



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Acuerdo del Comité de Transparencia (CT) del Instituto Nacional Electoral (INE) en atención a la solicitud de ampliación de plazo de reserva de la información correspondiente a la solicitud de acceso a la información 2210000132618 (UT/18/01225)

El presente acuerdo se emite en términos de los artículos 44, fracción VIII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 65, fracción VIII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).

ANTECEDENTES

1. El 6 de abril de 2018, ingresó la solicitud con folio 2210000132618, mediante la Plataforma Nacional de Transparencia (PNT); la Unidad Técnica de Transparencia y Protección de Datos Personales (UTTyPDP) la tuvo por recibida.
2. El 9 de abril de 2018, la solicitud de información se turnó a través del Sistema INFOMEX-INE a la Unidad Técnica de Servicios de Informática (UTSI).
3. El 16 de abril de 2018, la UTSI emitió respuesta a la solicitud de información.
4. El 27 de abril de 2018, la UTSI remitió un alcance a la respuesta primigenia en el cual se atendió el cuestionamiento referente al *“Listado de todos los sistemas de análisis de información electoral (sistemas informáticos que involucren información, de padrones electorales y/o elecciones), o para identificación, segmentación o perfilamiento de votantes.”*
5. El 26 de abril del 2018, el CT del INE aprobó mediante acuerdo INE-CT-ACAM-0019-2018 la ampliación del plazo previsto en el artículo 132 de la LGTAIP; 135 de la LFTAIP y 30 del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública (Reglamento).
6. El 30 de abril de 2018, se notificó la ampliación del plazo a la persona solicitante, por medio de la PNT.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

7. El 11 de mayo de 2018, el CT del INE aprobó la resolución INE-CT-R-0291-2018, mediante la cual determinó, entre otros aspectos, lo siguiente:

“III. Pronunciamiento de fondo.

A. Clasificación de Reserva Temporal.

*El área (UNICOM), al dar respuesta, respecto los códigos fuente y documentos de diseño de los sistemas desarrollados, precisó lo siguiente:
(...)*

Es importante precisar que este CT, observa que conforme a la reserva realizada por la UNICOM, respecto los códigos fuente y documentos de diseño de los sistemas desarrollados por la propia área, coloca al Instituto en riesgo de sufrir una vulneración a su seguridad informática, considerando que muchas actividades realizadas por el Instituto son realizadas con los sistemas del instituto.

En ese sentido es pertinente señalar que para garantizar la seguridad informática de los sistemas que obran en el Instituto, así como por razones de interés público y seguridad nacional, el área UNICOM clasifica la información como temporalmente reservada en términos de los artículos; 3, fracciones III y VI y 5 fracción I de la Ley de Seguridad Nacional que establecen:

"ARTICULO 3.- Para efectos de esta ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

I. (...)

III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;

IV.(...)

V. La preservación de la democracia, fundada en el desarrollo económico, social y político del país y sus habitantes." (Sic).

ARTÍCULO 5.- Para los efectos de la presente Ley, son amenazas o la Seguridad Nacional:

I. Actos tendientes a consumir espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;" (Sic).



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

En concordancia con La Ley General y la Ley Federal de Transparencia se reconocen, entre otras causales de reserva, las siguientes:

Ley General de Transparencia y Acceso a la Información Pública

"ARTÍCULO 113.

Como información reservada podrá clasificarse aquella cuya publicación:

- I. *Comprometa la Seguridad Nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y demostrable;"(Sic)*

Ley Federal de Transparencia y Acceso a la Información Pública

"ARTÍCULO 110.

Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

(...)

- I. *Comprometa la Seguridad Nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y demostrable;"(Sic)*

En razón de lo anterior, se precisa que al entregar dicha información atentaría contra las obligaciones establecidas en el artículo 11, fracción VI de la LFTAIP por lo que se podría incurrir en las responsabilidades que señala el artículo 186 de la LFTAIP.

Es importante mencionar 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 LFTAIP en el entendido que dichos preceptos legales tienen el siguiente alcance:

Prueba de daño:

El artículo 104 en relación con el diverso 114 de la LGTAIP y correlativo 14, apartado 3 del Reglamento, dispone 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 pública o a la seguridad nacional;*

El área UNICOM señaló que la información relativa a los códigos fuente y los documentos de diseño de los sistemas informáticos del instituto, se reserva con la finalidad de evitar vulneraciones a la seguridad informática del Instituto, pues los ejercicios de las atribuciones de éste se desarrollan en su mayoría con los



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

sistemas informáticos que se desarrollan, de entregar dicha información, causaría una inestabilidad en las atribuciones del Instituto; considerando que:

"código fuente es el conjunto de pasos que debe seguir un equipo de cómputo, servidor o dispositivo de procesamiento de datos para ejecutar un programa o sistema" (Sic).

En ese orden de ideas, atendiendo el concepto del código fuente, es claro que, el conocer como está construido un sistema y por ende su funcionamiento, coloca en riesgo la seguridad informática del instituto y, de entregar tal información provocaría un riesgo a recibir ataques cibernéticos.

Lo anterior es necesario a fin de que este Instituto pueda cumplir con la función establecida en el inciso e) del párrafo primero del artículo 30 de la Ley General de Instituciones y Procedimientos Electorales, inherente a garantizar la celebración periódica y pacífica de las elecciones para renovar los cargos de los tres Poderes de la Unión, además de cumplir con la atribución constitucional de la capacitación electoral en los procesos electorales.

LGIPE **"Artículo 30.**

1. Son fines del Instituto:

(...)

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 electora/es locales;

(...)" (Sic).

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

La UNICOM expresa que, entregar la información relativa a códigos fuente y los documentos de diseño de los sistemas informáticos del instituto es contrario al interés público, ya que dar a conocer la información, implica otorgar elementos que podrían eventualmente hacer vulnerables los sistemas desarrollados con que cuenta el Instituto, con ello se pondera el ejercicio de los derechos políticos electorales de las y los ciudadanos mexicanos por encima del derecho de acceso a la información de una persona.

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

Así también, el área UNICOM precisó que hacer pública la información solicitada, podría desembocar un riesgo real de recibir intentos de ataques cibernéticos directamente enfocados en tratar de comprometer las cuestiones operativas del



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Instituto; la información requerida, puede ser utilizada para desarrollar ataques específicos diseñados para intentar vulnerar los mecanismos, herramientas, infraestructura y sistemas con los que cuenta el INE, en un momento determinado del proceso electoral en curso, o incluso, en cualquier otro momento, afectando así las actividades cotidianas que no se encuentran relacionadas con los procesos electorales.

De lo anterior, se deriva que no procede la entrega de la información requerida, en virtud de que resulta jurídicamente aplicable la reserva, invocando la causal de seguridad nacional y pública prevista en las leyes de transparencia aplicables

- **Temporalidad.** *El área UNICOM considera mantener como temporalmente reservada por un periodo de 5 años, la información relativa al códigos fuente y los documentos de diseño de los sistemas informáticos del instituto.*

Por lo antes expuesto, este CT estima adecuado:

- **Confirmar la clasificación de reserva temporal** realizada por el área (UNICOM), por el periodo de cinco años que empezaran a correr a partir la presente resolución, respecto la información relativa a códigos fuente y los documentos de diseño de los sistemas informáticos del INE.
(...).

Resolución

(...)

Segundo. Se confirma la manifestación de **reserva temporal** formulada por el área (UNICOM) en términos del considerando **III inciso A)**, de la presente resolución.
(...)"

8. El 3 de febrero de 2023, el área UTSI mediante oficio INE/UTSI/0440/2023, solicitó al CT del INE la ampliación del periodo de reserva de la información relativa a los códigos fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información con folio 2210000132618, por un periodo de cinco años adicionales en virtud de que subsisten las causas que dieron origen a la clasificación de reserva; en términos de los artículos 101, segundo párrafo de LGTAIP y 99, segundo párrafo de la LFTAIP y numerales trigésimo cuarto y trigésimo quinto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas (Lineamientos generales en materia de clasificación y desclasificación) emitidos por el



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

9. El 6 de febrero de 2023, se suspendieron los plazos en materia de Transparencia, Acceso a la Información y Protección de Datos Personales reanudándose el 7 de febrero de la misma anualidad, 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-0007-2022 y la circular INE/DEA/002/2023.
10. El 9 de febrero de 2023 se realizó un requerimiento de aclaración al área UTSI a través de correo electrónico, a efecto de que robusteciera la motivación de la causal prevista en los artículos 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP.
11. El 9 de febrero de 2023, el área UTSI dio respuesta al requerimiento de aclaración mediante correo electrónico y oficio sin número.
12. El 9 de febrero de 2023, la Secretaría Técnica (ST) del CT, por instrucciones del Presidente de dicho órgano convocó a sus integrantes y al área que solicitó la ampliación del plazo de reserva, para discutir el presente acuerdo.

CONSIDERANDOS

I. Competencia

El CT del INE es competente para emitir el presente Acuerdo, de conformidad con los artículos 44, fracción VIII de la LGTAIP, 65, fracción VIII de la LFTAIP, 24, párrafo 1, fracción IX del Reglamento, aprobado por el Consejo General del INE el 26 de agosto de 2020 y numerales décimo quinto, trigésimo cuarto, trigésimo quinto y trigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación, que establece como atribuciones de dicho órgano colegiado solicitar y autorizar la ampliación del plazo de reserva de la información a que se refiere el artículo 101 de la LGTAIP.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

II. Requisitos para la solicitud de ampliación de plazo de reserva

De conformidad con el numeral trigésimo quinto de los Lineamientos generales en materia de clasificación y desclasificación, para ampliar el periodo de reserva de la información, el titular del área del sujeto obligado deberá hacer la solicitud de ampliación del periodo de reserva al CT con tres meses de anticipación al vencimiento del mismo.

Cabe señalar que la reserva fue otorgada el 11 de mayo de 2018, por lo que los tres meses de anticipación inician el 11 de febrero de 2023.

Además, se desprenden los **requisitos** que deben acreditarse para agotar dicho procedimiento:

I. Los documentos o expedientes respecto de los cuales expira el plazo de reserva;

- De acuerdo con la solicitud del área **UTSI** el documento respecto del cual expira el plazo de reserva es respecto a la información relativa al código fuente y documentos de diseño de los sistemas desarrollados objeto de la solicitud de información con folio 2210000132618.

II. La fecha en que expira el plazo de reserva de dichos documentos o expedientes;

- El área **UTSI** señala que el plazo de reserva expira el 11 de mayo de 2023.
- El Comité verificó que la resolución mediante la cual se confirmó la reserva temporal fue emitida el 11 de mayo de 2018; lo cual coincide con el plazo señalado por la UTSI.

III. Las razones y fundamentos por las cuales se reservó originalmente la información, así como la aplicación de la prueba de daño donde se expresen las razones y fundamentos por las cuales se considera que debe de seguir clasificada, mismos que deberán guardar estrecha relación con el nuevo plazo de reserva propuesto, y

- El área **UTSI** señaló las razones y fundamentos, conforme a lo siguiente:



“(...)

Fundamentación de la ampliación del periodo de reserva

Hacer públicos los códigos fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información número de folio UE/18/01225 coloca a los actuales sistemas informáticos en riesgo de sufrir una vulneración de seguridad informática, esto en virtud de que, como ya se mencionó los códigos fuente y los documentos de diseño que se reservaron con motivo de la solicitud mencionada, actualmente siguen utilizándose para el desarrollo de sistemas actuales, por lo que el periodo de reserva de la información debe ampliarse por cinco años adicionales; lo anterior con fundamento en los artículos 110, fracciones I y VII de la LFTAIP, artículo 113, fracciones I y VII de la LGTAIP, mismos que se encuentran vinculados con el numeral décimo séptimo, fracción III de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas emitidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Lineamientos generales), de conformidad con lo siguiente:

Información reservada	Causal de reserva	¿Qué se tutela?
Códigos fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información número de folio UE/18/01225.	<ul style="list-style-type: none"> ▪ Artículo 110, fracciones I y VII de la LFTAIP. ▪ Artículo 113, fracciones I y VII de la LGTAIP. ▪ Numeral décimo séptimo, fracción III de los Lineamientos generales. 	<ul style="list-style-type: none"> ▪ Desarrollo de la vida democrática y, por ende, la Seguridad Nacional. ▪ Derecho a la protección de los datos personales en posesión de los sujetos obligados. ▪ Derecho al voto de las y los ciudadanos mexicanos.

Condiciones que sustentan la prueba de daño

1. 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;

Como ya se mencionó, la presente ampliación del periodo de clasificación de reserva encuentra su fundamento en el artículo 113, fracción I de la LGTAIP, así como en el artículo 110, fracción I de la LFTAIP, el cual se vincula con el numeral décimo séptimo, fracción III de los Lineamientos generales:



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Décimo séptimo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando:

[...]

I. Se amenace o ponga en riesgo la gobernabilidad democrática porque se impida el derecho a votar o a ser votado, o cuando se obstaculice la celebración de elecciones;

[...]

No obstante, también resulta aplicable el artículo 113, fracción VII de la LGTAIP, así como el artículo 110, fracción VII de la LFTAIP, ya que con la clasificación se busca **prevenir** aquellos **delitos** establecidos en los artículos 211 bis 1 y 211 bis 2 del Código Penal Federal mismos que señalan lo siguiente, respectivamente:

- 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 de multa.
- 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 de multa.

En este sentido es importante resaltar que si bien, anteriormente no se había citado la causal referente a prevención de delitos señalada en la fracción VII de los artículos 113 y 110 de la LGTAIP y de la LFTAIP, respectivamente, en esta prueba de daño que se pone a consideración se ha hecho un análisis respecto del porqué esta causal resulta aplicable al caso en concreto, para lo cual es importante tomar en consideración el tiempo en el cual fue emitida la prueba de daño que dio origen a la reserva y el tiempo en el cual es emitida la actual prueba de daño con la que se busca ampliar el periodo de reserva. En este sentido es importante señalar que en los últimos años han aumentado los riesgos de ciberataques, por lo cual se ha visto un incremento de robo de información, espionaje informático y hasta terrorismo cibernético lo cual se traduce en que con mayor frecuencia existen mayores ataques a las instituciones.

Sirve como referencia a lo anterior, lo señalado en el cuaderno de investigación número 87, denominado *Ciberseguridad, desafío para México y trabajo legislativo* publicado en Marzo del 2022, en el cual el Dr. Juan Pablo Aguirre Quezada destaca lo siguiente¹:

¹ Aguirre Quezada, J.P. (2022). "Ciberseguridad, desafío para México y trabajo legislativo" Cuaderno de investigación No. 87, Instituto Belisario Domínguez, Senado de la República, Ciudad México, 23p. [Cuaderno de Investigación 87.pdf \(senado.gob.mx\)](#)



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

[...]

Cabe destacar que, de acuerdo con la compañía Cisco, “los ciberdelitos crecen año a año a medida que las personas intentan beneficiarse de los sistemas comerciales vulnerables. A menudo, los atacantes buscan rescates: el 53 % de los ciberataques da como resultado daños por USD 500 000 o más” (Cisco, 2021). Por lo que este tipo de agresiones son chantajes o apropiaciones indebidas a bienes de empresas o instituciones públicas, lo cual afecta gravemente su patrimonio.

Los ciberataques en diferentes partes del mundo aumentaron en frecuencia en los últimos meses, al coincidir con un mayor uso de ordenadores debido a los estragos por la pandemia de covid-19. Al respecto, la compañía Kaspersky dio a conocer que, de enero a agosto de 2020 se incrementó en 24% el número de este tipo de incidentes en América Latina. Con ello, se realizan docenas de ataques por segundo en todo el continente, al referir que “Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto)” (Kaspersky, 2021). Lo cual es una muestra de la magnitud del riesgo actual por esta amenaza en esta región.

[...]

Por otra parte, de acuerdo con el Informe sobre seguridad emitido por la empresa de seguridad CHECK POINT², el año 2021 representó uno de los más turbulentos periodos registrados en lo que respecta a la ciberseguridad o seguridad informática. A medida que los gobiernos y los negocios en todo el mundo continúan los esfuerzos de la transformación digital, acelerados por la pandemia y la consecuente adopción de modalidades de trabajo de manera híbrida y remota, los agentes de amenaza no han perdido tiempo de ninguna manera en virar la situación para su propia ventaja, registrándose los siguientes incidentes de manera más significativa durante el año 2021:

² <https://pages.checkpoint.com/cyber-security-report-2022-spanish.html>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Enero de 2021	<p>El Departamento de Justicia de los Estados Unidos confirmó que había sido afectado por el ataque a la cadena de suministro del software <u>SolarWinds</u>³ y que se había accedido al 3% de los buzones de correo electrónico de sus empleados con el fin de robar datos confidenciales.</p> <p>El Departamento de Justicia compró <u>SolarWinds</u>, una herramienta ampliamente utilizada para monitoreo de redes de comunicaciones que fue intervenida por hackers, ocasionando que 18,000 clientes de <u>SolarWinds</u> experimentaran una vulneración.</p>
Febrero de 2021	<p>En <u>Febrero</u>, la conocida plataforma de transmisión de música, Spotify, se vio afectada por un ataque de re uso de credenciales, solo tres meses después de un incidente similar⁴.</p> <p>El ataque utilizó credenciales robadas de unas 100,000 cuentas de usuarios y aprovechó una base de datos de inicio de sesión de Spotify maliciosa.</p>
Marzo de 2021	<p>En <u>Marzo</u>, la empresa de ciberseguridad <u>Volexity</u> reportó una vulnerabilidad en la plataforma de colaboración de Microsoft Exchange Server⁵, la cual fue usada para robar información de las bandejas de correos de los usuarios.</p> <p>Se estimó que 250,000⁶ servidores fueron comprometidos, principalmente en Estados Unidos, Reino <u>Unido</u> así como la Autoridad Bancaria Europea, el Parlamento Europeo y la Comisión para el Mercado Financiero (CMF) de Chile.</p>

<<<<Continúa en la siguiente página>>>>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Abril de 2021	En abril del 2021, la Agencia de Seguridad Nacional de los Estados Unidos, por sus siglas en inglés (NSA), publicó un aviso en la que advirtió que un grupo de atacantes vinculado a Rusia los cuales aprovecharon cinco (5) vulnerabilidades contra objetivos en Estados Unidos mediante la obtención de credenciales de acceso al software de administración del fabricante <u>Solarwinds</u> . ⁷
Mayo de 2021	En mayo, un ataque de <u>ransomware</u> interrumpió las operaciones del sistema de oleoductos de la compañía Colonial Pipeline, dicha compañía pagó aproximadamente cinco (5) millones de dólares para recuperar su información. ⁸
Junio de 2021	En <u>Junio</u> , la compañía de carnes JBS ubicada en Estados Unidos, sufrió un ataque de <u>ransomware</u> , que afectó sus operaciones en Norteamérica y Australia, lo que obligó a la compañía a cerrar sus plantas en Estados Unidos. ⁹ El director de <u>JBS</u> , reveló que se pagó un rescate de 11 (once) millones de dólares a los ciberdelincuentes para recuperar su información.
Julio de 2021	En Julio, un grupo de atacantes conocido como " <u>REvil</u> " atacó mediante un <u>ransomware</u> a un proveedor de servicios administrados de tecnologías de la información llamado <u>Kaseya</u> , en la que se estima que 1000 compañías fueron afectadas y aprovechándose de una vulnerabilidad en la herramienta de monitoreo y gestión de actualizaciones, a los afectados se les solicitaron rescates entre los 45 (cuarenta y cinco) mil dólares y los 5 (cinco) millones de dólares. ¹⁰
Agosto de 2021	En <u>Agosto</u> , se registró el ataque de negación de servicio (DdoS) ocasionado por 20,000 equipos interconectados (botnet) conocido con el nombre de " <u>Mirai</u> ", teniendo como objetivo dispositivos del Internet de las Cosas (IoT por sus siglas en inglés) como cámaras de vigilancia y ruteadores. ¹¹
Septiembre de 2021	En septiembre, la empresa de investigación en ciberseguridad <u>Checkpoint</u> informó que existió un incrementado de certificados falsos de vacunación COVID-19 en <u>Telegram</u> , la venta de dichos certificados se extendió por 28 países. El

	precio de venta fue entre los 100 (cien) y 200 (doscientos dólares). ¹²
Octubre de 2021	En Octubre, el grupo de atacantes conocido como <u>REvil</u> , quienes fueron responsables de los ciberataques a las compañías <u>Kaseya</u> y JBS, sufrió un ataque a su infraestructura lo que causó el desmantelamiento de dicho grupo delictivo. ¹³
Noviembre de 2021	En Noviembre, " <u>Emotet</u> " uno de los <u>botnets</u> <u>mas</u> conocidos de la historia, volvió a operar después de 10 meses de haber sido inhabilitado, infectando equipos mediante un tipo de virus troyano conocido como <u>Trickbot</u> , descargando y ejecutando la versión más reciente " <u>Emotet</u> ". ¹⁴
Diciembre de 2021	En diciembre, se informó de una vulnerabilidad que afecta a la biblioteca de registros de Java conocida como <u>Log4j</u> ¹⁵ , dicha biblioteca está integrada en casi todos los servicios y aplicaciones de internet, entre los cuales destacan Twitter, Amazon, Minecraft y Microsoft. Además, se identificaron variaciones de dicha vulnerabilidad en menos de 24 horas.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

En este mismo sentido, se destaca del informe en comento que, durante 2021, los ataques cibernéticos globales contra las redes corporativas se han incrementado un 50% en comparación con el año 2020. La categoría "Educación/Investigación" lidera como el sector más atacado, con un promedio de 1,605 ataques por organización cada semana, mientras que la categoría "Gobierno/Militar" es el segundo sector más atacado con un promedio de 1,136 ataques cada semana y con un incremento de ataques durante 2022 del 47% respecto a 2021.

Por otra parte, en un informe emitido por la INTERPOL en el año 2020, se da cuenta de un aumento alarmante de los ciberataques durante la epidemia de COVID-19, dentro de las principales preocupaciones de cara al futuro señaladas en dicho informe, es que es altamente probable que la ciberdelincuencia siga aumentando a corto plazo debido a las vulnerabilidades asociadas al teletrabajo y la posibilidad de obtener mayores ganancias, por lo que los ciberdelincuentes seguirán ampliando sus actividades y concebirán unos modus operandi más avanzados y complejos³.

En este sentido, como se mencionó previamente tomando en consideración el momento actual en el cual se realiza la presente prueba de daño, es que la casual de reserva referente a la prevención de delitos toma relevancia, ya que como ha quedado demostrado en los últimos años los intentos de ataques cibernéticos han ido en aumento, más aún después de los estragos generados por la epidemia del COVID-19.

Ahora bien, para prevenir este tipo de delitos tipificados en el Código Penal resulta necesario un adecuado manejo de la información de los sistemas, de la infraestructura y en general de cualquier activo de las Tecnologías de la Información y Comunicaciones, ya que es en los sistemas donde se procesa y almacena la información que permite a este Instituto hacer frente a sus atribuciones, así como datos personales de las y los ciudadanos. En este sentido, cabe precisar que, los datos personales que se manejan en las compañías e instituciones independientemente del tamaño o actividad, son uno de los activos más valiosos para los hackers, por ello es uno de los elementos que más peligro corren ante un ciberataque⁴, en este sentido hacer pública la información referente a los códigos fuente y documentos de diseño de los sistemas institucionales, proporcionaría datos que hacen vulnerable a toda la

³Secretaría General de INTERPOL 200, quai Charles de Gaulle 69006 Lyon Francia https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

⁴ Aguirre Quezada, J.P. (2022). "Ciberseguridad, desafío para México y trabajo legislativo" Cuaderno de investigación No. 87, Instituto Belisario Domínguez, Senado de la República, Ciudad México, 23p. [Cuaderno de Investigación 87.pdf \(senado.gob.mx\)](https://www.senado.gob.mx/imagenes/2022/07/20220720_Cuaderno%20de%20Investigacion%2087.pdf)



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

información almacenada en los sistemas institucionales y con ello podría dar lugar a la consecución de delitos que se buscan prevenir.

Por otra parte, tanto la causal de reserva referente a “Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable” y la referente a “Obstruya la prevención o persecución de los delitos” coexisten actualmente, ya que por una parte los sistemas institucionales no solo son utilizados para los Procesos Electorales Federales, sino son utilizados en los Procesos Electorales Locales y, actualmente se encuentran en Proceso Electoral los estados de Coahuila y Estado de México, por lo cual al citar la causal referente a prevención de delitos se busca prevenir un delito que pudiera suscitarse al intentar tener un acceso no autorizado a los sistemas. Asimismo, no se debe perder de vista que en este año comienza el Proceso Electoral Federal 2023-2024, lo que refuerza el sustento de la reserva como un asunto de seguridad nacional, ya que se podría amenazar o poner en riesgo la gobernabilidad democrática del país porque se impida el derecho a votar o a ser votado, o cuando se obstaculice la celebración de elecciones.

- ***La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional.***

Con base en el artículo 29 de la Ley General de Instituciones y Procedimientos Electorales (LGIPE), el Instituto contará con los recursos presupuestarios, técnicos, humanos y materiales que requiera para el ejercicio directo de sus facultades y atribuciones.

El artículo 30 de la LGIPE establece que son fines de este Instituto, entre otros: contribuir al desarrollo de la vida democrática, asegurar a los ciudadanos 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 el Instituto, para el ejercicio de sus atribuciones, ha desarrollado diversos sistemas informáticos con el objeto de optimizar el uso de recursos humanos, materiales y financieros, y brindar mayor certeza a la ciudadanía en las diferentes actividades que tiene a su cargo, principalmente aquellas que están relacionadas con los procesos electorales y la renovación de los poderes públicos.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

*En este sentido, la información reservada corresponde al **código fuente y documentos de diseño de los sistemas informáticos** objeto de la solicitud de información número de folio UE/18/01225; de hacer pública dicha información colocaría en un estado de vulnerabilidad permanente a los sistemas informáticos de este Instituto, así como a la información bajo resguardo del INE; ya que el código fuente y los documentos de diseño contienen instrucciones concretas, escritas en un lenguaje de programación, con el que se desarrollan los sistemas de información institucionales, diagramas de arquitectura (tanto de software como de hardware) y esquemas de protección en materia de seguridad informática que dan soporte a dichos sistemas institucionales, es información que debe ser resguardada y protegida en todo momento, en virtud de que en manos de un tercero malicioso representa un mapa tecnológico que permite encontrar la ruta de menor resistencia para vulnerar la seguridad de la infraestructura tecnológica de este Instituto, lo que haría posible acceder a la información que se resguarda en los mismos, entre la que se encuentran datos personales de las y los ciudadanos, así como información que permite el adecuado desarrollo de la vida democrática del país, en consecuencia, de hacerse pública dicha información, coloca en riesgo los datos personales de la ciudadanía, el voto de las y los ciudadanos, los resultados electorales, así como la capacidad operativa de este Instituto para hacer frente a las atribuciones que le fueron conferidas en la Constitución Política de los Estados Unidos Mexicanos, ya que, reiterando lo manifestado, el código fuente y documentos de diseño de los sistemas informáticos continúa vigente en los sistemas que actualmente tiene en operación este Instituto.*

Debido lo anterior, en una ponderación de intereses, por un lado, está el derecho de acceso a la información y, por el otro, está la seguridad informática del Instituto Nacional Electoral, que visto en perspectiva y dadas las atribuciones con las que cuenta, se trata de un asunto de seguridad nacional ya que está relacionado con el mantenimiento del orden constitucional y la preservación de la democracia. Asimismo, como ya se mencionó a través de la ampliación del periodo de reserva se busca prevenir delitos tipificados en el Código Penal Federal. Por ello, en este caso en particular, se considera que ampliar el periodo de reserva de los códigos fuente y documentos de diseño de los sistemas informáticos representa un interés público superior al de acceder a la información.

De igual manera, es importante mencionar que, en el ejercicio de las atribuciones de esta Unidad, referentes a establecer y aplicar reglas, procedimientos y estándares en materia de seguridad informática, es que se realiza la presente ampliación del periodo de reserva, ya que los posibles daños que pudieran generarse con la difusión de la información rebasan en gran medida el posible daño que podría ocasionarse con la restricción de la información.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

En consecuencia, se considera que el riesgo al que se expondrían los sistemas informáticos del Instituto, y, por ende, la propia capacidad del Instituto para llevar a cabo sus funciones rebasa los intereses jurídicos tutelados de acceso a la información.

Con la intención de brindar mejor claridad sobre el riesgo que supone el proporcionar la información, se informa lo siguiente:

Información que se considera reservada	Riesgo	Daño y/o afectación que podría causar en caso de conocerse la información
Código fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información número de folio UE/18/01225.	<p>Es un riesgo demostrable ya que pondría en estado de vulnerabilidad permanente a los sistemas del Instituto puesto que el código fuente y los documentos de diseño de un sistema informático permiten conocer cómo está construido éste y su funcionamiento, otorgar la información representa colocar en un gran riesgo a la seguridad informática del Instituto ya que se estarían otorgando los algoritmos desarrollados para el funcionamiento de los sistemas.</p> <p>Adicionalmente, 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:</p> <p>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.</p>	<p>La información sobre la cual se pretende ampliar el periodo de reserva forma parte también de los sistemas con los que actualmente cuenta el INE, por lo que mediante técnicas de <i>hacking</i> se podría tener acceso no autorizado a los sistemas y con ello poder extraer información referente a datos personales de personas físicas, así como diversa información que permite a este Instituto hacer frente a sus atribuciones y con la cual es posible organizar y ejecutar los procesos electorales, por lo que de vulnerarse dichos sistemas se pondría en riesgo el garantizar que este Instituto pueda llevar a cabo de manera adecuada sus funciones.</p>

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

Al respecto, se debe precisar que la divulgación de la información supera el interés público general para ser difundida, pues si bien es cierto que la Ley señala que los sujetos obligados deben dar acceso a la información y que se encuentre en sus archivos, también lo es que la LFTAIP y la LGTAIP señalan que existe un régimen de excepción, así como los supuestos en los que pueda clasificarse la información como reservada, en este sentido, con la intención de ejemplificar de mejor manera el por qué resulta perjudicial el hacer pública la información para esta institución, se informa lo siguiente:



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

¿Cómo evita un daño este Instituto al no proporcionar la información?	¿Qué daño puede ocasionarse si la información se hace de conocimiento de la ciudadanía?
La información otorga elementos que podrían eventualmente hacer vulnerable a los sistemas informáticos del Instituto, por lo que al no hacerse pública se lograría evitar causar un daño a los datos personales de terceros, así como la correcta operación institucional.	La divulgación de la información da la posibilidad de construir un ataque focalizado que representaría un riesgo inminente para la operación de los sistemas, y con ello a la operación institucional. En este sentido, el riesgo al que se expondrían los sistemas y la propia capacidad del Instituto para llevar a cabo las funciones electorales rebasan los intereses jurídicos tutelados de acceso a la información.

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

Por cuanto hace a este rubro, resulta importante señalar que en los apartados que anteceden ha quedado demostrado que el hacer pública la información relativa al código fuente y a los documentos de diseño de los sistemas pone en riesgo:

- *El derecho al voto de las y los ciudadanos mexicanos.*
- *La protección de los datos personales de personas físicas.*
- *El desarrollo de la vida democrática y, por ende, la Seguridad Nacional.*

Finalmente, con la intención de ejemplificar que la limitación al acceso a la información se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, se realiza la siguiente prueba de proporcionalidad⁵:

Test de proporcionalidad	Cuestionamientos	Justificación
Principio de idoneidad	¿Cuál es el fin para ampliar el periodo de reserva de la información y su fundamento?	La finalidad es proteger la información contenida en los sistemas y prevenir el acceso no autorizado a estos, ya que como se ha reiterado anteriormente la información relativa a los códigos fuente y documentos de diseño objeto de la solicitud de información número de folio UE/18/01225, sigue

⁵ La presente prueba se toma como referencia la información de Cervantes B. (2018) *La prueba de daño a la luz del principio de proporcionalidad*. Estudios en Derecho a la Información. Por Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Volumen 6. <https://doi.org/10.22201/ij.25940082e.2018.6.12466>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Test de proporcionalidad	Cuestionamientos	Justificación
		utilizándose en sistemas actuales, es por ello que debe permanecer la reserva de la información. Lo anterior, conforme a lo establecido en los artículos 99 y 110, fracciones I y VII de la LFTAIP, así como en los artículos 101 y 113, fracciones I y VII de la LGTAIP, mismos que se encuentran vinculados con el numeral décimo séptimo, fracción III de los Lineamientos generales.
	¿Con la ampliación del periodo de reserva de la información es posible alcanzar dicho fin?	Se alcanza el fin con la ampliación del periodo reserva, toda vez que, al no conocer la información relativa al código fuente y a los documentos de diseño de los sistemas, se pueden prevenir ataques focalizados en vulnerar las medidas de seguridad.
Principio de Necesidad	¿Existen medios alternativos que puedan garantizar el acceso a la información sin poner en riesgo alguna causa de reserva?	Particularmente para el caso que nos ocupa, no existe alguna otra información que pueda hacerse pública, toda vez que son datos técnicos específicos.
Principio de proporcionalidad	¿Qué tan importante es para el interés público dar a conocer la información solicitada de acuerdo con el contexto del caso?	Si bien es importante transparentar la información con la que cuenta este Instituto, es más importante salvaguardar los derechos de protección de datos personales, el derecho al voto de las mexicanas y mexicanos y preservar el desarrollo de la vida democrática, así como prevenir delitos tipificados en el Código Penal Federal, puesto que la publicidad de la información obstaculizaría las acciones implementadas para evitar la comisión de los delitos establecidos en los artículos 211 bis 1 y 211 bis 2 del Código referido.
	¿Qué tan alto sería el riesgo de divulgar la información solicitada?	De dar a conocer la información el riesgo es alto, toda vez que contienen las características y detalles técnicos de los sistemas institucionales por lo que, otorgar dicha información compromete la seguridad de los sistemas y por ende, la certeza en los procesos electorales. Es importante resaltar que, la información en manos de un tercero y con intenciones maliciosas representa un mapa tecnológico que da la posibilidad de construir un ataque focalizado.

Test de proporcionalidad	Cuestionamientos	Justificación
	¿La intervención del derecho de acceso a la información está justificada por la importancia del fin que se persigue al reservar la información?	Se encuentra justificada, toda vez que, al poder acceder a la información resulta más perjudicial que beneficioso al poner en riesgo diversos derechos.

• **Circunstancias de modo, tiempo y lugar del daño.**

Los diferentes riesgos a los que se enfrentaría este Instituto pueden suscitarse de manera permanentemente.



INE-CT-AC-0002-2023

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:

Circunstancias	Explicación
Modo	Cualquier tipo de ataque mediante el acceso o intento de acceso a los sistemas informáticos.
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.
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 los sistemas informáticos.

- **Temporalidad de la ampliación del periodo de reserva**
*Habiendo considerado la prueba de daño realizada, así como la naturaleza de la información relativa a los códigos fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información número de folio UE/18/01225, se considera que el periodo de reserva debe ampliarse por 5 (cinco) años más. Lo anterior, de conformidad con los artículos 101; 113, fracciones I y VII de la Ley General de Transparencia y Acceso a la Información Pública; 99 y 110, fracciones I y VII de la Ley Federal de la misma materia y; el numeral décimo séptimo de los Lineamientos generales, preceptos que obedecen a los principios reactivos de este Instituto.
(...)"*

IV. Señalar el plazo de reserva por el que se solicita que se amplíe, el cual no puede exceder de cinco años; así como el acta donde el Comité de Transparencia haya aprobado la ampliación del plazo antes citado.

- El área **UTSI** indicó que solicita la ampliación de reserva por un plazo de cinco años adicionales en virtud de que subsisten las causas que dieron origen a la clasificación de reserva.

Asimismo, precisó que el 11 de mayo de 2018, mediante resolución **INE-CT-R-0291-2018** el CT del INE confirmó la reserva de la información propuesta por la UTSI por 5 años a partir de la emisión de la resolución.

Además, el numeral trigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación dispone:



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

“Trigésimo sexto. Para los casos previstos por la fracción II del Lineamiento Décimo quinto, el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo.

El Pleno de los organismos garantes deberá resolver la solicitud de ampliación del periodo de reserva dentro de los 60 días siguientes, contados a partir de aquél en que recibió la solicitud.

El Pleno de los organismos garantes, cuando así lo estime necesario, podrá requerir, a través del sistema que para tal efecto se implemente en la Plataforma Nacional, dentro de los cinco días contados a partir de la recepción de la solicitud de ampliación del periodo de reserva, para que entreguen la información que permita a los organismos garantes contar con más elementos para determinar sobre la procedencia o no de la solicitud de ampliación. Los sujetos obligados, darán contestación al requerimiento antes citado en un plazo de cinco días contados a partir de la recepción del requerimiento.

El plazo mencionado en el segundo párrafo del presente numeral se suspenderá, hasta en tanto no se cuenten con los elementos necesarios para determinar la procedencia de la solicitud de la ampliación del periodo de reserva, y se reanudará una vez que el requerimiento haya sido desahogado por los sujetos obligados.

En caso de negativa de la solicitud de ampliación del periodo de reserva, el sujeto obligado deberá desclasificar la información.

La falta de respuesta por parte del organismo garante será considerada como una afirmativa ficta y el documento mantendrá el carácter de reservado”.

A su vez, remite al décimo quinto de dichos Lineamientos que establece:

“Décimo quinto. Los documentos y expedientes clasificados como reservados serán públicos cuando:

- I.** Se extingan las causas que dieron origen a su clasificación;
- II.** Expire el plazo de clasificación, salvo cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de la Ley General salvo que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; en cuyo caso, el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva propuesto; por lo menos, con tres meses de anticipación al vencimiento del periodo;
- III.** Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información, o



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Capítulo”.

III. Reserva temporal parcial. Análisis del CT del INE

El área **UTSI**, clasificó como temporalmente reservada la información relativa a los códigos fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información con folio 2210000132618, por un plazo de cinco años adicionales al plazo de reserva aprobado mediante resolución INE-CT-R-0291-2018 de fecha 11 de mayo de 2018.

Cabe señalar que, en su solicitud primigenia de reserva, aprobada mediante resolución INE-CT-R-0291-2018 de fecha 11 de mayo de 2018, el área **UTSI** invocó como causal de reserva la señalada en los artículos 113, fracción I de la LGTAIP y, 110, fracción I de la LFTAIP, que refieren lo siguiente:

LGTAIP

“Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

...

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

(...)”.

LFTAIP

“Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

(...)”.

No obstante, en la solicitud de ampliación de plazo de reserva que nos ocupa, el área **UTSI**, de manera adicional a la causal invocada en su solicitud primigenia, invoca la causal señalada en los artículos 113, fracción VII de la LGTAIP y, 110, fracción VII de la LFTAIP, que refieren lo siguiente:

LGTAIP

“Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

(...)

VII. Obstruya la prevención o persecución de los delitos;

(...)”.

LFTAIP



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

“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;

(...).”

Al respecto, el área **UTSI** indicó que también resulta aplicable el artículo 113, fracción VII de la LGTAIP, así como el artículo 110, fracción VII de la LFTAIP, ya que con la clasificación se busca **prevenir** aquellos **delitos** establecidos en los artículos 211 bis 1 y 211 bis 2 del Código Penal Federal los cuales señalan lo siguiente, respectivamente:

- 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 de multa.
- 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 de multa.

En este sentido, el área resaltó que si bien, anteriormente no se había citado la causal referente a prevención de delitos señalada en la fracción VII de los artículos 113 y 110 de la LGTAIP y de la LFTAIP, respectivamente, en la prueba de daño que se pone a consideración se ha hecho un análisis respecto del por qué esta causal resulta aplicable al caso en concreto, para lo cual es importante tomar en consideración el tiempo en el cual fue emitida la prueba de daño que dio origen a la reserva y el tiempo en el cual es emitida la actual prueba de daño con la que se busca ampliar el periodo de reserva.

Es así que precisó que en los últimos años han aumentado los riesgos de ciberataques, por lo cual se ha visto un incremento de robo de información, espionaje informático y hasta terrorismo cibernético lo cual se traduce en que con mayor frecuencia existen mayores ataques a las instituciones.

Sirve como referencia a lo anterior, lo señalado en el cuaderno de investigación número 87, denominado *Ciberseguridad, desafío para México y trabajo legislativo* publicado en marzo del 2022, en el cual el Dr. Juan Pablo Aguirre Quezada destaca



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

lo siguiente⁶:

[...]

Cabe destacar que, de acuerdo con la compañía Cisco, “los ciberdelitos crecen año a año a medida que las personas intentan beneficiarse de los sistemas comerciales vulnerables. A menudo, los atacantes buscan rescates: el 53 % de los ciberataques da como resultado daños por USD 500 000 o más” (Cisco, 2021). Por lo que este tipo de agresiones son chantajes o apropiaciones indebidas a bienes de empresas o instituciones públicas, lo cual afecta gravemente su patrimonio.

Los ciberataques en diferentes partes del mundo aumentaron en frecuencia en los últimos meses, al coincidir con un mayor uso de ordenadores debido a los estragos por la pandemia de covid-19. Al respecto, la compañía Kaspersky dio a conocer que, de enero a agosto de 2020 se incrementó en 24% el número de este tipo de incidentes en América Latina. Con ello, se realizan docenas de ataques por segundo en todo el continente, al referir que “Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto)” (Kaspersky, 2021). Lo cual es una muestra de la magnitud del riesgo actual por esta amenaza en esta región.

[...].”

Por otra parte, el área refirió que de acuerdo con el Informe sobre seguridad emitido por la empresa de seguridad CHECK POINT⁷, el año 2021 representó uno de los más turbulentos periodos registrados en lo que respecta a la ciberseguridad o seguridad informática, ya que a medida que los gobiernos y los negocios en todo el mundo continúan los esfuerzos de la transformación digital, acelerados por la pandemia y la consecuente adopción de modalidades de trabajo de manera híbrida y remota, los agentes de amenaza no han perdido tiempo de ninguna manera en virar la situación para su propia ventaja, registrándose los siguientes incidentes de manera más significativa durante el año 2021:

Enero de 2021	El Departamento de Justicia de los Estados Unidos confirmó que había sido afectado por el ataque a la cadena de suministro del software SolarWinds ⁸ y que se había accedido al 3% de los buzones de correo electrónico de sus empleados con el fin de robar datos
----------------------	---

⁶ Aguirre Quezada, J.P. (2022). “Ciberseguridad, desafío para México y trabajo legislativo” Cuaderno de investigación No. 87, Instituto Belisario Domínguez, Senado de la República, Ciudad México, 23p. [Cuaderno de Investigación 87.pdf \(senado.gob.mx\)](#)

⁷ <https://pages.checkpoint.com/cyber-security-report-2022-spanish.html>

⁸ <https://www.theguardian.com/technology/2021/jan/06/doj-email-systems-solarwinds-hackers>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

	<p>confidenciales.</p> <p>El Departamento de Justicia compró SolarWinds, una herramienta ampliamente utilizada para monitoreo de redes de comunicaciones que fue intervenida por hackers, ocasionando que 18,000 clientes de SolarWinds experimentaran una vulneración.</p>
Febrero de 2021	<p>En febrero, la conocida plataforma de transmisión de música, Spotify, se vio afectada por un ataque de re uso de credenciales, solo tres meses después de un incidente similar⁹.</p> <p>El ataque utilizó credenciales robadas de unas 100,000 cuentas de usuarios y aprovechó una base de datos de inicio de sesión de Spotify maliciosa.</p>
Marzo de 2021	<p>En marzo, la empresa de ciberseguridad Volexity reportó una vulnerabilidad en la plataforma de colaboración de Microsoft Exchange Server¹⁰, la cual fue usada para robar información de las bandejas de correos de los usuarios.</p> <p>Se estimó que 250,000¹¹ servidores fueron comprometidos, principalmente en Estados Unidos, Reino Unido así como la Autoridad Bancaria Europea, el Parlamento Europeo y la Comisión para el Mercado Financiero (CMF) de Chile.</p>
Abril de 2021	<p>En abril del 2021, la Agencia de Seguridad Nacional de los Estados Unidos, por sus siglas en inglés (NSA), publicó un aviso en la que advirtió que un grupo de atacantes vinculado a Rusia los cuales aprovecharon cinco (5) vulnerabilidades contra objetivos en Estados Unidos mediante la obtención de credenciales de acceso al software de administración del fabricante Solarwinds.¹²</p>

⁹ <https://www.darkreading.com/attacks-breaches/spotify-hit-with-another-credential-stuffing-attack>

¹⁰ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855>

¹¹ <https://www.checkpoint.com/latest-cyber-attacks/microsoft-exchange-hack/>

¹² <https://www.fbi.gov/news/press-releases/press-releases/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabilities-to-compromise-us-and-allied-networks>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Mayo de 2021	En mayo, un ataque de ransomware interrumpió las operaciones del sistema de oleoductos de la compañía Colonial Pipeline, dicha compañía pagó aproximadamente cinco (5) millones de dólares para recuperar su información. ¹³
Junio de 2021	En junio, la compañía de carnes JBS ubicada en Estados Unidos, sufrió un ataque de ransomware que afectó sus operaciones en Norteamérica y Australia, lo que obligó a la compañía a cerrar sus plantas en Estados Unidos. ¹⁴ El director de JBS, reveló que se pagó un rescate de 11 (once) millones de dólares a los ciberdelincuentes para recuperar su información.
Julio de 2021	En Julio, un grupo de atacantes conocido como “REvil” atacó mediante un ransomware a un proveedor de servicios administrados de tecnologías de la información llamado Kaseya, en la que se estima que 1000 compañías fueron afectadas y aprovechándose de una vulnerabilidad en la herramienta de monitoreo y gestión de actualizaciones, a los afectados se les solicitaron rescates entre los 45 (cuarenta y cinco) mil dólares y los 5 (cinco) millones de dólares. ¹⁵
Agosto de 2021	En agosto, se registró el ataque de negación de servicio (DdoS) ocasionado por 20,000 equipos interconectados (botnet) conocido con el nombre de “Mirai”, teniendo como objetivo dispositivos del Internet de las Cosas (IoT por sus siglas en inglés) como cámaras de vigilancia y ruteadores. ¹⁶
Septiembre de 2021	En septiembre, la empresa de investigación en ciberseguridad Checkpoint informó que existió un incrementado de certificados falsos de vacunación COVID-19 en Telegram, la venta de dichos certificados se extendió por 28 países. El precio de venta fue entre los 100 (cien) y 200 (doscientos dólares). ¹⁷
Octubre de	En octubre, el grupo de atacantes conocido como REvil,

¹³ <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>

¹⁴ <https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs>

¹⁵ <https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689>

¹⁶ <https://thehackernews.com/2021/08/cloudflare-mitigated-one-of-largest.html>

¹⁷ <https://blog.checkpoint.com/2021/09/14/amid-vaccine-mandates-fake-vaccine-certificates-become-a-full-blown-industry/>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

2021	quienes fueron responsables de los ciberataques a las compañías Kaseya y JBS, sufrió un ataque a su infraestructura lo que causó el desmantelamiento de dicho grupo delictivo. ¹⁸
Noviembre de 2021	En noviembre, “Emotet” uno de los botnets mas conocidos de la historia, volvió a operar después de 10 meses de haber sido inhabilitado, infectando equipos mediante un tipo de virus troyano conocido como Trickbot, descargando y ejecutando la versión más reciente “Emotet”. ¹⁹
Diciembre de 2021	En diciembre, se informó de una vulnerabilidad que afecta a la biblioteca de registros de Java conocida como Log4j ²⁰ , dicha biblioteca está integrada en casi todos los servicios y aplicaciones de internet, entre los cuales destacan Twitter, Amazon, Minecraft y Microsoft. Además, se identificaron variaciones de dicha vulnerabilidad en menos de 24 horas.

Asimismo, el área destacó que del informe en comento se advierte que, durante 2021, los ataques cibernéticos globales contra las redes corporativas se han incrementado un 50% en comparación con el año 2020. La categoría “Educación/Investigación” lidera como el sector más atacado, con un promedio de 1,605 ataques por organización cada semana, mientras que la categoría “Gobierno/Militar” es el segundo sector más atacado con un promedio de 1,136 ataques cada semana y con un incremento de ataques durante 2022 del 47% respecto a 2021.

Por otra parte, señaló que en un informe emitido por la INTERPOL en el año 2020, se da cuenta de un aumento alarmante de los ciberataques durante la epidemia de COVID-19, dentro de las principales preocupaciones de cara al futuro señaladas en dicho informe, es que es altamente probable que la ciberdelincuencia siga aumentando a corto plazo debido a las vulnerabilidades asociadas al teletrabajo y la posibilidad de obtener mayores ganancias, por lo que los ciberdelinquentes seguirán ampliando sus actividades y concebirán unos *modus operandi* más

¹⁸ <https://techcrunch.com/2021/10/18/revil-ransomware-group-goes-dark-after-its-tor-sites-were-hijacked/?quccounter=1>

¹⁹ <https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action>

²⁰ <https://research.checkpoint.com/2021/the-laconic-log4shell-faq/>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

avanzados y complejos²¹.

En este sentido, señaló que tomando en consideración el momento actual en el cual se realiza la presente prueba de daño, es que la causal de reserva referente a la prevención de delitos toma relevancia, ya que como ha quedado demostrado en los últimos años los intentos de ataques cibernéticos han ido en aumento, más aún después de los estragos generados por la epidemia del COVID-19.

Es así que refirió que para prevenir este tipo de delitos tipificados en el Código Penal resulta necesario un adecuado manejo de la información de los sistemas, de la infraestructura y en general de cualquier activo de las Tecnologías de la Información y Comunicaciones, ya que es en los sistemas donde se procesa y almacena la información que permite a este Instituto hacer frente a sus atribuciones, así como datos personales de las y los ciudadanos. En este sentido, precisó que, los datos personales que se manejan en las compañías e instituciones independientemente del tamaño o actividad, son uno de los activos más valiosos para los *hackers*, por ello es uno de los elementos que más peligro corren ante un ciberataque²², en este sentido hacer pública la información referente a los códigos fuente y documentos de diseño de los sistemas institucionales, proporcionaría datos que hacen vulnerable a toda la información almacenada en los sistemas institucionales y con ello podría dar lugar a la consecución de delitos que se buscan prevenir.

Por otra parte, indicó que tanto la causal de reserva referente a “*Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable*” y la referente a “*Obstruya la prevención o persecución de los delitos*” coexisten actualmente, ya que por una parte los sistemas institucionales no solo son utilizados para los Procesos Electorales Federales, sino son utilizados en los Procesos Electorales Locales y, actualmente se encuentran en Proceso Electoral los estados de Coahuila y Estado de México, por lo cual al citar la causal referente a prevención de delitos se busca prevenir un delito que pudiera suscitarse al intentar tener un acceso no autorizado a los sistemas. Asimismo, indicó que no se debe perder de vista que en este año comienza el Proceso Electoral Federal 2023-2024, lo que refuerza el sustento de la

²¹Secretaría General de INTERPOL, 200, quai Charles de Gaulle 69006 Lyon Francia https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

²² Aguirre Quezada, J.P. (2022). “Ciberseguridad, desafío para México y trabajo legislativo” Cuaderno de investigación No. 87, Instituto Belisario Domínguez, Senado de la República, Ciudad México, 23p. [Cuaderno de Investigación 87.pdf \(senado.gob.mx\)](https://www.senado.gob.mx/contenido/documentos/15444)



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

reserva como un asunto de seguridad nacional, ya que se podría amenazar o poner en riesgo la gobernabilidad democrática del país porque se impida el derecho a votar o a ser votado, o cuando se obstaculice la celebración de elecciones.

En razón de lo anterior, se precisa que al entregar dicha información atentaría contra las obligaciones establecidas en el artículo 11, fracción VI de la LFTAIP por lo que se podría incurrir en las responsabilidades que señala el artículo 186 de la LFTAIP.

Es importante mencionar 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 LFTAIP en el entendido que dichos preceptos legales tienen el siguiente alcance:

Por lo anterior, se considera información temporalmente reservada, de conformidad con los artículos 110, fracciones I y VII de la LFTAIP, 113, fracciones I y VII de la LGTAIP y los numerales décimo séptimo, fracción III y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación.

De la descripción del área **UTSI**, se advierte que el código fuente es el conjunto de pasos que debe seguir un equipo de cómputo, servidor o dispositivo de procesamiento de datos, para ejecutar una tarea o instrucción -o un conjunto de estas- de forma automática; por lo que el código fuente y los documentos de diseño de un sistema informático permiten conocer cómo está construido éste, su funcionamiento y, en su caso, la forma en que procesa y/o almacena datos; otorgar la información representa colocar en un gran riesgo a la seguridad informática del Instituto ya que se estarían otorgando los algoritmos desarrollados para el funcionamiento de los sistemas actuales, por lo que debe permanecer la reserva de la información.

Asimismo, se advierte que si bien estos códigos y documentos de diseño fueron utilizados en los sistemas objeto de la solicitud 210000132618 actualmente, dicha información sigue utilizándose en los sistemas con los que cuenta el Instituto; en consecuencia, no pueden otorgarse los códigos fuente y documentos de diseño de los sistemas que se encontraban vigentes al momento de dar atención a la solicitud que dio origen a la reserva, ya que representaría un riesgo para los sistemas que actualmente operan en la institución y, más relevante aún, un riesgo para el adecuado control de acceso a la información que estos almacenan.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

De igual forma, en caso de hacer pública la información, es posible que un tercero malicioso ejecute ataques focalizados, ya que todos los ataques dan inicio con una etapa de reconocimiento durante la cual la persona hace uso de diversas técnicas que tienen como propósito recopilar y consolidar información técnica acerca de los sistemas que se pretenden vulnerar, así como de la infraestructura tecnológica subyacente, por lo que a partir de la obtención de información y ejecución de dichas técnicas, la persona atacante intenta reconstruir los elementos de diseño (código fuente, servidores, dispositivos de procesamiento de datos, servicios de autenticación), que coexisten en la red de datos, para documentar las versiones de dichos componentes, con el fin de dirigir ataques específicos, ya que con esta información se buscan componentes que podrían tener vulnerabilidades y mediante herramientas de ataque que permiten aprovechar las mismas, se podría afectar la seguridad de determinados sistemas que el Instituto utiliza para ejercer sus atribuciones, ya que se estarían otorgando los elementos necesarios para hacerlo.

Cabe señalar que, si se otorgan dichos elementos también se podría afectar la infraestructura en donde se alojan dichos sistemas con los que cuenta el Instituto Nacional Electoral y exponer la información que debe ser resguardada por éste; por lo tanto, se considera que esas agresiones serían potencialmente más riesgosas que aquellas que se pudieran generar sin el conocimiento exacto del código fuente y documentos de diseño.

En consecuencia, el riesgo al que se expondrían los sistemas informáticos del Instituto rebasa los intereses jurídicos tutelados de acceso a la información, ya que como se mencionó la información objeto de reserva actualmente sigue utilizándose para el desarrollo de los sistemas actuales.

Sirve como antecedente la resolución número EXT-15/CT/09/06/2022.04, emitida por el CT del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en la cual se confirma la solicitud de ampliación del periodo de reserva del expediente DGTI-PNT-001, relativa al código fuente de la PNT y el diagrama entidad relación de su base de datos, a solicitud de la Dirección General de Tecnologías de la Información del INAI. Para pronta referencia se cita el resolutivo primero de la resolución referida:

“PRIMERO. Se confirma la ampliación del plazo de reserva, por un periodo de cinco años del expediente DGTI-PNT-001 que contiene el código fuente de la Plataforma Nacional de Transparencia y diagrama entidad relación de su base de datos indicado por la Dirección General de Tecnologías de la Información.”



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Ahora bien, una vez señalado lo anterior esta autoridad tiene el deber de apearse en todo momento a las disposiciones legales, tal como se aprecia a continuación:

La LGTAIP y la LFTAIP, así como los Lineamientos generales en materia de clasificación y desclasificación reconocen, entre otras causales de reserva, las siguientes:

LGTAIP

“Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

...

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

...

*VII. Obstruya la prevención o persecución de los delitos;
(...)”.*

LFTAIP

“Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

...

*VII. Obstruya la prevención o persecución de los delitos;
(...)”.*

Lineamientos generales en materia de clasificación y desclasificación

“Décimo séptimo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando:

(...)

III. Se amenace o ponga en riesgo la gobernabilidad democrática porque se impida el derecho a votar o a ser votado, o cuando se obstaculice la celebración de elecciones;

(...).

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;



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

- 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”.*

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, fracciones I y VII de la LGTAIP, 110, fracciones I y VII de la LFTAIP y numerales décimo séptimo, fracción III y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación y 14, numeral 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, es un riesgo **demostrable** ya que pondría en estado de vulnerabilidad permanente a los sistemas del Instituto puesto que el código fuente y los documentos de diseño de un sistema informático permiten conocer cómo está construido éste y su funcionamiento, otorgar la información representa colocar en un gran riesgo a la seguridad informática del Instituto ya que se estarían otorgando los algoritmos desarrollados para el funcionamiento de los sistemas.

Adicionalmente, indicó que 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.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

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, ya que se encuentra relacionada con aspectos básicos de seguridad informática de los sistemas.

Asimismo, precisó que la información sobre la cual se pretende ampliar el periodo de reserva forma parte también de los sistemas con los que actualmente cuenta el INE, por lo que mediante técnicas de hacking se podría tener acceso no autorizado a los sistemas y con ello poder extraer información referente a datos personales de personas físicas, así como diversa información que permite a este Instituto hacer frente a sus atribuciones y con la cual es posible organizar y ejecutar los procesos electorales, por lo que de vulnerarse dichos sistemas se pondría en riesgo el garantizar que este Instituto pueda llevar a cabo de manera adecuada sus funciones.

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

El área **UTSI** señaló que la divulgación de la información supera el interés público general para ser difundida, pues si bien es cierto que la Ley señala que los sujetos obligados deben dar acceso a la información y que se encuentre en sus archivos, también lo es que la LFTAIP y la LGTAIP señalan que existe un régimen de excepción, así como los supuestos en los que pueda clasificarse la información como reservada, en este sentido, con la intención de ejemplificar de mejor manera el por qué resulta perjudicial el hacer pública la información para esta institución, informa lo siguiente:

¿Cómo evita un daño este Instituto al no proporcionar la información?	¿Qué daño puede ocasionarse si la información se hace de conocimiento de la ciudadanía?
La información otorga elementos que podrían eventualmente hacer vulnerable a los sistemas informáticos del Instituto, por lo que al no hacerse pública se lograría evitar causar un daño a los datos personales de terceros, así como la correcta operación institucional.	La divulgación de la información da la posibilidad de construir un ataque focalizado que representaría un riesgo inminente para la operación de los sistemas, y con ello a la operación institucional. En este sentido, el riesgo al que se expondrían los sistemas y la propia capacidad del Instituto para llevar a cabo las funciones electorales rebasan los intereses jurídicos tutelados de acceso a la información.

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



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

El área **UTSI** indicó que el hacer pública la información relativa al código fuente y a los documentos de diseño de los sistemas pone en riesgo:

- El derecho al voto de las y los ciudadanos mexicanos.
- La protección de los datos personales de personas físicas.
- El desarrollo de la vida democrática y, por ende, la Seguridad Nacional.

Finalmente, con la intención de ejemplificar que la limitación al acceso a la información se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, realiza la siguiente prueba de proporcionalidad²³:

Test de proporcionalidad	Cuestionamientos	Justificación
Principio de idoneidad	¿Cuál es el fin para ampliar el periodo de reserva de la información y su fundamento?	La finalidad es proteger la información contenida en los sistemas y prevenir el acceso no autorizado a estos, ya que como se ha reiterado anteriormente la información relativa a los códigos fuente y documentos de diseño objeto de la solicitud de información número de folio UE/18/01225, sigue

<<<<Continúa en la siguiente página>>>>

²³ La presente *prueba* se toma como referencia la información de Cervantes B. (2018) *La prueba de daño a la luz del principio de proporcionalidad*. Estudios en Derecho a la Información. Por Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Volumen 6. <https://doi.org/10.22201/ijj.25940082e.2018.6.12466>



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Test de proporcionalidad	Cuestionamientos	Justificación
		utilizándose en sistemas actuales, es por ello que debe permanecer la reserva de la información. Lo anterior, conforme a lo establecido en los artículos 99 y 110, fracciones I y VII de la LFTAIP, así como en los artículos 101 y 113, fracciones I y VII de la LGTAIP, mismos que se encuentran vinculados con el numeral décimo séptimo, fracción III de los Lineamientos generales.
	¿Con la ampliación del periodo de reserva de la información es posible alcanzar dicho fin?	Se alcanza el fin con la ampliación del periodo reserva, toda vez que, al no conocer la información relativa al código fuente y a los documentos de diseño de los sistemas, se pueden prevenir ataques focalizados en vulnerar las medidas de seguridad.
Principio de Necesidad	¿Existen medios alternativos que puedan garantizar el acceso a la información sin poner en riesgo alguna causa de reserva?	Particularmente para el caso que nos ocupa, no existe alguna otra información que pueda hacerse pública, toda vez que son datos técnicos específicos.
Principio de proporcionalidad	¿Qué tan importante es para el interés público dar a conocer la información solicitada de acuerdo con el contexto del caso?	Si bien es importante transparentar la información con la que cuenta este Instituto, es más importante salvaguardar los derechos de protección de datos personales, el derecho al voto de las mexicanas y mexicanos y preservar el desarrollo de la vida democrática, así como prevenir delitos tipificados en el Código Penal Federal, puesto que la publicidad de la información obstaculizaría las acciones implementadas para evitar la comisión de los delitos establecidos en los artículos 211 bis 1 y 211 bis 2 del Código referido.
	¿Qué tan alto sería el riesgo de divulgar la información solicitada?	De dar a conocer la información el riesgo es alto, toda vez que contienen las características y detalles técnicos de los sistemas institucionales por lo que, otorgar dicha información compromete la seguridad de los sistemas y por ende, la certeza en los procesos electorales. Es importante resaltar que, la información en manos de un tercero y con intenciones maliciosas representa un mapa tecnológico que da la posibilidad de construir un ataque focalizado.

Test de proporcionalidad	Cuestionamientos	Justificación
	¿La intervención del derecho de acceso a la información está justificada por la importancia del fin que se persigue al reservar la información?	Se encuentra justificada, toda vez que, al poder acceder a la información resulta más perjudicial que beneficioso al poner en riesgo diversos derechos.

Asimismo, señaló las circunstancias de modo, tiempo y lugar de la búsqueda de la información, en los siguientes términos:



INE-CT-AC-0002-2023

Circunstancias	Explicación
Modo	Cualquier tipo de ataque mediante el acceso o intento de acceso a los sistemas informáticos.
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.
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 los sistemas informáticos.

- **Plazo de reserva:** El área **UTSI** indicó que solicita la ampliación de reserva por un plazo de cinco años adicionales, en virtud de la prueba de daño realizada, así como la naturaleza de la información relativa a los códigos fuente y documentos de diseño de los sistemas informáticos, objeto de la solicitud de información número de folio UE/18/01225.
- Asimismo, precisó que el 11 de mayo de 2018, mediante resolución INE-CT-R-0291-2018 el CT del INE confirmó la reserva de la información propuesta por la UTSI por 5 años a partir de la emisión de la resolución.

Conclusión: En virtud de lo anterior el CT coincide con la ampliación del plazo de reserva propuesta por el área de **UTSI**, por un plazo de cinco años adicionales al plazo de reserva aprobado mediante resolución INE-CT-R-0291-2018 de fecha 11 de mayo de 2018, en términos de los artículos 113, fracciones I y VII de la LGTAIP, 110, fracciones I y VII de la LFTAIP y numerales décimo séptimo, fracción III y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación.

IV. Fundamento legal

A continuación, mencionamos las normas que sustentan el pronunciamiento del CT:

Artículos 44, fracción VIII de la LGTAIP, 65, fracción VIII de la LFTAIP, 24, párrafo 1, fracción IX del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública (Reglamento), aprobado por el



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Consejo General del INE el 26 de agosto de 2020 y numerales décimo quinto, trigésimo cuarto, trigésimo quinto y trigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación.

LGTAIP

*“Artículo 44. Cada Comité de Transparencia tendrá las siguientes funciones:
(...)”*

*VIII. Solicitar y autorizar la ampliación del plazo de reserva de la información a que se refiere el artículo 101 de la presente Ley, y
(...)”.*

LFTAIP

*“Artículo 65. Los Comités de Transparencia tendrán las facultades y atribuciones siguientes:
(...)”*

*VIII. Autorizar la ampliación del plazo de reserva de la información, a que se refiere el artículo 99 de esta Ley, y
(...)”.*

Reglamento

“Artículo 24.

De las funciones del Comité

1. Las funciones del Comité son:

(...)”

*IX. Solicitar y autorizar la ampliación del plazo de reserva de la información a que se refiere el artículo 101 de la Ley General de Transparencia;
(...)”.*

Lineamientos generales en materia de clasificación y desclasificación

“Décimo quinto. Los documentos y expedientes clasificados como reservados serán públicos cuando:

I. Se extingan las causas que dieron origen a su clasificación;

II. Expire el plazo de clasificación, salvo cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de la Ley General salvo que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; en cuyo caso, el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva propuesto; por lo menos, con tres meses de anticipación al vencimiento del periodo;

*III. Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información,
o*



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Capítulo.

Trigésimo cuarto. El periodo máximo por el que podría reservarse la información será de cinco años. El periodo de reserva correrá a partir de la fecha en que el Comité de Transparencia confirme la clasificación respectiva.

Los titulares de las áreas deberán determinar que el plazo de reserva sea el estrictamente necesario para proteger la información mientras subsistan las causas que dieron origen a la clasificación, salvaguardando el interés público protegido.

Asimismo, deberán señalar las razones por las cuales se estableció el plazo de reserva determinado y sustentadas en la prueba del daño.

Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el plazo de reserva hasta por un periodo de cinco años adicionales, siempre y cuando se justifique que subsisten las causas que dieron origen a su clasificación.

Trigésimo quinto. Para ampliar el periodo de reserva de la información, el titular del área del sujeto obligado deberá hacer la solicitud de ampliación del periodo de reserva al Comité de Transparencia con tres meses de anticipación al vencimiento del mismo, a través del sistema que para tal efecto se incluya en la Plataforma Nacional, en el que deberá señalar, como mínimo:

- I.** Los documentos o expedientes respecto de los cuales expira el plazo de reserva;
- II.** La fecha en que expira el plazo de reserva de dichos documentos o expedientes;
- III.** Las razones y fundamentos por las cuales se reservó originalmente la información, así como la aplicación de la prueba de daño donde se expresen las razones y fundamentos por las cuales se considera que debe de seguir clasificada, mismos que deberán guardar estrecha relación con el nuevo plazo de reserva propuesto, y
- IV.** Señalar el plazo de reserva por el que se solicita que se amplíe, el cual no puede exceder de cinco años; así como el acta donde el Comité de Transparencia haya aprobado la ampliación del plazo antes citado.

Trigésimo sexto. Para los casos previstos por la fracción II del Lineamiento Décimo quinto, el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo.

El Pleno de los organismos garantes deberá resolver la solicitud de ampliación del periodo de reserva dentro de los 60 días siguientes, contados a partir de aquél en que recibió la solicitud.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

El Pleno de los organismos garantes, cuando así lo estime necesario, podrá requerir, a través del sistema que para tal efecto se implemente en la Plataforma Nacional, dentro de los cinco días contados a partir de la recepción de la solicitud de ampliación del periodo de reserva, para que entreguen la información que permita a los organismos garantes contar con más elementos para determinar sobre la procedencia o no de la solicitud de ampliación. Los sujetos obligados, darán contestación al requerimiento antes citado en un plazo de cinco días contados a partir de la recepción del requerimiento.

El plazo mencionado en el segundo párrafo del presente numeral se suspenderá, hasta en tanto no se cuenten con los elementos necesarios para determinar la procedencia de la solicitud de la ampliación del periodo de reserva, y se reanudará una vez que el requerimiento haya sido desahogado por los sujetos obligados.

En caso de negativa de la solicitud de ampliación del periodo de reserva, el sujeto obligado deberá desclasificar la información.

La falta de respuesta por parte del organismo garante será considerada como una afirmativa ficta y el documento mantendrá el carácter de reservado”.

ACUERDO

Primero. Ampliación de plazo de reserva. Se aprueba la ampliación de plazo de reserva de la información relativa a los códigos fuente y documentos de diseño de los sistemas informáticos objeto de la solicitud de información con folio 2210000132618, por un plazo de cinco años adicionales al plazo de reserva aprobado mediante resolución INE-CT-R-0291-2018 de fecha 11 de mayo de 2018, de conformidad con lo previsto en los artículos 101 de la LGTAIP y 99 de la LFTAIP y en términos de los artículos 113, fracciones I y VII de la LGTAIP, 110, fracciones I y VII de la LFTAIP y numerales décimo séptimo, fracción III y vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación.

Segundo. Se pone a disposición del organismo garante el oficio INE/UTSI/0440/2023, el documento denominado ampliación del periodo de reserva-requerimiento, la resolución número INE-CT-R-0291-2018 emitida por el CT del INE de fecha 11 de mayo de 2018, la resolución número EXT-15/CT/09/06/2022.04, emitida por el CT y la presente resolución.

Tercero. Se instruye a la ST de este CT a hacer del conocimiento del organismo garante el presente acuerdo y realizar la solicitud y autorización de ampliación de



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

plazo. En términos de los artículos 44, fracción VIII de la LGTAIP, 65, fracción VIII de la LFTAP y el numeral trigésimo sexto de Lineamientos generales en materia de clasificación y desclasificación.

Notifíquese al organismo garante y al área responsable **UTSI** por la herramienta electrónica correspondiente.

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

Autorizó: SLMV Supervisó: MAAR Elaboró: ANRC

“Este documento ha sido firmado electrónicamente en atención a lo establecido por el Acuerdo INE/CG82/2020 emitido por el Consejo General del INE por el que se determinó suspender los plazos como una de las medidas preventivas y de actuación con motivo de la pandemia del COVID-19 y 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 las Unidades de Transparencia 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/DGEPPPOEP/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.



INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2023

Acuerdo del Comité de Transparencia (CT) del Instituto Nacional Electoral (INE) en atención a la solicitud de ampliación de plazo de reserva de la información correspondiente a la solicitud de acceso a la información **2210000132618 (UT/18/01225)**.

El presente acuerdo fue aprobado por unanimidad de votos de los integrantes del Comité de Transparencia, en Sesión Extraordinaria Especial celebrada el 10 de febrero de 2023.

Lic. Adrián Gerardo Pérez Cortes SUPLENTE DEL PRESIDENTE CON DERECHO A VOTO	Asesor de Consejero Presidente, en su carácter de Suplente del Presidente del Comité de Transparencia
Mtro. Agustín Pavel Ávila García INTEGRANTE SUPLENTE CON DERECHO A VOTO	Asesor del Secretario Ejecutivo, en su carácter de Integrante Suplente del Comité de Transparencia
Mtra. Cecilia del Carmen Azuara Arai INTEGRANTE TITULAR CON DERECHO A VOTO	Titular de la Unidad Técnica de Transparencia y Protección de Datos Personales, en su carácter de Integrante del Comité de Transparencia
Lic. Ivette Alquicira Fontes	Directora de Acceso a la Información y Protección de Datos Personales, en su carácter de Secretaria Técnica (titular) del Comité de Transparencia

