 2021 al 26 de febrero de 2024.				

(...)

### **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
<b>El detalle de los pormenores de los ataques intentados de enero a diciembre de 2014.</b>	<b>5 años a partir de la aprobación por parte del Comité de Transparencia.</b>
<b>El detalle de los pormenores de los ataques intentados del 20 de noviembre de 2021 al 26 de febrero de 2024.</b>	<b>5 años a partir de la aprobación por parte del Comité de Transparencia.</b>

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 constitucionales 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.

En este sentido, la información requerida por la persona solicitante y correspondiente al periodo antes descrito se encuentra reservada, por lo tanto, no puede ser proporcionada, ya que los motivos que dieron origen a su clasificación subsisten actualmente, y la temporalidad por la que fue aprobada



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

la clasificación por el Comité de Transparencia del Instituto mediante resolución **INE-CT-R-0122-2024**, se encuentra vigente.

### ◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.

Por otro lado, respecto de la información detallada sobre los ataques del **27 de febrero del 2024 al 12 de agosto de 2024**, se informa que dicha información no puede ser otorgada y se propone la **reserva temporal** de la misma, ya que proporcionar los datos correspondientes a **la fecha exacta, lugar de origen y tipo de ataque** pondrían en riesgo la seguridad nacional informática de los sistemas del INE. En ese sentido, a continuación, se expresan los fundamentos necesarios que respaldan la propuesta de reserva temporal, mediante la siguiente prueba de daño:

(...)

#### **Temporalidad de la reserva**

Una vez considerado lo plasmado en 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 guardar el carácter de reservada conforme lo siguiente:

<b>Información</b>	<b>Temporalidad de reserva</b>
<i>El detalle de los pormenores de los ataques intentados del <b>27 de febrero del 2024 al 12 de agosto de 2024</b>.</i>	<i>5 años a partir de la aprobación por parte del Comité de Transparencia.</i>

Lo anterior, debido a que reservar la información por un periodo menor al establecido, representa un en riesgo a 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:



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

<b>Circunstancias</b>	<b>Descripción</b>
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.

Cabe señalar que el área, clasificó como totalmente reservados los siguientes periodos:

- ◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.
- ◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.

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 a continuación:

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 (...)*



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

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:



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.

*“(…) 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*



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

decir, la certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, así como propiciar el acceso ilícito a sistemas y equipos de informática.” (sic)

◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.

*“(…) 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*



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

*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:

◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.

*“(…) 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.*



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

*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)*

### ◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.

*“(…) 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*



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

*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**, señaló que:

◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.

*“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)*

◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.

*“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 VII de la LGTAIP y 110 fracción VII 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, de los siguientes periodos:**

◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024.

◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.

Cabe señalar que el CT, ya se ha pronunciado por la clasificación de información relativa a los detalles de los ataques digitales como lo son la fecha exacta, lugar de origen y tipo de ataque, del siguiente periodo del 1 de enero de 2023 al 26 de febrero de 2024, confirmando la clasificación.



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

Resolución	Fecha de aprobación	Resolutivos
INE-CT-R-0122-2024	26 de marzo de 2024	“(…)  <u>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.</u>  “(…)” (Sic)

Por lo anterior, la UTTPDP hizo a bien realizar el descuento respectivo del plazo transcurrido, por lo que los plazos de reserva correspondiente son los siguientes:

Periodo	Plazo de reserva
Periodo del 1 de enero de 2023 al 26 de febrero de 2024.	4 años, 5 meses 29 días
Periodo del 27 de febrero del 2024 al 12 de agosto de 2024.	5 años

**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**, de los siguientes periodos y plazos de reserva:

- ◆ Periodo del 1 de enero de 2023 al 26 de febrero de 2024, por 4 años 5 meses 29 días
- ◆ Periodo del 27 de febrero del 2024 al 12 de agosto de 2024, por un plazo de 5 años.

### C. Modalidad de entrega de la información

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

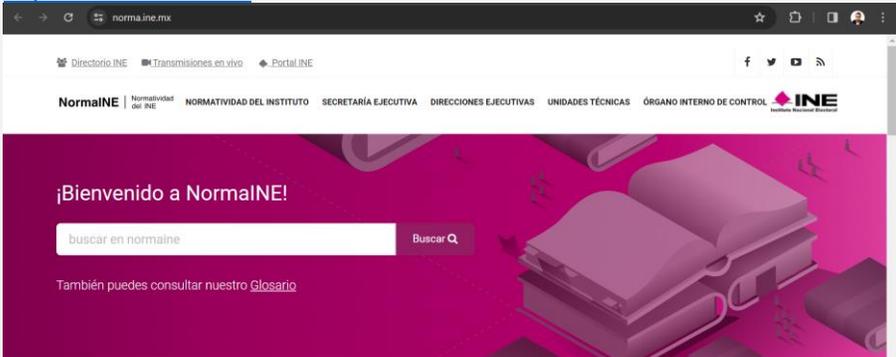
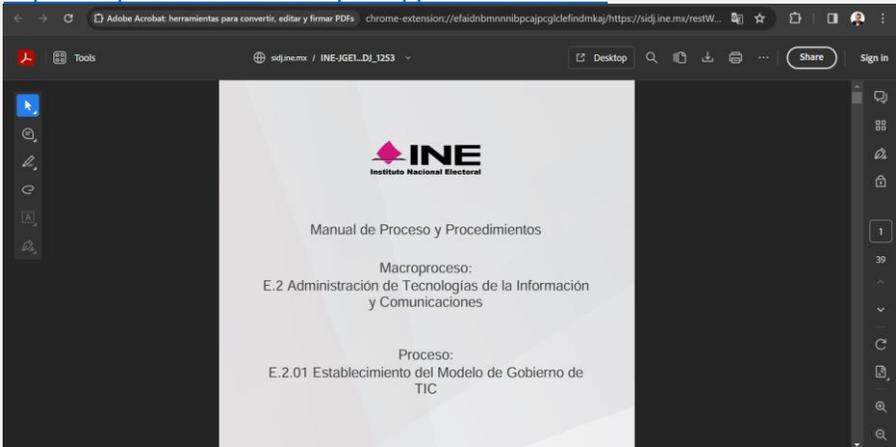
Por lo tanto, los archivos señalados en los puntos **1** a **7** serán remitidos por medio de la PNT y correo electrónico.

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



INSTITUTO NACIONAL ELECTORAL

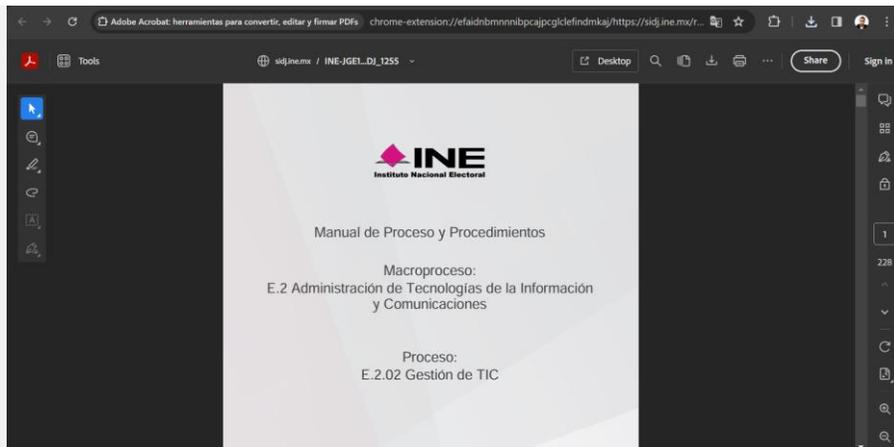
## INE-CT-R-0365-2024

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



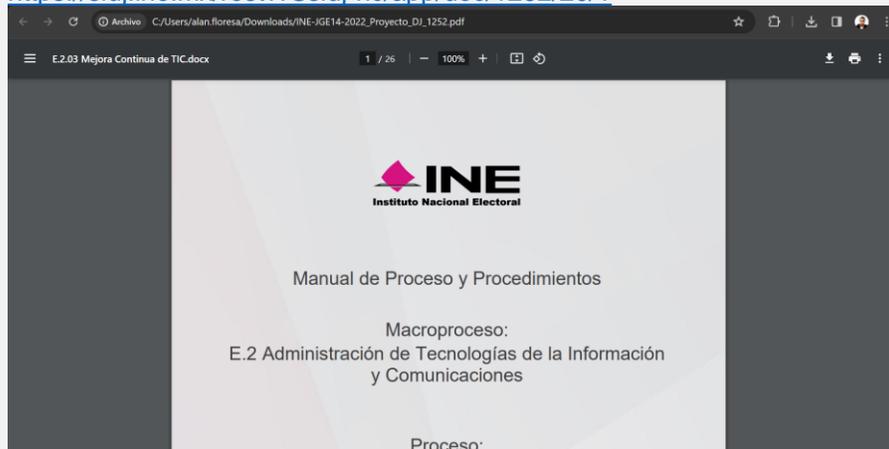
INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024



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>



### UTTyPDP

7. Aviso de privacidad, mediante 1 archivo electrónico.

#### Formato disponible

- 3 archivos electrónicos
- 4 ligas electrónicas

#### Modalidad de entrega

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

**Archivos electrónicos.** - La información puesta a disposición en los puntos 1 a 7 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



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

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.**

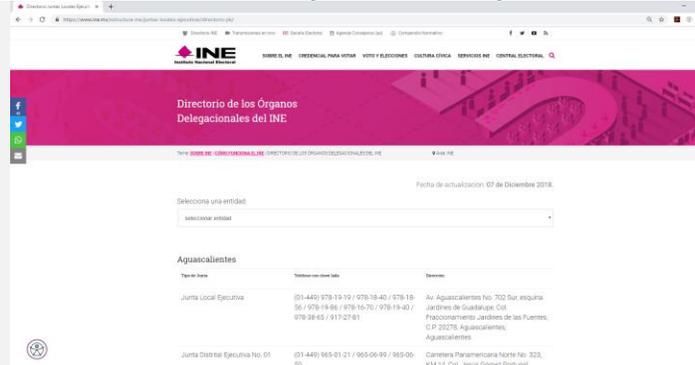
En caso de radicar en la Ciudad de México, se proporciona la dirección para la entrega del material (CD, DVD, disco duro externo, etc.):

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](mailto:miriam.acosta@ine.mx) y [nayeli.morgado@ine.mx](mailto:nayeli.morgado@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](mailto:miriam.acosta@ine.mx) y [nayeli.morgado@ine.mx](mailto:nayeli.morgado@ine.mx).



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

	<p>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.</p>
<b>Cuota de recuperación</b>	<p>\$11.00 (ONCE PESOS 00/100 M.N.), por 1 CD con las respuestas proporcionadas por las áreas.</p> <p>[Precio unitario por CD \$11.00 (ONCE PESOS 00/100 M.N.)]</p> <p><b>No se omite manifestar, que dicho CD contendrá la misma información que le será remitida mediante la PNT y correo electrónico.</b></p> <p>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.</p>
<b>Especificaciones de pago</b>	<p>Depósitos entre cuentas BBVA: Se debe realizar el alta en la banca móvil el convenio CIE: 001741667, para realizar la transferencia.</p> <p>Transferencias desde otros bancos: Se realiza a la Cuenta CLABE INTERBANCARIA: 012914002017416675.</p> <p>En ambos casos, es obligatorio poner como referencia: <b>18COPIAS7</b> (espacio) y el concepto de pago, por ejemplo: <b>18COPIAS7 pago cd</b></p> <p><b>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.</b></p> <p>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.</p> <p>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 específica distinta a la de la Administración Pública Federal (APF).</p> <p>Los costos están previstos en el Acuerdo del CT INE-CT-ACG-0001-2024.</p>
<b>Plazo para reproducir la información</b>	<p>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.</p>
<b>Plazo para disponer de la información</b>	<p>Una vez generada la información y notificada su disposición a la persona solicitante, contará con un plazo de 60 días para recogerla.</p> <p>El pago deberá efectuarse en un plazo no mayor de 30 días hábiles.</p>



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

	Transcurrido el plazo referido y de no recoger la información, los particulares deberán realizar una nueva solicitud de acceso a la información.
<b>Fundamento legal</b>	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



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

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). Se adjunta al presente documento.***<sup>4</sup>

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

Autorizó: SLMV      Supervisó: MAAR      Elaboró: NMC

“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.

<sup>4</sup> [https://ine.mx/wp-content/uploads/2024/02/infomexaviso\\_de\\_privacidad\\_simplificado.pdf](https://ine.mx/wp-content/uploads/2024/02/infomexaviso_de_privacidad_simplificado.pdf)



INSTITUTO NACIONAL ELECTORAL

## INE-CT-R-0365-2024

Resolución del Comité de Transparencia (CT) del Instituto Nacional Electoral (INE) en atención a la solicitud de acceso a la información **330031424003367 (UT/24/03205)**.

La presente resolución fue aprobada por unanimidad de votos de los integrantes del CT, en Sesión Extraordinaria Especial celebrada el 27 de agosto de 2024.

<b>Lic. José Alonso Pérez Jiménez</b> SUPLENTE DEL PRESIDENTE CON DERECHO A VOTO	Director de Normatividad y Consulta de la Dirección Jurídica, en su carácter de Suplente del Presidente del CT.
<b>Lic. Sergio Vitaly Téllez Peña</b> INTEGRANTE TITULAR CON DERECHO A VOTO	Asesor de la Secretaría Ejecutiva A, en su carácter de Integrante del CT
<b>Mtra. Fanny Aimee Garduño Néstor</b> INTEGRANTE SUPLENTE CON DERECHO A VOTO	Directora de Políticas de Transparencia de la Unidad Técnica de Transparencia y Protección de Datos Personales, en su carácter de Integrante Suplente del CT
<b>Lic. Ivette Alquicira Fontes</b>	Directora de Acceso a la Información y Protección de Datos Personales, en su carácter de Secretaria Técnica del CT.

"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."



