INSTITUTO NACIONAL ELECTORAL

INE-CT-AC-0002-2024

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 2210000113819 (UT/19/01095)

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).

A n t e c e d e n t e s

1. El 22 de mayo de 2019, ingresó la solicitud con folio 2210000113819, mediante la Plataforma Nacional de Transparencia (PNT) y la Unidad Técnica de Transparencia y Protección de Datos Personales (UTTyPDP) la tuvo por recibida.

2. El 23 de mayo de 2019, la solicitud de información 2210000113819 (UT/19/01095), se turnó a través del Sistema INFOMEX-INE a la Unidad Técnica de Servicios de Informática (UTSI).

3. El 28 de mayo de 2019, la UTSI emitió respuesta a la solicitud información 2210000113819 (UT/19/01095).

4. El 6 de junio de 2019, el CT del INE aprobó la resolución INE-CT-R-0124-2018[1], mediante la cual determinó, entre otros aspectos, lo siguiente:

Por lo antes expuesto, este CT estima adecuado:

- Confirmar la clasificación de reserva temporal realizada por el área (UNICOM), por el periodo de 5 años, respecto del número de ataques cibernéticos que ha recibido el INE de diciembre de 2018 la fecha.

5. El 7 de marzo de 2024, el área **UTSI** mediante oficio INE/UTSI/1372/2024, solicitó al CT del INE la ampliación del plazo de reserva de la información referente a todos los detalles de los intentos de ataques a los sistemas informáticos del

[1] Cabe señar que, si bien la resolución se establece que es del año 2018, lo cierto es que la citada resolución fue aprobada el 6 de junio de 2019.

Instituto y de manera particular, lo relativo a la fecha, lugar y tipo de estos que se ubiquen en el periodo comprendido del 1 de diciembre de 2018 al 23 de mayo de 2019 (fecha de recepción de la solicitud de información UT/19/01095), por un plazo de cinco años adicionales; en términos de los artículos 101, segundo párrafo de LGTAIP y 99, segundo párrafo de la LFTAIP, así como con fundamento en los lineamientos trigésimo cuarto y trigésimo quinto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos generales en materia de clasificación y desclasificación).

Es importante puntualizar que el área señaló que la reserva primigenia que confirmó el Comité de Transparencia mediante resolución INE-CT-R-0124-2018, además de los detalles de los intentos de ataques, se reservó también el número de intentos de ataques por el plazo de 5 años, no obstante, mediante la resolución al Recurso de Revisión RRA 12927/20, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), determinó que el **número de ataques** no sea considerado como información reservada, de conformidad con lo siguiente:

> *[…]*
>
> *En ese tenor, para el caso en concreto, el sujeto obligado en cuestión clasificó la información con respecto al requerimiento número uno, el cual versa sobre el número de ataques cibernéticos que ha registrado y sufrido el Instituto Nacional Electoral, en el cual señaló que se estarían exponiendo los mecanismos, herramientas y sistemas con los que el sujeto obligado cuenta para garantizar la seguridad informática de todos los procesos sistematizados que implementa y ejecuta, así como su funcionamiento, situación que pondría en riesgo la capacidad del sujeto obligado.*
>
> *No obstante, del análisis del dato requerido por el ahora recurrente en el numeral primero de la solicitud, es decir, número de ataques cibernéticos que ha registrado y sufrido no se advierte de qué forma podría vulnerar los sistemas de infraestructura informáticos del sujeto obligado y mucho menos se desprende que derivado de la entrega de este tipo de información pudiera generarse alguna de estas consecuencias:*
>
> *• Que la información que se solicita puede ser utilizada para desarrollar ataques específicamente diseñados para intentar vulnerar los mecanismos, herramientas, infraestructura y sistemas con los que cuenta el sujeto obligado, afectando así las actividades cotidianas del Instituto, sean éstas relacionadas o no, con los procesos electorales.*

> *• El proporcionar dicha información se pondría al sujeto obligado en un estado de vulnerabilidad y riesgo real, en relación con diversos ataques ocurridos en todo el mundo, por lo que sería un riesgo real la seguridad del Instituto Nacional Electoral y latente de sufrir intentos de ataques o acceso no autorizados a la red del sujeto obligado.*

En este sentido, la solicitud de ampliación de reserva que a continuación se presenta, versa únicamente respecto de los detalles de los intentos de ataques cibernéticos que ha sufrido el Instituto.

6. El 8 de marzo 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.

C o n s i d e r a n d o s

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 del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública (Reglamento), aprobado por el Consejo General del INE el 26 de agosto de 2020 y numerales décimo quinto, trigésimo cuarto, trigésimo quinto y trigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación, que establecen 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.

II. Previo y especial pronunciamiento

El 10 de febrero de 2023, el INE, promovió ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) la solicitud de ampliación del plazo de reserva, de la información correspondiente a la solicitud de acceso a la información 2210000132618 (UT/18/01225).

El 1 de marzo del año en curso el Pleno del INAI resolvió mediante resolución SAPR 1/23, lo siguiente:

> *“PRIMERO. Declarar improcedente Solicitud de ampliación del plazo de reserva, con fundamento en el artículo 99, último párrafo de la Ley Federal*

> *de Transparencia y Acceso a la Información Pública, y el numeral Noveno de los Lineamientos que establecen el Procedimiento para la atención de solicitudes de ampliación del periodo de reserva por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales".*

Lo anterior de conformidad con el Considerando Segundo, que señala lo siguiente:

> *"SEGUNDO. ANÁLISIS DE PROCEDENCIA.*
> *(…)*
>
> *Finalmente, la Ponencia a la que se le turne la solicitud de ampliación será la encargada de analizar la petición a efecto de determinar su procedencia y de elaborar el proyecto de resolución respectivo donde se verifique la existencia de circunstancias similares a aquéllas acontecidas en el momento en que se clasificó la información.*
>
> *Señalado lo anterior, es importante destacar que la ampliación del plazo de reserva puede llevarse a cabo bajo 2 procedimientos distintos y circunstancias específicas.*
>
> *El primero, de aprobación interna y generalizada, que consiste en la posibilidad de ampliar el periodo de reserva por primera vez, cualquiera que fuera el supuesto de los previstos en el artículo 110 de la Ley Federal, por un periodo de 5 años adicionales, el cual está sujetó sólo a la aprobación del Comité de Transparencia del sujeto obligado y que se acredite que subsisten las causas que dieron origen a su clasificación.*
>
> *Por otra parte, el segundo, de aprobación externa y limitada, que deriva en la posibilidad de ampliar por una segunda ocasión el plazo de reserva, siempre que:*
>
> *• La información 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 previstas en la fracción IV del artículo 110 de la Ley Federal.*
>
> *• El Comité de Transparencia haga la solicitud correspondiente al Instituto, 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.*
>
> *• Exista una primera ampliación del plazo de reserva.*
>
> *Establecido lo anterior, debe precisarse que, de la revisión a las constancias ofrecidas por el sujeto obligado, se tiene que la clasificación de la información*

surgió con motivo de la presentación de la solicitud de información 2210000132618 y que de origen fue reservada por un periodo de 5 años, mediante resolución INE-CT-R-0291-2018 del Comité de Transparencia del Instituto Nacional Electoral el 11 de mayo de 2018.

Así, una vez trascurrido el plazo de reserva de la información, a través del Acuerdo INE-CT-AC-0002-2023 de la Sesión Extraordinaria Especial del Comité de Transparencia, celebrada el 10 de febrero de 2023, se aprobó la primera ampliación del plazo de reserva por un periodo de 5 años más, con base en el artículo 113, fracciones I y VII de la Ley General de Transparencia y Acceso a la Información Pública.

Lo cual deviene relevante, pues atendiendo a los elementos para acreditar la procedencia de la solicitud de ampliación del plazo de reserva, el caso que nos ocupa se ubica en el relativo al proceso de aplicación interna y generalizada, pues se trata de la primera vez que se amplía el plazo de reserva, cuya aprobación recae en el Comité de Transparencia del sujeto obligado, y no de este Instituto.

Hecho que se refuerza, al tomar en consideración que el sujeto obligado ya aprobó la ampliación del plazo de reserva, requiriendo a este Instituto únicamente que se autorice la procedencia de la misma.

Lo cual resulta innecesario, ya que por el momento en el que se encuentra dicho proceso de ampliación, al ser la primera de ellas, la potestad para resolver sobre su procedencia es interna, es decir, propia del sujeto obligado, y no de este Instituto, el cual debe ser requerido e interviene, en el momento en el que vaya a expirar el plazo de la primera ampliación del plazo.

En mérito de lo anterior, se concluye que la solicitud de ampliación del plazo de reserva promovida por el sujeto obligado ante este Instituto no reúne los requisitos de procedencia previstos en la Ley Federal, los Lineamientos de clasificación y los Lineamientos de ampliación, pues se trata de la primera aprobación de la ampliación, la cual recae de manera particular en el Comité de Transparencia del sujeto obligado.

Por lo tanto, con base en el artículo 99, último párrafo de la Ley Federal, y el numeral Noveno de los Lineamientos de ampliación, resulta improcedente la solicitud de ampliación del plazo de reserva promovida por el Instituto Nacional Electoral.

Cabe precisar, que con la presente resolución no se deja sin efectos ni se trastoca la determinación adoptada por el sujeto obligado, por medio de la cual aprobó ampliar por primera vez y por un periodo de 5 años la información correspondiente, ya que no es posible pronunciarse respecto si ésta es

> *procedente o no, y por ende, esta resolución tampoco tiene efectos de validación sobre la ampliación del plazo referida por el sujeto obligado.*
> *(…)".*

Asimismo, el 17 de febrero de 2023, el INE, promovió ante el INAI la solicitud de ampliación del plazo de reserva, de la información correspondiente a la solicitud de acceso a la información 2210000170218 (UT/18/01586).

El 1 de marzo del año en curso el Pleno del INAI resolvió mediante resolución SAPR 2/23, lo siguiente:

> *"PRIMERO. Con fundamento en el artículo 99, último párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública, y el numeral Noveno de los Lineamientos que establecen el Procedimiento para la atención de solicitudes de ampliación del periodo de reserva por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, se declara improcedente la solicitud de ampliación del plazo de reserva."*

Lo anterior de conformidad con el Considerando Segundo, que señala lo siguiente:

> *"SEGUNDO.*
> *(…)*
> *Finalmente, la Ponencia a la que se le turne la solicitud de ampliación será la encargada de analizar la petición a efecto de determinar su procedencia y de elaborar el proyecto de resolución respectivo donde se verifique la existencia de circunstancias similares a aquéllas acontecidas en el momento en que se clasificó la información.*
>
> *Señalado lo anterior, es importante destacar que la ampliación del plazo de reserva puede llevarse a cabo bajo 2 procedimientos distintos y circunstancias específicas.*
>
> *El primero, de aprobación interna y generalizada, que consiste en la posibilidad de ampliar el periodo de reserva por primera vez, cualquiera que fuera el supuesto de los previstos en el artículo 110 de la Ley Federal, por un periodo de 5 años adicionales, el cual está sujetó solo a la aprobación del Comité de Transparencia del sujeto obligado y que se acredite que subsisten las causas que dieron origen a su clasificación.*
>
> *El segundo, de aprobación externa y limitada, que deriva en la posibilidad de ampliar por una segunda ocasión el plazo de reserva, siempre que:*

• La información 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 previstas en la fracción IV del artículo 110 de la Ley Federal;
• El Comité de Transparencia haga la solicitud correspondiente al Instituto, 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, y

• Exista una primera ampliación del plazo de reserva.

Establecido lo anterior, debe precisarse que, de la revisión a las constancias ofrecidas por el sujeto obligado, se tiene que la clasificación de la información surgió con motivo de la presentación de la solicitud de información 2210000170218 y que de origen fue reservada por un periodo de 5 años, mediante el acta INE-CT-R- 0324-2018 del Comité de Transparencia del Instituto Nacional Electoral, de fecha 17 de mayo de 2018.

Así, una vez trascurrido el plazo de reserva de la información, a través del Acta de la Sesión Extraordinaria Especial del Comité de Transparencia del Instituto Nacional Electoral, de fecha 16 de febrero de 2023, se aprobó la primera ampliación del plazo de reserva por un periodo de 5 años más, con base en el artículo 110, fracciones I y VII de la Ley Federal de la materia.

Lo cual deviene relevante, pues atendiendo a los elementos para acreditar la procedencia de la solicitud de ampliación del plazo de reserva, el caso que nos ocupa se ubica en el relativo al proceso de aplicación interna y generalizada, pues se trata de la primera vez que se amplía el plazo de reserva, cuya aprobación recae en el Comité de Transparencia del sujeto obligado, y no de este Instituto.

Hecho que se refuerza, al tomar en consideración que el sujeto obligado ya aprobó la ampliación del plazo de reserva, requiriendo a este Instituto únicamente que se pronuncie de manera definitiva sobre la procedencia de la misma.

Lo cual resulta innecesario, ya que por el momento en el que se encuentra dicho proceso de ampliación, al ser la primera de ellas, la potestad para resolver sobre su procedencia es interna, es decir, propia del sujeto obligado, y no de este Instituto, el cual debe ser requerido e interviene, en el momento en el que vaya a expirar el plazo de la primera ampliación del plazo.

En mérito de lo anterior, se concluye que la solicitud de ampliación del plazo de reserva promovida por el sujeto obligado ante este Instituto no reúne los requisitos de procedencia previstos en la Ley Federal, los Lineamientos de clasificación y los Lineamientos de ampliación, pues se trata de la primera

> *aprobación de la ampliación, la cual recae de manera particular en el Comité de Transparencia del sujeto obligado.*
>
> *Por lo tanto, con base en el artículo 99, último párrafo de la Ley Federal, y el numeral Noveno de los Lineamientos de ampliación, resulta improcedente la solicitud de ampliación del plazo de reserva promovida por el Instituto Nacional Electoral.*
>
> *Cabe precisar, que con la presente resolución no se deja sin efectos ni se trastoca la determinación adoptada por el sujeto obligado, por medio de la cual aprobó ampliar por primera vez y por un periodo de 5 años la información correspondiente, ya que no es posible pronunciarse respecto si esta es procedente o no y, por ende, esta resolución tampoco tiene efectos de validación sobre la ampliación del plazo referida por el sujeto obligado.*
> *(…)".*

Por lo anteriormente expuesto, en virtud de la interpretación que realiza el INAI a la extensión para ampliar el plazo de reserva, el CT procederá a analizar la propuesta que realiza la UTSI para el caso que nos ocupa.

III. 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 plazo de reserva de la información, el titular del área del sujeto obligado deberá hacer la solicitud de ampliación del plazo de reserva al CT con tres meses de anticipación al vencimiento del mismo.

Cabe señalar que la reserva fue otorgada el 6 de junio de 2019, por lo que los tres meses de anticipación inician el 6 de marzo de 2024.

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** señaló que subsisten las causas que dieron origen a la clasificación de reserva, respecto a la información referente a todos los detalles de los intentos de ataques a los sistemas informáticos del Instituto y de manera particular, lo relativo a la fecha, lugar y tipo de estos que se ubiquen

en el periodo comprendido del 1 de diciembre de 2018 al 23 de mayo de 2019, y que fue objeto de la solicitud de información con números de folio2210000113819, por un plazo de cinco años adicionales.

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 6 de junio de 2024.

- El Comité verificó que la resolución mediante la cual se confirmó la reserva temporal fue emitida el 6 de junio de 2019; 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 pública la información relativa a los detalles de los intentos de ataques cibernéticos a los sistemas informáticos del Instituto, específicamente lo referente a la fecha, lugar y tipo, objeto de la solicitud de información con número de folio UT/19/01095 coloca a la seguridad de la infraestructura, redes, sistemas y en general tecnologías de la información y comunicaciones del INE, en riesgo de sufrir una vulneración en materia de seguridad informática, esto en virtud de que, como ya se mencionó, la información que se reservó con motivo de la citada solicitud, con independencia de la temporalidad de que se trate, pues nada asegura que la información que hoy se entregue pueda o no ser usada con posterioridad, sin necesidad de que un proceso electoral se encuentre en curso, 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?*
Detalles de los intentos de ataques cibernéticos a los sistemas informáticos del Instituto, por el periodo comprendido del 1 de diciembre de 2018 al 23 de mayo de 2019, información objeto de la solicitud con número de folio UT/19/01095.	▪ *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.*	▪ *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;

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:

> ***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;*

Asimismo, 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 casual referente a prevención de delitos señalada en la fracción VII de los artículos 113 y 110 de a 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 siguiente[2]:

[…]

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.

[2] 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)

[…]
Por otra parte, de acuerdo con el Informe sobre seguridad emitido por la empresa de seguridad CHECK POINT3, 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:

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[3] y que se había accedido al 3% de los buzones de correo electrónico de sus empleados con el fin de robar datos confidenciales.* *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.*
Febrero de 2021	*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 similar[4].* *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.*
Marzo de 2021	*En marzo, la empresa de ciberseguridad Volexity reportó una vulnerabilidad en la plataforma de colaboración de Microsoft Exchange Server[5], la cual fue usada para robar información de las bandejas de correos de los usuarios.* *Se estimó que 250,000[6] 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.*
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 Solarwinds.[7]*

[3] https://www.theguardian.com/technology/2021/jan/06/doj-email-systems-solarwinds-hackers
[4] https://www.darkreading.com/attacks-breaches/spotify-hit-with-another-credential-stuffing-attack
[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
[6] https://www.checkpoint.com/latest-cyber-attacks/microsoft-exchange-hack/
[7] https://www.fbi.gov/news/press-releases/press-releases/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabilities-to-compromise-us-and-allied-networks

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.*[8]
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.* [9] *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.*[10]
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 objetivos 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 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).* [12]
Octubre de 2021	*En octubre, el grupo de atacantes conocido como REvil, 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.*[13]
Noviembre de 2021	*En noviembre, "Emotet" uno de los botnets más 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".*[14]
Diciembre de 2021	*En diciembre, se informó de una vulnerabilidad que afecta a la biblioteca de registros de Java conocida como Log4j*[15]*, dicha biblioteca está integrada en casi todos los servicios y aplicaciones de internet, entre los cuales destacan Twitter, Amazon, Minecraft*

[8] https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
[9] https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs
[10] https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689
[11] https://thehackernews.com/2021/08/cloudflare-mitigated-one-of-largest.html
[12] https://blog.checkpoint.com/2021/09/14/amid-vaccine-mandates-fake-vaccine-certificates-become-a-full-blown-industry/
[13] https://techcrunch.com/2021/10/18/revil-ransomware-group-goes-dark-after-its-tor-sites-were-hijacked/?guccounter=1
[14] https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action
[15] https://research.checkpoint.com/2021/the-laconic-log4shell-faq/

	y Microsoft. Además, se identificaron variaciones de dicha vulnerabilidad en menos de 24 horas.

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 complejos[16]*.*

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.

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 ciberataque18. En esa tesitura, hacer pública la información referente a los intentos por vulnerar la seguridad de los sistemas informáticos de los servicios de telecomunicaciones del Instituto, 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.

[16]Secretaría 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

Por otra parte, tanto la casual 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 "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" coexisten actualmente, ya que por una parte no hay algún otro organismo en el país que ejecute las funciones que le han sido conferidas constitucional y legalmente al Instituto, las cuales son exclusivas de este. Aunado a ello, es de suma importancia precisar que dichas actividades se desarrollan cotidianamente, y no necesariamente se circunscriben a los procesos electorales federales o locales, sino que se desarrollan día con día con motivo de sus funciones. Asimismo, no se debe perder de vista que en este año se está llevando a cabo 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. Por su parte, 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.

En esa tesitura, se desprende que, para el ejercicio de sus funciones, el Instituto se apoya de diferentes sistemas informáticos y de la infraestructura de telecomunicaciones con el objeto de optimizar el uso de recursos humanos, materiales y financieros, además de 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.

En este sentido, la información reservada corresponde a los detalles de los intentos de ataques cibernéticos (fecha, lugar y tipo) que ha recibido este Instituto desde el 1 diciembre de 2018 al 23 de mayo de 2019; de hacer pública dicha información colocaría en un estado de vulnerabilidad permanente a los sistemas informáticos, a la infraestructura de telecomunicaciones de este Instituto y a la información bajo resguardo del INE, ya que la información reservada constituye parte fundamental

para el acceso a la RedINE, y de esta red depende en gran medida el ejercicio de las atribuciones del Instituto.

En ese orden de ideas, 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 sistemas institucionales, 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, se pondrían 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, dar a conocer la información que se solicita, implica otorgar elementos que podrían eventualmente hacer vulnerables los sistemas con los que cuenta este Instituto y sobre los cuales se apoya para el debido ejercicio de sus funciones.

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.

En consecuencia, se considera que el riesgo al que se expondrían los sistemas informáticos y la infraestructura de telecomunicaciones 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***
El detalle de los intentos de ataques cibernéticos que ha recibido el Instituto por el periodo del 1 de diciembre de 2018, al 23 de mayo de 2019, objeto de la	*Es un riesgo **demostrable** ya que además de los ataques que ha sufrido el Instituto y que, gracias a las medidas de seguridad con las que se cuenta y de las que, de entregarse la información se pondrían en estado de vulnerabilidad y riesgo real, existen numerosos ejemplos de acciones de este tipo (intentos de ataques cibernéticos) que*	*Mediante técnicas de hacking se podría tener acceso no autorizado a la infraestructura tecnológica que da soporte a los sistemas informáticos institucionales y con ello*

Información que se considera reservada	***Riesgo***	***Daño y/o afectación que podría causar en caso de conocerse la información***
solicitud de información con número de folio UT/19/001095.	*han causado estragos a diversos sistemas informáticos en todo el mundo.* *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:* *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.*	*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.*

• 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**:**

¿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 informáticos, y con ello a la operación institucional.* *En este sentido, el riesgo al que se expondrían los sistemas informáticos 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 a los detalles de los intentos de ataques cibernéticos que ha recibido el Instituto por el periodo señalado por la persona solicitante, objeto de la solicitud de información con número de folio UT/19/01095, se 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 proporcionalidad[17]*:*

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 detalles de los intentos de ataques cibernéticos a los sistemas del Instituto durante el periodo del 1 de diciembre de 2018 al 23 de*

[17] 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/iij.25940082e.2018.6.12466

Test de proporcionalidad	***Cuestionamientos***	***Justificación***
		mayo de 2019, objeto de la solicitud de información con número de folio UT/19/01095, sigue utilizándose para el funcionamiento de los equipos de interconexión de la RedINE con la que se proporciona acceso a los sistemas de apoyo institucional, sistemas de información electoral y diversos servicios actuales, es por ello que debe permanecer la reserva de la información, además de que son utilizados para todos los sistemas institucionales. *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 a los detalles de los intentos de ataques cibernéticos a los sistemas del Instituto, se pueden prevenir ataques focalizados en vulnerar las medidas de seguridad con las que se cuenta.*
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.*

Test de proporcionalidad	***Cuestionamientos***	***Justificación***
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 los detalles de los intentos de ataques cibernéticos de los sistemas del Instituto, los cuales soportan la correcta operación de estos, por lo que, hacer pública dicha información compromete la seguridad de los sistemas informáticos 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 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 permanente.

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 cibernético mediante el acceso o intento de acceso a los sistemas informáticos del Instituto.*
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 detalles de los intentos de ataques cibernéticos a los sistemas del Instituto durante el periodo del 1 de diciembre de 2018 al 23 de mayo de 2019, objeto de la solicitud de información con número de folio UT/19/01095, 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 reactores de este Instituto." (Sic)

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 6 de junio de 2019, mediante la resolución **INE-CT-R-0124-2018** 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:

> ***"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". (Sic)*

A su vez, remite al décimo quinto de dichos Lineamentos 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*
> ***IV.*** *El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Capítulo".(Sic)*

IV. Reserva temporal parcial. Análisis del CT del INE

El área **UTSI**, clasificó como temporalmente reservada la información respecto de todos los detalles de los intentos de ataques a los sistemas informáticos del Instituto y de manera particular, lo relativo a la fecha, lugar y tipo de estos que se ubiquen en el periodo comprendido del 1 de diciembre de 2018 al 23 de mayo de 2019 (fecha de recepción de la solicitud de información UT/19/01095), y que fue objeto de la solicitud de información con número de folio 2210000113819, por un plazo de cinco años adicionales al plazo de reserva aprobado mediante la resolución INE-CT-R-0124-2018 de fecha 6 de junio de 2019.

Cabe señalar que, en la solicitud de reserva, aprobadas mediante la INE-CT-R-0124-2018 de fecha 6 de junio 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***
> *"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 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.

Ahora bien, una vez señalado lo anterior esta autoridad tiene el deber de apegarse 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;*
> ***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 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. Por su parte, 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.

En esa tesitura, se desprende que, para el ejercicio de sus funciones, el Instituto se apoya de diferentes sistemas informáticos y de la infraestructura de telecomunicaciones con el objeto de optimizar el uso de recursos humanos, materiales y financieros, además de 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.

En este sentido, la información reservada corresponde a los detalles de los intentos de ataques cibernéticos (fecha, lugar y tipo) que ha recibido este Instituto desde el 1 diciembre de 2018 al 23 de mayo de 2019; de hacer pública dicha información colocaría en un estado de vulnerabilidad permanente a los sistemas informáticos, a la infraestructura de telecomunicaciones de este Instituto y a la información bajo resguardo del INE, ya que la información reservada constituye parte fundamental para el acceso a la RedINE, y de esta red depende en gran medida el ejercicio de las atribuciones del Instituto.

En ese orden de ideas, 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 sistemas institucionales, 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, se

pondrían 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, dar a conocer la información que se solicita, implica otorgar elementos que podrían eventualmente hacer vulnerables los sistemas con los que cuenta este Instituto y sobre los cuales se apoya para el debido ejercicio de sus funciones.

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.

En consecuencia, se considera que el riesgo al que se expondrían los sistemas informáticos y la infraestructura de telecomunicaciones 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***
El detalle de los intentos de ataques cibernéticos que ha recibido el Instituto por el periodo del 1 de diciembre de 2018, al 23 de mayo de 2019, objeto de la solicitud de información con	*Es un riesgo **demostrable** ya que además de los ataques que ha sufrido el Instituto y que, gracias a las medidas de seguridad con las que se cuenta y de las que, de entregarse la información se pondrían en estado de vulnerabilidad y*	*Mediante técnicas de hacking se podría tener acceso no autorizado a la infraestructura tecnológica que da soporte a los sistemas informáticos institucionales y con*

Información que se considera reservada	***Riesgo***	***Daño y/o afectación que podría causar en caso de conocerse la información***
número de folio UT/19/001095.	*riesgo real, existen numerosos ejemplos de acciones de este tipo (intentos de ataques cibernéticos) que han causado estragos a diversos sistemas informáticos en todo el mundo.* *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:* *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.*	*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, se 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 informáticos, y con ello a la operación institucional. En este sentido, el riesgo al que se expondrían los sistemas informáticos 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.*

El área **UTSI** indicó que el hacer pública la información relativa a los detalles de los intentos de ataques cibernéticos que ha recibido el Instituto por el periodo señalado por la persona solicitante, objeto de la solicitud de información con número de folio UT/19/01095, se 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 proporcionalidad[18]:

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 detalles de los intentos de ataques cibernéticos a los sistemas del Instituto durante el periodo del 1 de diciembre de 2018 al 23 de mayo de 2019, objeto de la solicitud de información con número de folio UT/19/01095, sigue utilizándose para el funcionamiento de los equipos de interconexión de la RedINE con la que se proporciona acceso a los sistemas de apoyo institucional, sistemas de información electoral y diversos servicios actuales, es por ello que debe permanecer la reserva de la información, además de que son utilizados para todos los sistemas institucionales. 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.

[18] 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/iij.25940082e.2018.6.12466

Test de proporcionalidad	Cuestionamientos	Justificación
	¿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 a los detalles de los intentos de ataques cibernéticos a los sistemas del Instituto, se pueden prevenir ataques focalizados en vulnerar las medidas de seguridad con las que se cuenta.
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.

Test de proporcionalidad	Cuestionamientos	Justificación
	¿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 los detalles de los intentos de ataques cibernéticos de los sistemas del Instituto, los cuales soportan la correcta operación de estos, por lo que, hacer pública dicha información compromete la seguridad de los sistemas informáticos 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.
	¿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 poder acceder a la información resulta más perjudicial que beneficioso al poner en riesgo diversos derechos.

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

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

Circunstancias	Explicación
	perpetrados desde cualquier lugar del mundo, causando daño en los sistemas informáticos.

Cabe resaltar que, en el presente caso se trata de una aprobación interna y generalizada, que consiste en la posibilidad de ampliar el plazo de reserva por primera vez, cualquiera que fuera el supuesto de los previstos en el artículo 110 de la LFTAIP, por un plazo de 5 años adicionales, el cual está sujetó solo a la aprobación del CT del sujeto obligado, ya que se acredito que subsisten las causas que dieron origen a su clasificación.

Plazo de reserva: El área UTSI solicitó la ampliación de reserva temporal por un plazo de cinco años adicionales, en virtud de la prueba de daño realizada, así como la naturaleza de la información referente a todos los detalles de los intentos de ataques a los sistemas informáticos del Instituto y de manera particular, lo relativo a la fecha, lugar y tipo de estos que se ubiquen en el periodo comprendido del 1 de diciembre de 2018 al 23 de mayo de 2019 (fecha de recepción de la solicitud de información UT/19/01095) y que fue objeto de la solicitud de información con números de folios 2210000113819.

Asimismo, precisó que el 6 de junio de 2019, mediante resolución INE-CT-R-0124-2018, 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

Por lo que el nuevo plazo de reserva concluye el 12 de marzo de 2029.

Conclusión: En virtud de lo anterior el CT **confirma** 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-0124-2018 de fecha 6 de junio de 2019, 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.

V. 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, 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.

> ***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*
***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.*
>
> *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". (Sic)*

A C U E R D O

Primero. Ampliación de plazo de reserva. Se aprueba la ampliación de plazo de reserva de la información relativa a todos los detalles de los intentos de ataques a los sistemas informáticos del Instituto y de manera particular, lo relativo a la fecha, lugar y tipo de estos que se ubiquen en el periodo comprendido del 1 de diciembre de 2018 al 23 de mayo de 2019 (fecha de recepción de la solicitud de información UT/19/01095) y que fue objeto de la solicitud de información con número de folio 2210000113819, por un plazo de cinco años adicionales al plazo de reserva aprobado mediante resoluciones INE-CT-R-0124-2018, de fecha 6 de junio de 2019, 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.

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

Aviso de privacidad del Sistema INFOMEX-INE; y de la PNT (INAI).[19]
----------*Inclúyase la Hoja de Firmas debidamente formalizada*---------
---

Autorizó: SLMV Supervisó: MAAR Elaboró: AKLC

"Este documento ha sido firmado electrónicamente de conformidad con el criterio SO/007/2019 emitido por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) el cual señala: "Documentos sin firma o membrete. Los documentos que son emitidos por las Unidades de Transparencia (UT) son válidos

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

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

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

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

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

en el ámbito de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) cuando se proporcionan a través de la Plataforma Nacional de Transparencia (PNT), aunque no se encuentren firmados y no contengan membrete."

Asimismo, se da cuenta del oficio INAI/SAI/DGEPPOEP/0547/2020 emitido por el INAI, en el cual señaló que las respuestas otorgadas por la UT del Instituto Nacional Electoral (INE) en el que el Comité de Transparencia (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-0002-2024

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 2210000113819 (UT/19/01095).

El presente acuerdo fue aprobado por unanimidad de votos de los integrantes del CT, en Sesión Extraordinaria Especial celebrada el 12 de marzo de 2024.

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

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

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

FIRMADO POR: VAZQUEZ BARAJAS JUAN MANUEL
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2933693
HASH:
A1A691D9F668BB89EFCF4C1576C6C9AA1BF6D8C6F30C5C44A4F92BF2E03F12C3

FIRMADO POR: MURILLO VARGAS SENDY LUCIA
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2933693
HASH:
A1A691D9F668BB89EFCF4C1576C6C9AA1BF6D8C6F30C5C44A4F92BF2E03F12C3

FIRMADO POR: MAESTRO OCEGUERA DIEGO ARMANDO
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2933693
HASH:
A1A691D9F668BB89EFCF4C1576C6C9AA1BF6D8C6F30C5C44A4F92BF2E03F12C3

FIRMADO POR: URIAS PALMA MARIA DEL CARMEN
AC: Autoridad Certificadora del Instituto Nacional Electoral
ID: 2933693
HASH:
A1A691D9F668BB89EFCF4C1576C6C9AA1BF6D8C6F30C5C44A4F92BF2E03F12C3