COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/155/2022

FOLIO: 330031922000544

Visto el expediente relativo a la clasificación parcial de información reservada, que somete la **Coordinación de Humanidades**, en relación con la solicitud de acceso a la información con número de folio **330031922000544,** se procede a dictar la presente resolución con base en los siguientes:

A N T E C E D E N T E S

I. Con fecha 11 de marzo de 2022, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia, se recibió la solicitud de acceso a la información con número de folio **330031922000544** en la que la persona solicitante requirió, entre otros puntos, lo siguiente:

> *"1) Solicito el documento de seguridad a que se refiere el artículo 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de las siguientes áreas*
>
> *- Instituto de Investigaciones Sociales*
>
> *…"* (sic).

II. En la solicitud de acceso a la información, la persona solicitante eligió como modalidad de entrega de la información, por medio electrónico, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia.

III. En cumplimiento a lo dispuesto en el punto Segundo, fracción II del Acuerdo por el que se constituyen la Unidad de Transparencia y el Comité de Transparencia de la UNAM, la Unidad de Transparencia remitió la solicitud de acceso a la información con número de folio **330031922000544**, mediante correos electrónicos de fecha 14 de marzo de 2022 a la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades**, a la **Facultad de Medicina**, a la **Dirección General de Asuntos del Personal Académico**, a la **Dirección General de Cómputo y de Tecnologías de Información y Comunicación**, a la **Oficina de la Abogacía General**, a la **Facultad de Derecho**, a la **Coordinación de Humanidades** y a la **Facultad de Arquitectura**.

IV. A través de correo electrónico de fecha 16 de marzo de 2022, dirigido a la Presidencia del Comité de Transparencia, la Facultad de Arquitectura solicitó la ampliación de plazo para dar respuesta.

Por lo anterior, con fecha 23 de marzo de 2022 y con fundamento en los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 132 de la Ley General de Transparencia y Acceso a la Información Pública; 135 de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 10, 15 y 53, fracción V, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad

Nacional Autónoma de México, se amplió el plazo para emitir la respuesta a la solicitud por 10 días más, contados a partir del día hábil siguiente a su vencimiento.

V. Mediante oficio COHU/STOJ/242/2022, recibido con fecha 29 de marzo de 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Humanidades** informó lo siguiente:

> *"En relación con la solicitud de acceso a la información folio **330031922000544**, turnada a esta Coordinación de Humanidades a través de correo electrónico de la Unidad de Transparencia, mediante la cual se requirió:*
>
> *…*
>
> *La Coordinadora de Vinculación e Intercambio del Instituto de Investigaciones Sociales (IIS) hizo llegar a esta Coordinación de Humanidades el Documento de Seguridad para la Protección de Datos Personales de dicho instituto.*
>
> *Ante esta solicitud de información, respetuosamente solicito a este H. Comité la reserva parcial del Documento de Seguridad para la Protección de Datos Personales del Instituto de Investigaciones Sociales.*
>
> *Lo anterior, toda vez que dicho documento se ajustan al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y acceso a la información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, los cuales establecen que podrá clasificarse como información reservada aquella cuya publicación '**VII.** Obstruya la prevención o persecución de los delitos…'.*
>
> *En correlación con lo anterior, el Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas establece que Para clasificar la información como reservada, 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.*
>
> *De los preceptos normativos referidos, es posible desprender que podrá reservarse aquella información cuya publicación obstruya la prevención o persecución de los delitos. Para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la afectación a 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.*

De esa manera, es oportuno señalar que el documento de seguridad que se requiere en la solicitud del Instituto de Investigaciones Sociales, describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad integridad y disponibilidad de los datos personales que tenga en su posesión, que contiene, entre otros:

- *En análisis de riesgos.*
- *El análisis de brecha.*
- *El plan de trabajo.*

Aunado a lo anterior, debe señalarse que el plan de trabajo define las acciones a implementar de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Por su parte, el análisis de riesgo y el análisis de brecha consideran las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, hardware, software, personal del responsable, entre otros; y establece las medidas de seguridad existentes contra las faltantes, se advierte que la difusión del análisis de riesgo y brecha del documento de seguridad potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales que posee ese Instituto de la Universidad Nacional Autónoma de México.

Por otra parte, es de señalar que el artículo 103 de la Ley General de Transparencia y Acceso a la Información Pública establece que, para motivar la clasificación de la información, se deberán señalar las razones, motivos o circunstancias especiales que llevaron a esta entidad a concluir que en el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento.

Por lo antes señalado, es posible advertir que algunas de las posibles consecuencias podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad de ese Instituto con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal virtud, esta Área Universitaria considera que la divulgación del documento cuya reserva parcial se plantea, podría obstruir, entre otras cuestiones, el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que se manejan y confían a esa Entidad Académica, así como de quienes son titulares dichos datos, pues se darían a conocer los controles implementados por ese

Instituto para garantizar la seguridad de la información que obra en sus sistemas, lo que los dejaría expuestos a la perpetración de actos perniciosos que pudieran ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales. Lo anterior, en detrimento de la seguridad y el debido tratamiento de los datos personales que obran en dichos sistemas, pues se pondría en riesgo el derecho a la protección de estos, la integridad y la confidencialidad de la información personal, así como el derecho a la autodeterminación informativa que únicamente pueden ejercer los titulares de dichos datos personales.

Aunado a lo anterior, los titulares de la información también quedarían expuestos a la perpetración de ilícitos tendientes a afectar su integridad, tales como la suplantación de su identidad u otro tipo de ataques informáticos, lo que constituye un riesgo a su seguridad.

…

Ahora bien, a efecto de cumplir con lo señalado, de conformidad con los artículos 104 de la Ley General de Transparencia y Acceso a la Información Pública y 39 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, se realiza la siguiente ***prueba de daño****:*

La divulgación del documento de seguridad para la protección de datos personales, particularmente en sus partes de plan de trabajo, análisis de riesgo y análisis de brecha, del Instituto de Investigaciones Sociales ocasionaría lo siguiente:

1. *Un potencial* ***riesgo real, demostrable e identificable de perjuicio significativo al interés público*** *toda vez que se le colocaría en un estado de vulnerabilidad en cuanto a las medidas de seguridad de los datos personales que posee, permitiendo el acceso ilícito a sus sistemas y equipos informáticos, facilitando accesos no autorizados a los sistemas, robos de información y suplantación de identidades. Lo anterior en tanto que … como sujeto obligado, acorde al artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tiene por objeto esencial establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.*

   Por ello, se estima que, con la difusión del análisis de riesgo y brecha del documento de seguridad se ocasionaría un perjuicio irreversible en protección, observancia, promoción, estudio y divulgación de los datos

personales que posee, máxime que si bien de conformidad con el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados no se advierte que dichos documentos contengan datos personales, lo cierto es que el proporcionar los mismos ocasionaría que una persona ajena a la entidad académica tenga acceso a los datos personales almacenados en los sistemas tecnológicos … como podrían ser los datos personales recabados con motivo del otorgamiento de apoyos.

2. *Con base en lo anterior, **el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información**, ya que el resguardo del plan de trabajo que contiene, además, el análisis de riesgo y brecha del documento de seguridad con que cuenta el Sujeto Obligado, implica llevar a cabo acciones de prevención de diversos delitos tipificados en el Código Penal Federal (accesos no autorizados a los sistemas, robos de información, suplantación de identidades), lo cual cobra importancia si se considera que dichas conductas implican vulnerar las medidas de seguridad de los datos personales que posee.*

3. *Asimismo, **la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen.*

*En razón de lo antes señalado, me permito someter a consideración y, en su caso, aprobación de ese H. Comité de Transparencia que dignamente usted preside, la **clasificación de reserva parcial** del documento de seguridad para la protección de datos personales del Instituto de Investigaciones Sociales, por un periodo de **cinco años**, se anexa la versión pública donde ha sido testado lo relativo al plan de trabajo, el análisis de riesgo y el análisis de brecha del documento de seguridad, lo anterior con fundamento en el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública.*

Lo anterior, de conformidad con lo dispuesto por los artículos 101, párrafo segundo de la Ley General de Transparencia y Acceso a la Información Pública; 100 de la Ley Federal de Transparencia y Acceso a la Información Pública; 32, 36, 38 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

…" (sic)

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

C O N S I D E R A C I O N E S

PRIMERA. De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva parcial de la información, propuesta por la **Coordinación de Humanidades** para atender la parte de la solicitud de acceso a la información con número de folio **330031922000544**, mencionada en el antecedente I de la presente resolución, y determinar, en consecuencia, si la confirma, modifica o revoca.

SEGUNDA. De conformidad con lo dispuesto en los artículos 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, esa clasificación.

En tal virtud, la **Coordinación de Humanidades** clasificó como información reservada por un periodo de cinco años, la mencionada en el antecedente V de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

> *"… Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *[…]*
>
> ***VII.** Obstruya la prevención o persecución de los delitos;*
>
> *[…]".*

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:

> *"**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.***
>
> *…".*
>
> **Énfasis añadido.**

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Al respecto, cabe tener en consideración lo establecido en el documento de trabajo del 12º. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: "*La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad…*".

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

Desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Asimismo, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia el 28 de enero de 1981**,** publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De igual forma, de conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrá pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

Por otro lado, en términos de lo previsto por el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, debe entenderse por Documento de Seguridad, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Ahora bien, de conformidad con los artículos 60, 61 y 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personas que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Además de lo anterior, de conformidad con la fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

En este sentido, de darse a conocer el plan de trabajo, el análisis y la brecha de riesgos, se ocasionaría una grave vulneración a las medidas de seguridad de datos personales, entendiendo por ésta la falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de información reservada propuesta por el Área Universitaria, se motiva en evitar o prevenir la comisión de una conducta ilícita identificada como acceso ilícito a equipos y sistema de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

> "Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa".
>
> *"Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *…".*

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, **sean o no propiedad del Estado**¸ o bien conozca o copie dicha información.

Por lo que en relación con la información relativa al **análisis de riesgos, de brecha y el plan de trabajo** que forman parte del documento de seguridad requerido por la persona solicitante, se darían a conocer las acciones a implementar de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, hardware, software, personal del responsable, entre otros, lo que representa para el Área Universitaria un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la entrega de esa información revelaría elementos que de manera concatenada con otra información que pudiera generarse o que se haya generado,

evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados por el Instituto de Investigaciones Sociales.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial para la infraestructura tecnológica del Área Universitaria, ya que la información técnica puede ser utilizada para propiciar ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a las infraestructuras informáticas, programas y desarrollos tecnológicos del Área Universitaria, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, como lo es el acceso ilícito a sistemas y equipos de informática.

Por lo anterior, se concluye que la información solicitada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

> *"Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
>
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio".*

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

De difundirse el plan de trabajo, el análisis de riesgos y el análisis de brecha del documento de seguridad, se afectarían las medidas y acciones implementadas por el Área Universitaria para reducir el riesgo de que se cometa una conducta o un comportamiento que puedan dañar o convertir a esta Universidad y su comunidad en sujetos o víctimas de un ilícito como lo es el **delito de acceso ilícito a sistemas y equipos de informática**.

Lo anterior, toda vez que la publicidad de la información contenida en el **análisis de riesgos, de brecha** y el **plan de trabajo** que forman parte del documento de seguridad requerido por la persona solicitante, representa un riesgo potencial para la infraestructura tecnológica del Área Universitaria, pues a través de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar ataques informáticos de diversa índole, disminuyendo la capacidad del Área Universitaria para responder ante posibles amenazas.

En ese sentido la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

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

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al solicitante de no recibirla, pues con la difusión de la información técnica contenida en el **análisis de riesgos, de brecha y el plan de trabajo** que forman parte del documento de seguridad requerido por la persona solicitante, se limitaría la capacidad del Área Universitaria para prevenir la comisión de conductas ilícitas como es el caso del delito de acceso ilícito a sistemas y equipos de informática.

De ahí resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda.

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

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso a la persona solicitante, a cambio de garantizar la capacidad del Área Universitaria para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita como lo es el acceso ilícito a sistemas y equipos informática que contienen datos personales tratados por el área universitaria, en contra de este sujeto obligado.

En ese sentido, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive

de manera trascendente el acceso a la información, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva parcial de la información propuesta por la **Coordinación de Humanidades**, por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** parcial de la información, propuesta por la **Coordinación de Humanidades,** para atender parte de la solicitud de acceso a la información con número de folio **330031922000544**, en relación con el **plan de trabajo**, el **análisis de riesgos**, y el **análisis de brecha** que forman parte del documento de seguridad para la protección de datos personales del Instituto de Investigaciones Sociales, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

Lo anterior, en términos de la consideración **SEGUNDA** de la presente resolución.

SEGUNDO. La persona solicitante podrá interponer el recurso de revisión previsto en los artículos 142 y 143 de la Ley General de Transparencia y Acceso a la Información Pública y 61 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o ante la Unidad de Transparencia de la UNAM, dentro de los quince días siguientes a la fecha de la notificación de la respuesta o del vencimiento del plazo para su notificación.

TERCERO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo electrónico institucional a la **Coordinación de Humanidades**, así como a la Unidad de Transparencia de esta Universidad, para que por conducto de esta última sea notificada a la persona solicitante**,** para los efectos procedentes.

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

POR MI RAZA HABLARÁ EL ESPÍRITU”
Ciudad Universitaria, Cd. Mx., 8 de abril de 2022

Archivo	15-ctunam-155-2022-0544.pdf		
Identificador único (hash)	20e71478d5d3bbeeec335c8d2d0cccc84dd3c3a566d584181e2f2e91db65dcaa		
Fecha y hora de cierre	08/04/2022 16:27:48	**Fecha y hora de emisión**	08/04/2022 16:56:50
Número de páginas	14	**Firmantes**	6

Firmantes

Nombre	Alfredo Sánchez Castañeda	**Fecha y hora de firma**	08/04/2022 16:27:48
Presidente del Comité de Transparencia			
Hash Firma	4fba05f118e1d553cb7acb1e62ae3ee1dc3feaa7d65b4a64b860d6d9bfca51130ce8479d023e1107140311f50bec5d52		

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	08/04/2022 14:44:48
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	9d2de50c485a8ee99d0c436624e1c07a159285335a077ee6da93fbe24b5aed6fbcf87b02bdce94ebb436c49a1d2f8ecc		

Nombre	Dra. Guadalupe Barrena Nájera	**Fecha y hora de firma**	08/04/2022 15:01:55
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
Hash Firma	231ba8cd276eee313168a058b96c429e37bf60b7fb9fc19e9c664bf05045b298b2036c1e32f065e9dbb8f71d08eea4c5		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	08/04/2022 15:20:19
Director General de Servicios Generales y Movilidad			
Hash Firma	82a2425e44686fcf0e4cd756c87a2282cc3bf4236e94829fc6e94d32edc3c0ee901fda4530595f7b7516a4968782afa7		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	08/04/2022 16:21:19
Titular de la Unidad de Transparencia			
Hash Firma	2588823463aae639c74a1194914a42a46673f827fae1c6e1d2cdf6815c7a5efdc51eaa1312f52cbc26b45b49eec6c8a3		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	08/04/2022 14:47:46
Especialista			
Hash Firma	ec8b42c0f8d7b8a57f3f762b4a66c70cd76c1abecfae07d31e9bc36ea7ce5b60c81b393c6cc87ea78f440ab09787bea5		