

**ASUNTOS
JURÍDICOS**
COORDINACIÓN GENERAL DE
ASUNTOS JURÍDICOS

No. Control Interno: CGAJ/UTAI/040/2024

No. de Folio: 270504200004024

**ACUERDO DE DISPONIBILIDAD DE INFORMACIÓN EN VERSIÓN
PÚBLICA**

CUENTA: Que mediante la Plataforma Nacional de Transparencia (PNT), se presentó la solicitud de acceso a la información con número de folio **270504200004024**, recepcionada el día 21 de octubre de 2024. En consecuencia, atento a lo previsto en los artículos 49, 50 y 138 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, procédase a emitir el acuerdo que en derecho corresponda. - - - - - **Conste.**

DEPARTAMENTO DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DE LA COORDINACIÓN GENERAL DE ASUNTOS JURÍDICOS, A LOS ONCE DÍAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL VEINTICUATRO, EN LA CIUDAD DE VILLAHERMOSA, CAPITAL DEL ESTADO DE TABASCO. - - - - -

Visto: La cuenta que antecede, **se acuerda.** - - - - -

PRIMERO. Que vía electrónica se tuvo por presentada la solicitud de acceso a la información de fecha 10 de octubre de 2024, con número de folio de la PNT **270504200004024**, que se cita de manera textual:

**"SOLICITO COPIA EN VERSION ELECTRONICA DEL
DOCUMENTO DE SEGURIDAD QUE TODO SUJETO**





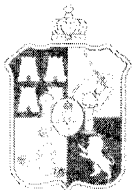
OBLIGADO DEBE POSEER DE ACUERDO A LO PREVISTO EN LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE TABASCO, ASI COMO LOS ACUERDOS DE PRIVACIDAD ACTUALIZADOS." (Sic)

En ese sentido, el particular ejerciendo su derecho humano y constitucional de acceso a la información pública que comprende el de *solicitar y recibir información* consagrado en el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos; 4° y 130 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. - - - - -

SEGUNDO. Que con fundamento en los artículos 49 y 50 fracciones III, VI Y XI, 132 Y 137 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco; y 21 del Reglamento Interior de la Coordinación General de Asuntos Jurídicos; esta Unidad de Transparencia, es competente para tramitar y resolver la solicitud de acceso a la información pública presentada por el particular en la PNT. - - - - -

TERCERO. Que el **22 de octubre del presente año**, el Departamento de Transparencia y Acceso a la Información Pública de este Sujeto Obligado, a través del oficio con número **CGAJ/UTAI/091/2024**, remitió al Enlace de Transparencia del Departamento de Transparencia y Acceso a la Información Pública para que en el ejercicio de las facultades y atribuciones que le confiere el artículo 21 fracción XIV del Reglamento Interior





ASUNTOS JURÍDICOS

COORDINACIÓN GENERAL DE
ASUNTOS JURÍDICOS

de la Coordinación General de Asuntos Jurídicos, diera respuesta a lo peticionado por la persona referida en el punto que antecede. - - - - -

CUARTO. Que con fecha 25 de octubre de 2024, el Enlace de Transparencia mediante el oficio con número CGAJ/UTAI/002/2024 informó:

"En primer lugar, de la revisión a la Solicitud de Acceso a la Información antes señalada, se advierte que el peticionario no señala la temporalidad en la información que requiere, por lo que atendiendo al criterio orientador 3/19 emitido por el Instituto Nacional de Transparencia (INAI), cito textual:

"03/19 Periodo de búsqueda de la información. Cuando la persona solicitante no señale el periodo respecto del cual requiere la información se considerará que el requerimiento se refiere al año inmediato anterior, contado a partir de la fecha de recepción de la solicitud".

En ese tenor, y tomando en consideración que la solicitud de mérito es de fecha 21 de octubre de 2024, la búsqueda de la información que se peticiona se entregará a partir del año inmediato anterior hasta la fecha en que entró la petición, es decir, desde el 21 de octubre 2023 hasta el 21 de octubre del presente año; bajo esa óptica, se informa al





particular que después de haber realizado una búsqueda minuciosa y razonable en los archivos físicos y electrónicos que obran en esta unidad, se encontró el DOCUMENTO DE SEGURIDAD actualizado mismo que se adjunta al presente para mejor proveer; para el caso de los AVISOS DE PRIVACIDAD respectivos, estos se encuentran localizados en el portal oficial de la Coordinación General de Asuntos Jurídicos (CGAJ); Pudiendo acceder a la siguiente liga electrónica :

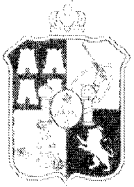
<https://tabasco.gob.mx/avisos-de-privacidad>" (Sic)

Con base a lo anterior, se pone a disposición del solicitante toda la documentación que remitió como respuesta a la solicitud de información, el enlace de Transparencia. - - - - -

QUINTO. Que en virtud de lo expuesto en el presente acuerdo y en atención a que el enlace de Transparencia, que provee contestación a la presente solicitud, es la competente para atender lo peticionado y tal como lo establece el artículo 21 fracción XIV del Reglamento Interior de la Coordinación de Asuntos Jurídicos; y con fundamento en lo dispuesto en el artículo 138 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, este Departamento de Transparencia informa al peticionario que la respuesta es de Disponibilidad de Información en Versión Pública. - - -

Handwritten signature or mark.





SEXTO. Que de conformidad en lo dispuesto por el artículo 6 párrafos sexto y séptimo de la multicitada Ley, mismos que señalan que: "ningún Sujeto Obligado está forzado a proporcionar información cuando se encuentre impedido de acuerdo a lo que señala esta ley para proporcionarlo o no esté en su posesión al momento de efectuarse la solicitud", asimismo, señala que "la información se proporcionará en el estado en que se encuentre. La obligatoriedad de los Sujetos Obligados de proporcionar información no comprende el procesamiento de la misma, ni de presentarla conforme al interés del solicitante". - - - - -

SÉPTIMO. Se informa al peticionario que, en caso de no estar conforme con el presente acuerdo, dispone de un plazo de quince (15) días hábiles contados a partir del día siguiente a la notificación del presente proveído, para interponer por sí mismo o a través de su representante legal, Recurso de Revisión ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública o ante este Departamento de Transparencia y Acceso a la Información Pública de este Sujeto Obligado, debiendo cubrir los requisitos exigidos por el artículo 150 de la Ley en la materia. - - - - -

OCTAVO. Notifíquese al solicitante el presente Acuerdo de Disponibilidad, a través de la Vía elegida por él mismo, con fundamento en el artículo 132 primer párrafo y 133 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. - - - - -





TABASCO
GOBIERNO DEL PUEBLO

**ASUNTOS
JURÍDICOS**
COORDINACIÓN GENERAL DE
ASUNTOS JURÍDICOS

NOVENO. CÚMPLASE. - - - - -

ASÍ LO ACUERDA, MANDA Y FIRMA, LIC. TILO TRINIDAD HERNÁNDEZ
ARIAS, TITULAR DEL DEPARTAMENTO DE TRANSPARENCIA Y ACCESO A LA
INFORMACIÓN PÚBLICA DE LA COORDINACIÓN GENERAL DE ASUNTOS
JURÍDICOS; EN LA CIUDAD DE VILLAHERMOSA, CAPITAL DEL ESTADO DE
TABASCO, A LOS ONCE DÍAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL
VEINTICUATRO. - - - - -

Este Acuerdo de Disponibilidad de Información en Versión Pública,
corresponde al Expediente con número de control interno CEAJ/UTAI/040/2024,
con folio 270504200004024. - - - - -

UTAI/L*TTHA/L*DJPV

**DOCUMENTO
DE SEGURIDAD**

31 DE MAYO DE 2024

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

ÍNDICE

Introducción	01
Objetivo	01
Marco jurídico	02
Glosario	03
Implementación de medidas de seguridad	05
Datos personales y documentos confidenciales	08
Inventario de los datos personales	09
Criterios emitidos por el INAI	14
Resoluciones emitidas por el INAI	17
Inventario de sistemas de datos personales	34
Obligaciones del personal responsable del tratamiento de Datos Personales en posesión de la Coordinación General de Asuntos Jurídicos	36
Funciones de los responsables, administradores y encargados del tratamiento de Datos Personales en posesión de la Coordinación General de Asuntos Jurídicos	37
Análisis de riesgos	38
Análisis de brecha	40
Medidas de seguridad físicas	42
Plan de contingencia para la protección de la información de la Coordinación General de Asuntos Jurídicos	46
Principios sobre la privacidad y protección de datos personales	54
Derechos ARCO	56
Deberes	57
Programa general de capacitación	58
Plan de trabajo	59
Monitoreo de las medidas de seguridad	61

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

INTRODUCCIÓN

La información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la organización; en ese tenor, el presente documento contiene las disposiciones en materia de protección de Datos Personales que deben observar las Unidades Administrativas adscritas a la Coordinación General de Asuntos Jurídicos, en términos de sus funciones y de conformidad con lo establecido en los artículos 38 y 40 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.

OBJETIVO

Establecer las funciones y obligaciones de los servidores públicos que traten datos personales, así como implementar los mecanismos de monitoreo, revisión de las medidas de seguridad y capacitación, en los sistemas de tratamiento en esta Coordinación General de Asuntos Jurídicos.

El Documento de seguridad se define como el instrumento que describe y da cuenta de modo 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.

MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Responsabilidades Administrativas.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Código Nacional de Procedimientos Penales.
- Constitución Política del Estado Libre y Soberano de Tabasco.
- Ley Orgánica del Poder Ejecutivo del Estado de Tabasco.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.
- Código Penal para el Estado de Tabasco.
- Código Civil para el Estado Libre y Soberano de Tabasco.
- Código de Procedimientos Civiles para el Estado de Tabasco.
- Reglamento Interior de la Coordinación General de Asuntos Jurídicos.
- Lineamientos Generales para el Proceso de Elaboración, Validación, Suscripción y Registro de Convenios y demás Instrumentos Jurídicos Similares, que celebren las Dependencias, Órganos y Organismos que Integran la Administración Pública Centralizada y Paraestatal.

GLOSARIO

- **Administrador del Sistema:** El servidor público que tiene a su cargo la responsabilidad de la administración del sistema y de los operadores.
- **Base de datos personales:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
- **Dato:** Es el elemento primario de la información conformado por símbolos (letras, números, dibujos, señas, gestos) que reunidos pueden cobrar significado. Solo o aislado el dato no posee relevancia, pero utilizado en las premisas de un razonamiento puede llevarnos a una conclusión.
- **Dato personal:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.
- **Dato personal sensible:** El que se refiere a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.
- **Documento de seguridad:** 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.
- **Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del Responsable, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del Responsable.
- **Operador:** Servidor (es) público (s) que opera (n) el sistema en la CGAJ.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- **Responsable:** El Sujeto Obligado, es decir la Coordinación General de Asuntos Jurídicos.
- **Responsable del sistema:** El titular de la Unidad Administrativa donde se administre el sistema.
- **Sistema:** Conjunto de elementos relacionados entre sí que funcionan como un todo. Módulo ordenado de elementos que se encuentran interrelacionados y que interactúan entre sí. Conjunto de elementos con relaciones de interacción e interdependencia que le confieren entidad propia al formar un todo unificado.
- **Sistema de tratamiento de datos personales:** Base de datos personales, contenido en un sistema, a las que se le aplica algún tratamiento.
- **Sub-Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del Encargado, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del Encargado.
- **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
- **Usuario:** Ciudadano o servidor público que hace uso del sistema, distinto al operador.
- **Usuario responsable:** Persona física o jurídica, pública o privada, ajena a la organización del Sub-Encargado, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del Sub-Encargado.

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Es importante aclarar las diferencias que existen entre las medidas de seguridad administrativa, física y técnica para que se cuente con los elementos teóricos al momento de elaborar el Documento de Seguridad.

- a) Las medidas de seguridad administrativa son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:
- Política de seguridad. Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.
 - Cumplimiento de la normatividad. Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable.
 - Organización de la seguridad de la información. Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.
 - Clasificación y control de activos. Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.
 - Seguridad relacionada a los recursos humanos. Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.
 - Administración de incidentes. Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- Continuidad de las operaciones. Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.
- b) Las medidas de seguridad física atañen a las acciones que deben implementarse para contar con:
- Seguridad física y ambiental. Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.
- c) Las medidas de seguridad técnica son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:
- Gestión de comunicaciones y operaciones. Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.
 - Control de acceso. Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.
 - Adquisición, desarrollo, uso y mantenimiento de sistemas de información. Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

- Tipo de soportes: Físicos y electrónicos. Es importante explicar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que el sujeto obligado implemente para cada sistema de datos personales está estrechamente relacionado con el tipo de soportes utilizados.

Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el INAI:

- **Soportes físicos.** Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, entre otros.
- **Soportes electrónicos.** Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil. El Decimoséptimo y el Trigésimo de los Lineamientos de Protección de Datos Personales hacen mención de los conceptos arriba señalados cuando se alude a los tipos de soportes, medios de almacenamiento o formatos -físicos o electrónicos- en los cuales residen los datos personales del sistema que custodia el sujeto obligado. Una vez explicado lo anterior, es preciso señalar que el sujeto obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en: soporte físico, soporte electrónico o ambos tipos de soportes.

DATOS PERSONALES Y DOCUMENTOS CONFIDENCIALES

La Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) así como la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) en sus artículos 116 y 113 fracción I, respectivamente, consideran que información confidencial "es la que contiene datos personales concernientes a una persona identificada o identificable... no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello".

A su vez, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO) en su artículo 3, fracciones IX y X, establece que se entenderá como datos personales los siguientes:

- Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Asimismo, define como datos personales sensibles los siguientes:

- Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Existen documentos que contienen datos personales, sin embargo, algunas secciones de los mismos son públicas. Para ello, se han expedido criterios y resoluciones de diversas instancias como son el INAI y el ITAIP acerca de cuándo se deberán testar los datos personales y realizar, en su caso, una versión pública de dichos documentos, como es el caso de la cédula profesional o la credencial para votar.

INVENTARIO DE LOS DATOS PERSONALES

Los datos personales tienen un valor potencial significativo, tanto para los titulares y responsables, como para cualquier persona no autorizada que pudiera beneficiarse de ellos, lo cual representa el riesgo inherente por tipo de dato.

A continuación, se ofrecen ejemplos de categorías de datos personales según su naturaleza:

- a) **Nivel estándar:** Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.
- b) **Nivel sensible:** Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país. También son datos de nivel sensible aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito.

Las medidas de seguridad que son aplicables a cada uno de los sistemas a cargo de la Coordinación General de Asuntos Jurídicos, deberán considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido, siendo estándar y sensibles, como a continuación se establece:

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Nivel Estándar

Identificables	<ul style="list-style-type: none">• Nombre• Fotografía• Lugar y Fecha de Nacimiento• Edad• Nacionalidad• Número Telefónico Particular• RFC• Firma• CURP• INE/IFE• Matrícula del Servicio Militar Nacional• Pasaporte• Estado Civil• Sexo• Licencia de Conducir• Número de Seguridad Social• Datos de Familiares
Información contenida en los siguientes documentos	<ul style="list-style-type: none">• Comprobante de Domicilio• Actas expedidas por el Registro Civil del titular y sus beneficiarios: nacimiento, adopción, matrimonio y defunción.
Informáticos	<ul style="list-style-type: none">• Correos electrónicos Particulares
Laborales	<ul style="list-style-type: none">• Solicitud de empleo• Recomendaciones• Nombramientos• Incidencias• Referencias personales• Gastos de Viáticos• Datos contenidos en facturas y tickets de comprobación de viáticos
Académicos	<ul style="list-style-type: none">• Título Profesional• Cédula Profesional• Carta Pasante• Escolaridad• Promedio• Constancias

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Nivel Sensible

Identificables	<ul style="list-style-type: none">• Domicilio Particular
Biométricos	<ul style="list-style-type: none">• Geometría de la Mano• Huella Digital• Rostro• Retina• Iris• Estructura de las Venas• Forma de la Oreja
Patrimoniales	<ul style="list-style-type: none">• Número de Cuenta• Tipo de Cuenta• Número de Tarjeta Bancaria• Número de Cliente• CLABE Bancaria• Régimen Fiscal contenido en cédulas del RFC
Salud	<ul style="list-style-type: none">• Certificado Médico• Certificados de Incapacidad
Procedimientos jurisdiccionales	<ul style="list-style-type: none">• Información relacionada íntimamente con el individuo, contenida en procedimientos administrativos o juicios en materia laboral, civil, penal, fiscal, mercantil u otra rama del Derecho.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

INVENTARIO DE DATOS PERSONALES

INVENTARIO	NIVEL
Nombre	Estándar
Fotografía	Estándar
Lugar y Fecha de Nacimiento	Estándar
Edad	Estándar
Nacionalidad	Estándar
Número Telefónico Particular	Estándar
RFC	Estándar
Firma	Estándar
CURP	Estándar
INE/IFE	Estándar
Matrícula del Servicio Militar Nacional	Estándar
Pasaporte	Estándar
Estado Civil	Estándar
Sexo	Estándar
Licencia de Conducir	Estándar
Número de Seguridad Social	Estándar
Datos de Familiares	Estándar
Comprobante de Domicilio	Estándar
Actas expedidas por el Registro Civil del titular y sus beneficiarios: nacimiento, adopción, matrimonio y defunción	Estándar
Correos electrónicos Particulares	Estándar
Solicitud de empleo	Estándar
Recomendaciones	Estándar
Nombramientos	Estándar
Incidencias	Estándar
Referencias personales	Estándar
Gastos de Viáticos	Estándar
Datos contenidos en facturas y tickets de comprobación de viáticos	Estándar
Título Profesional	Estándar
Cédula Profesional	Estándar
Carta Pasante	Estándar
Escolaridad	Estándar
Promedio	Estándar
Constancias	Estándar
Domicilio Particular	Sensible
Geometría de la Mano	Sensible
Huella Dactilar	Sensible

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Número de Cuenta	Sensible
Tipo de Cuenta	Sensible
Número de Tarjeta Bancaria	Sensible
Número de Cliente	Sensible
CLABE Bancaria	Sensible
Régimen Fiscal contenido en cédulas del RFC	Sensible
Certificado Médico	Sensible
Certificados de incapacidad	Sensible
Información relacionada íntimamente con el individuo, contenida en procedimientos administrativos o juicios en materia laboral, civil, penal, fiscal, mercantil u otra rama del Derecho	Sensible

CRITERIOS EMITIDOS POR EL INAI

El INAI es un Organismo Constitucional Autónomo garante del cumplimiento de los derechos fundamentales de acceso a la información pública y de protección de datos personales, cuyo órgano máximo de dirección es el Pleno, integrado por siete Comisionadas y Comisionados designados por el Senado de la República, de los cuales uno funge como Comisionado Presidente, y el mismo sesiona periódicamente. Entre las principales facultades del INAI están las de emitir criterios de carácter orientador, de los cuales destacan los siguientes:

DATOS PERSONALES	SUSTENTO
Cédula profesional	Que en los Criterios 02/10 y 01/13 emitidos por el INAI se establece que la cédula profesional es un documento que tiene por objeto acreditar que una persona cuenta con la autorización para ejercer la profesión indicada en la misma; a través del conocimiento de algunos de los datos ahí contenidos se puede corroborar la idoneidad de la persona para ocupar el empleo, cargo o comisión encomendado. En tal sentido, ante una solicitud de acceso a la información que se relacione con la cédula profesional, las dependencias y entidades de la Administración Pública Federal deberán elaborar una versión pública en la que se omitirán los datos personales que no refieran al perfil profesional de su titular, tales como la Clave Única de Registro de Población y la firma. La fotografía de una persona física que conste en su título o cédula profesional no es susceptible de clasificarse con carácter de confidencial, en virtud del interés público que existe de conocer que la persona que se ostenta con una calidad profesional determinada es la misma que aparece en los documentos oficiales de referencia. Lo anterior es así, ya que en el momento en que una persona se somete a un registro fotográfico con el objetivo de recibir una identificación oficial que lo avala como profesionista, consiente que tanto la imagen de su rostro como su nombre y profesión, sean elementos de acreditación e identificación frente a terceros.
Clave Única de Registro de Población (CURP)	Que el Criterio 18/17 emitido por el INAI señala que la Clave Única de Registro de Población (CURP) se integra por datos personales que sólo conciernen al particular titular de la misma, como lo son su nombre, apellidos, fecha de nacimiento, lugar de nacimiento y sexo. Dichos datos, constituyen información que distingue plenamente a una persona física del resto de los habitantes del país, por lo que la CURP está considerada como información confidencial.
	Que en el Criterio 01/09 el INAI estableció que los datos de

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Datos de identificación del representante o apoderado legal	identificación del representante o apoderado legal , es decir, el nombre, la firma y la rúbrica de una persona física que actúe como representante o apoderado legal de un tercero que haya celebrado un acto jurídico con algún sujeto obligado, es información pública, en razón de que tales datos fueron proporcionados con el objeto de expresar el consentimiento obligacional del tercero y otorgar validez a dicho instrumento jurídico.
Expediente clínico	Que en el Criterio 4/09 el INAI determinó que el expediente clínico contiene información relacionada con el <i>estado de salud del paciente</i> -titular de los datos-, por lo que con independencia de que puedan obrar opiniones, interpretaciones y criterios de los profesionales de la salud que trataron al paciente, dicha información se ubica dentro de la definición de datos personales. Esta clasificación únicamente resulta oponible frente a terceros, pero no frente a su <i>titular o representante legal</i> , ya que son precisamente estos últimos quienes tienen derecho a solicitar su acceso o corrección, por tratarse de información personal concerniente a su persona y, por lo tanto, información de la que únicamente ellos pueden disponer. Por lo anterior, la información contenida en el expediente clínico debe ser protegida con fundamento en el artículo 116 primer párrafo de la LGTAIP y el artículo 113 fracción I de la LFTAIP.
Información bancaria de los particulares	<p>Que el Criterio 10/13 emitido por el INAI determina que el número de cuenta bancaria de los particulares es información confidencial por referirse a su patrimonio.</p> <p>Derivado de lo anterior, se considera que dichos datos están asociados al patrimonio de una persona física, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona (física o moral) y que constituyen una universalidad jurídica.</p> <p>Por lo tanto, los datos relativos al número de cuenta, número de CLABE interbancaria y estado de cuenta bancario, constituyen información relacionada con el patrimonio de una persona física identificada y únicamente le incumbe a su titular o personas autorizadas para el acceso o consulta de información patrimonial, así como para la realización de operaciones bancarias.</p> <p>En este sentido, el sujeto obligado se encuentra obligado a proteger el carácter de confidencial de la información, aunado a que su divulgación facilitaría que cualquier persona pudiera afectar el patrimonio de los particulares.</p>
Nombres de actores en juicios laborales	Que en el Criterio 19/13 , el INAI determinó que el nombre de actores en juicios laborales constituye, en principio, información confidencial, pues el nombre es un atributo de la personalidad y la manifestación principal del derecho a la identidad, en razón de que por sí mismo permite identificar a una

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>persona física. Por lo que respecta al nombre de las personas que han entablado un juicio laboral, éste permite identificar a los actores que presentaron una demanda laboral y participan en un juicio, lo cual constituye una decisión personal que refleja un acto de voluntad de quien lo realiza. Las acciones legales que emprenden los actores en el ejercicio de sus derechos laborales hacen evidente la posición jurídica en la cual se han colocado por decisión propia, <i>con relación a determinados órganos de gobierno</i>, para la obtención de algunas prestaciones laborales o económicas, lo cual constituye cuestiones de carácter estrictamente privado. En este tenor, el nombre de los actores de los juicios laborales que se encuentran en trámite o que, en su defecto, concluyeron con la emisión de un laudo desfavorable a los intereses personales del actor constituye información confidencial. No obstante, procede la entrega del nombre de los actores en juicios laborales cuando, en definitiva, se haya condenado a una dependencia o entidad al pago de las prestaciones económicas reclamadas o la reinstalación del servidor público, en virtud de que el cumplimiento de dicho fallo se realiza necesariamente con recursos públicos a cargo del presupuesto del sujeto obligado, lo cual permite, por una parte, dar cumplimiento a las obligaciones de transparencia contenidas en la Ley y, por la otra, transparenta la gestión pública y favorece la rendición de cuentas a los ciudadanos, ya que se refiere al ejercicio de los recursos públicos y al cumplimiento que se da a las resoluciones emitidas por alguna autoridad jurisdiccional encargada de dirimir conflictos laborales.</p>
Número de cuenta bancaria y/o CLABE interbancaria de personas físicas y morales privadas	<p>Que el Criterio 10/17 emitido por el INAI señala que el número de cuenta bancaria y/o CLABE interbancaria de particulares es información confidencial, al tratarse de un conjunto de caracteres numéricos utilizados por los grupos financieros para identificar las cuentas de sus clientes, a través de los cuales se puede acceder a información relacionada con su patrimonio y realizar diversas transacciones; por tanto, constituye información clasificada.</p>
Número de empleado	<p>Que en el Criterio 06/09 el INAI acordó que cuando el número de empleado, o su equivalente, se integra con datos personales de los trabajadores o funciona como una clave de acceso que no requiere adicionalmente de una contraseña para ingresar a sistemas o bases de datos personales, procede su clasificación como información confidencial.</p>
Registro Federal de Contribuyentes (RFC)	<p>Que el INAI emitió el Criterio 19/17, el cual establece que el Registro Federal de Contribuyentes (RFC) de personas físicas es una clave de carácter fiscal, única e irrepetible, que permite identificar al titular, su edad y fecha de nacimiento, por lo que es un dato personal de carácter confidencial.</p>

RESOLUCIONES EMITIDAS POR EL INAI

El Pleno del INAI resuelve acerca de las respuestas de los sujetos obligados a los recursos de revisión y otros medios de impugnación mediante la emisión de **resoluciones** vinculatorias, definitivas e inatacables, como lo establece la Constitución. Ello implica que el cumplimiento de dichas resoluciones es obligatorio y que éstas no son impugnables o combatibles por medios administrativos o jurisdiccionales (salvo por los particulares, que pueden promover juicio de amparo en su contra).

En las resoluciones, el Pleno del INAI llega a pronunciarse respecto a la clasificación de información confidencial, cuando por ejemplo se trata de datos personales, con base en un análisis que le dé sustento conforme a la normatividad de acceso a la información y transparencia. Lo anterior aplica a los sujetos obligados del ámbito federal.

Las siguientes son algunas de las **resoluciones** emitidas por el INAI y que pueden servir de referente para la clasificación de datos personales:

Datos personales	Sustento
Acta de defunción	Que el INAI estableció en su Resolución RDA 1189/2005 que el acta de defunción obra en una fuente de acceso público como lo es el Registro Civil en dónde se puede consultar y, en principio, no podría considerarse como información confidencial; sin embargo, ésta contiene datos personales, por lo que en virtud del principio de finalidad, los sujetos obligados se encuentran impedidos para otorgar su acceso, toda vez que el fin para el cual se recabó dicho documento no fue el otorgar acceso a terceros acerca de los mismos.
Acta de matrimonio	Que el INAI estableció en su Resolución RDA 2015/2006 que el acta de matrimonio obra en una fuente de acceso público como lo es el Registro Civil en dónde puede ser consultada, por lo que en principio no podría considerarse información confidencial; sin embargo, ésta contiene datos personales, por lo que en virtud del principio de finalidad, los sujetos obligados se encuentran impedidos para otorgar su acceso, toda vez que el fin para el cual se recabó dicho documento no fue el otorgar acceso a terceros acerca de los mismos.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Acta de nacimiento	<p>Que el INAI estableció en sus Resoluciones RDA 12/2006 y RDA 245/2009, que si bien el Acta de Nacimiento obra en una fuente de acceso público como lo es el Registro Civil en dónde puede ser consultada, en principio no podría considerarse información confidencial; sin embargo, esta contiene datos personales, por lo que en virtud del principio de finalidad, los sujetos obligados se encuentran impedidos para otorgar su acceso, toda vez que el fin para el cual se recabó dicho documento no fue el otorgar acceso a los mismos a terceros.</p>
Cadena original del complemento de certificación digital del Servicio de Administración Tributaria (SAT)	<p>Que en la Resolución RRA 7502/18, el INAI advierte que deberá entenderse como cadena original del complemento de certificación digital del Servicio de Administración Tributaria, a la secuencia de datos formada con la información fiscal de la persona moral, contenida dentro de la factura electrónica; sus especificaciones se establecen en el rubro C del anexo 20 de la Resolución de Miscelánea Fiscal.</p> <p>Por tanto, se actualizan las fracciones 1 y 2 del artículo 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, por contener datos personales y fiscales de una persona moral.</p>
Cadena original del complemento de certificación digital del SAT	<p>Que en la Resolución RRA 09673/20 señaló el INAI que de la cadena original se pueden obtener datos personales de los contribuyentes, tales como: RFC del emisor, RFC del receptor, folio fiscal y resumen general de la factura electrónica tales como totales de percepciones, y retenciones. De acuerdo a lo anterior, se advierte que la cadena original se constituye como información que únicamente les atañe a los contribuyentes; así en el caso que nos ocupa, al acceder a la Cadena Original, también se estaría dando acceso al RFC del particular; en virtud de lo anterior, resulta procedente la confidencialidad de dicho dato, de conformidad con el artículo 113, fracciones I y III de la Ley Federal de la materia.</p>
Capital social	<p>Que en la Resolución RRA 0098/17 el INAI considero el capital social de la empresa (acciones), al estar representado por títulos nominativos que sirven para acreditar y transmitir la calidad y los derechos de los mismos, pueden traducirse en la propiedad que una persona física tiene de una parte de la sociedad mercantil, por lo que se advierte que es información que incide directamente en su patrimonio.</p> <p>Es decir, el capital social se integra por las acciones aportadas por cada uno de los accionistas que forman a la sociedad, por lo que <i>dichas acciones representan el</i></p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p><i>porcentaje monetario que cada uno aporta a dicha sociedad.</i></p> <p>Por lo anterior, el capital social entendido como los porcentajes de las acciones de cada accionista, así como el importe que representan, debe clasificarse como confidencial, ya que da cuenta de datos relacionados con su patrimonio.</p>
Cartilla militar y número de cartilla militar	<p>Que en la Resolución 0245/09 el INAI advirtió que la cartilla militar es una tarjeta de identificación intransferible, en virtud de que pertenece exclusivamente a la persona a cuyo nombre se expidió, en la que obra información de carácter confidencial, tal como nombre completo, fecha de nacimiento, lugar de nacimiento, estado civil, domicilio, edad, ocupación, firma y huella digital, así como el número de matrícula asignado por la Secretaría de la Defensa Nacional, el cual no podrá conferirse a ninguna otra persona.</p> <p>Asimismo, se advierte que el número de cartilla militar (matrícula) de una persona física es información confidencial, ya que la existencia del documento mismo, así como la información contenida en este son datos que únicamente le atañen al particular, ya que lo distingue plenamente del resto de los habitantes, aunado a que es un documento de carácter personalísimo cuyo propósito es que sea utilizado únicamente por su titular. Por lo tanto, el citado número constituye información confidencial.</p>
Cédula profesional	<p>Que en su Resolución RRA 1024/16, el INAI determinó que la cédula profesional es un documento que tiene por objeto acreditar que una persona cuenta con la autorización para ejercer la profesión indicada en la misma, avalando los conocimientos idóneos del profesionista así acreditado. Tales constancias contienen los siguientes datos:</p> <ul style="list-style-type: none">• Número de cédula profesional.• Fotografía.• Firma del titular.• Nombre del titular.• Clave Única de Registro de Población.• Nombre y firma del Director General de Profesiones, de la Secretaría de Educación Pública. <p>Así pues, en resumen, se desprende que el <i>número de cédula profesional, la fotografía, y el nombre del titular</i>, son datos que <i>no actualizan la clasificación como confidencial</i>, de conformidad con el artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>Información Pública, de ahí que resulte procedente su entrega.</p> <p>En cuanto al <i>nombre y firma del Director General de Profesiones</i>, es de carácter público debido a que da fe que la expedición de la cédula profesional fue en ejercicio de las facultades conferidas, y en consecuencia son datos que no actualizan la clasificación como confidencial de conformidad con el artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, de ahí que resulte procedente su entrega.</p> <p>En cambio, la <i>Clave Única de Registro de Población</i>, así como la <i>firma del titular</i> de la cédula profesional <i>sí son datos personales y se consideran confidenciales</i>, en tanto que pueden identificar otra información de su titular como fecha de nacimiento, edad, lugar de nacimiento y origen, motivo por el que debe ser protegido con fundamento en el artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública</p> <p>Por tanto, solo el nombre y la fotografía del titular, el número de cédula profesional, el nombre y firma del servidor público que expidió el documento son públicos.</p>
Clave Única del Registro de Población (CURP)	<p>Que el INAI en la Resolución RRA 5279/19 señaló que para la integración de la Clave Única de Registro de Población se requieren datos personales como es el nombre y apellidos, fecha de nacimiento y lugar de nacimiento, asimismo, se asigna una homoclave y un dígito verificador que es individual, como se establece en el Instructivo Normativo para la Asignación de la Clave Única de Registro de Población de la Dirección General Nacional de Población e Identificación Personal de la Secretaría de Gobernación.</p> <p>Por lo anterior, al tratarse de una clave que distingue plenamente a la persona del resto de los habitantes, haciendo identificable al titular de los datos, se considera que la Clave Única de Registro de Población es Información confidencial, en términos de lo dispuesto en el artículo 113, fracción 1, de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
CURP	<p>Que en la Resolución RRA 09673/20 señaló el INAI que la CURP es un dato personal, derivado de su conformación. De acuerdo con lo señalado en los artículos 86 y 91 de la Ley General de Población, la CURP se asigna a una persona para permitir certificar y acreditar fehacientemente su identidad, la cual sirve entonces para identificar en forma individual a las personas.</p> <p>La CURP se integra a partir de los siguientes datos: Nombre(s) y apellido (s); Fecha de nacimiento; Lugar de nacimiento; Sexo, y Homoclave y un dígito verificador que</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>son asignados de manera única e individual por la Secretaría de Gobernación.</p> <p>En ese sentido, en virtud de que la CURP se integra por datos que únicamente atañen a la persona a la que se asigna, por lo que se concluye que se trata de datos personales de carácter confidencial, en términos de lo dispuesto en el artículo 3, fracción II de la Ley de la materia, y se considera confidencial, de conformidad con lo dispuesto en el artículo 18, fracción II de la misma Ley.</p>
Código QR	<p>Que en la Resolución RRA 7502/18, el INAI advierte que el código QR (del inglés <i>Quick Response Code</i>, código de respuesta rápida) es la evolución del código de barras. Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional, el cual presenta tres cuadrados en las esquinas que permiten detectar la posición del código al lector.</p> <p>Los códigos QR almacenan información y están adaptados a los dispositivos electrónicos como Smartphones o tabletas, permitiendo descifrar el código y trasladarlo directamente a un enlace o archivo, decodificando la información encriptada, por lo que podrían dar acceso a la información relativa a una persona física o moral que únicamente incumbe a su titular o personas autorizadas para el acceso o consulta de la misma, por lo que resulta procedente su clasificación, fundamento en la fracción 1 del artículo 113 de la Ley Federal de Transparencia y Acceso a la Información pública.</p>
Comprobante de domicilio	<p>Que en la Resolución RRA 3142/12, el INAI consideró que el comprobante de domicilio revela un tipo de servicio con el que cuenta una persona identificada, por ejemplo, de luz, teléfono (en cuyo caso, también se revela la empresa con la que se decidió contratar el servicio), agua, etcétera. Aunado a que puede tener información referente al patrimonio de la persona (costo del servicio, pagos efectuados, saldo), número de teléfono y domicilio particular.</p> <p>En razón de lo anterior el INAI concluyó que no es procedente entregar el comprobante de domicilio, ya que se trata de información confidencial.</p>
Correo electrónico	<p>Que en las Resoluciones RRA 1774/18, RRA 1780/18 Resolución y RRA 5279/19 el INAI señaló que el correo electrónico se puede asimilar al teléfono o domicilio particular, cuyo número o ubicación, respectivamente, se considera como un dato personal, toda vez que es otro medio para comunicarse con la persona titular del mismo y la hace localizable. Así también, se trata de información de una persona física identificada o identificable que, al darse a conocer,</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>afectaría la intimidad de la persona.</p> <p>En virtud de lo anterior, el correo electrónico de un particular constituye un dato personal confidencial, conforme a lo dispuesto en el artículo 113 fracción I y III de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Credencial paravotar	<p>Que en su Resolución RRA 1024/16, el INAI determinó que la credencial para votar contiene diversa información que, en su conjunto, configura el concepto de dato personal previsto en la Ley Federal de Transparencia y Acceso a la Información Pública, al estar referida a personas físicas identificadas, tales como: nombre, firma, sexo, edad, fotografía, huella dactilar, domicilio, clave de elector, número de OCR, localidad, municipio, estado, sección, año de registro, año de emisión, votación, fecha de vigencia, fecha de nacimiento, CURP, clave alfanumérica, QR, los espacios necesarios para marcar el año y elección.</p> <p>En este sentido, se estima procedente la clasificación de los datos contenidos en la credencial para votar referidos por parte del sujeto obligado.</p> <p>Asimismo, de acuerdo con la Resolución 4214/13 el INAI, los únicos datos que deben proporcionarse son: nombre y firma del Secretario Ejecutivo del Instituto Nacional Electoral y el folio de la misma.</p>
Curriculum vitae	<p>Que en su Resolución RRA 1024/16, el INAI determinó que el curriculum vitae da cuenta de diversos datos personales, tales como los que de manera enunciativa más no limitativa se mencionan a continuación: nombre, domicilio, teléfono, correo electrónico, sexo, edad, entre otros. En esa tesitura, es preciso señalar que, de acuerdo a lo analizado previamente, tales datos son considerados como confidenciales, por lo que procede su clasificación.</p>
Curriculum vitae del empleado responsable de una persona moral	<p>Que en la Resolución RRA 7502/18, el INAI advierte que el curriculum vitae es una expresión documental que contiene información sobre la experiencia y logros profesionales, tanto académicos como laborales y, cuando menos, el grado máximo de estudios (nivel, institución educativa, carrera, estatus), entre otros datos.</p> <p>Dicho curriculum vitae da cuenta de las decisiones personales de una persona física identificada, que no es servidor público, sino empleado de una persona moral. Si bien en el caso concreto se advierte que la persona es responsable en un proyecto, lo cierto es que el ámbito de</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>decisión que le es otorgado deviene de la decisión de la asociación, empresa o persona moral a la que pertenece o reporta. Por lo que no se advierte que exista obligación normativa de su difusión, sino por el contrario, por tratarse de datos personales concernientes a una persona identificada o identificable, corresponde a información de la esfera privada de una persona física identificada, así se tiene que es un dato personal de una persona física identificada o identificable y resulta procedente su confidencialidad en términos del artículo 113 fracción 1 de la Ley de la materia.</p>
<p>Datos de identificación y ubicación de instituciones educativas</p>	<p>Que en la Resolución RRA 12057/19, el INAI confirmó que en principio de cuentas dichos datos podrían considerarse públicos, en tanto que las instituciones educativas tienen como fin brindar un servicio al público, aunado a que existe un Sistema de Información y Gestión Educativa en el cual es posible llevar a cabo la consulta de dichos datos.</p> <p>Sin embargo, en el caso particular, los datos refieren a instituciones educativas de menores de edad que se encuentran relacionados con los servidores públicos del sujeto obligado, por lo que dar a conocer los mismos podría hacer identificable la institución precisa a la que acuden, lo cual únicamente les atañe a ellos, al tratarse de una decisión de carácter completamente personal.</p> <p>Por tal motivo, es que dichos datos deben ser considerados como confidenciales en los documentos en los que se encuentran, en términos de lo establecido en el artículo 113, fracción I de la ley Federal de Transparencia y Acceso a la Información Pública.</p>
<p>Deducciones contenidas en recibos de pago</p>	<p>Que en las Resoluciones RDA 1159/05 y RDA 843/12 emitidas por el INAI, determinó que las deducciones contenidas en recibos de pago son datos personales, pues es a partir de ellas como se determina la remuneración neta de cualquier persona, incluidos los servidores públicos. Existen ciertas deducciones que se refieren única y exclusivamente al ámbito privado de dichas personas, como pudieran ser aquellas derivadas de una resolución judicial, la contratación de un seguro o descuentos por préstamos personales; las mismas revelan parte de las decisiones que adopta una persona respecto del uso y destino de su remuneración salarial, lo cual incide en la manera en que se integra su patrimonio, por lo que se considera que esa información no es de carácter público, sino que constituye información confidencial en virtud de que corresponden a decisiones personales y se debe clasificar como información confidencial.</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Domicilio de particulares	<p>Que, en las Resoluciones, RRA 1774/18, RRA 1780/18 y RRA 5279/19 el INAI señaló que el domicilio de particulares, al ser el lugar en donde reside habitualmente una persona física, constituye un dato personal y, por ende, confidencial, ya que su difusión podría afectar la esfera privada de la misma.</p> <p>Por lo tanto, el domicilio de particulares se considera confidencial, y sólo podrá otorgarse mediante el consentimiento expreso de su titular, en virtud de tratarse de datos personales que reflejan cuestiones de la vida privada de las personas, en términos del artículo 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Domicilio particular de persona física	<p>Que en la Resolución RRA 09673/20 el INAI señaló que el Domicilio particular de persona física, en términos del artículo 29 del Código Civil Federal, el domicilio es el lugar en donde reside habitualmente una persona física. En este sentido, constituye un dato personal y, por ende, confidencial, ya que incide directamente en la privacidad de personas físicas identificadas, y su difusión podría afectar la esfera privada de las mismas.</p> <p>Por consiguiente, dicha información es confidencial y sólo podrá otorgarse mediante el consentimiento expreso del titular de los datos personales; por ello, la calle y número exterior, colonia, delegación o municipio, entidad federativa y el código postal, que se traduce en el domicilio particular, se considera clasificado, con fundamento en el artículo 113 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Domicilio de persona moral	<p>Que en la Resolución RRA 09673/20 el INAI señaló que el domicilio de persona moral, Consiste en el lugar donde una persona moral tiene su centro de trabajo, es decir, se establece con precisión un lugar físico, en el caso que nos ocupa el presente dato se encuentra vinculado a la identificación de las personas morales, por lo que conceder el presente dato, haría identificable a la persona moral, por lo que es susceptible de ser clasificado, con fundamento en el artículo 113, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Edad	<p>Que en la Resolución RRA 09673/20 señaló el INAI que la edad es un dato personal, toda vez que el mismo consiste en información concerniente a una persona física identificada o identificable. Se trata de datos personales confidenciales, en virtud de que refieren a una característica física por lo que al darlos a conocer se</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>afectaría la intimidad de la persona titular de los mismos. En términos de lo anterior, se actualiza el supuesto de clasificación establecido en el artículo 113 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Edad y fecha de nacimiento	<p>Que el INAI en las Resoluciones RRA 0098/17 y RRA 5279/19 señaló que tanto la edad como la fecha de nacimiento son datos personales, toda vez que los mismos consisten en información concerniente a una persona física identificada o identificable. Ambos datos están estrechamente relacionados, toda vez que, al dar a conocer la fecha de nacimiento, se revela la edad de una persona. Se trata de datos personales confidenciales, en virtud de que al darlos a conocer se afectarían la intimidad de la persona titular de los mismos. Por lo anterior, el INAI considera procedente su clasificación, en términos del artículo 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Estado civil	<p>Que en las Resoluciones RRA 0098/17 y RRA 5279/19 el INAI señaló que el estado civil constituye un atributo de la personalidad que se refiere a la posición que ocupa una persona en relación con la familia; en razón de lo anterior, por su propia naturaleza es considerado como un dato personal, en virtud de que incide en la esfera privada de los particulares, por ello, es clasificado con fundamento en el artículo 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Fax	<p>Que en su Resolución RDA 6768/15, el INAI determinó que el fax permite que un usuario envíe y reciba mensajes y archivos; es decir, permite mantener una comunicación con el titular del mismo, situación por la cual se podría identificar o hacer identificable a quien ostenta el fax; por ello, se estima procedente considerarlo un dato personal confidencial, conforme a lo dispuesto en el artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Firma	<p>Que en las Resoluciones RRA 1774/18, RRA 1780/18 y RRA 5279/19 el INAI señaló que la firma es un conjunto de rasgos propios de su titular, un atributo de la personalidad de los individuos y busca que la misma no pueda ser reproducida por otra persona. La firma identifica o hace identificable a su titular, aunado a que ésta es utilizada como una prueba del consentimiento y aprobación por parte de una persona, motivo por el cual debe ser resguardada. En ese sentido, se considera que la firma es un dato personal confidencial en términos de</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	la fracción I del numeral 113 de la Ley Federal de Transparencia y Acceso a la Información Pública.
Firma de la credencial de elector	Que en su Resolución RRA 1024/16 , el INAI determinó que la firma se trata de un dato personal confidencial, en tanto que identifica o hace identificable al titular de la credencial de elector . En este sentido dicha información es susceptible de clasificarse en términos del artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.
Folio fiscal	<p>Que en la Resolución RRA 7502/18 y RRA 09673/20 el INAI advierte que el número de folio de la factura permite identificar el documento emitido. La <i>factura electrónica</i> es entonces un comprobante fiscal digital y se define como un documento digital con validez legal, que utiliza estándares técnicos de seguridad internacionalmente reconocidos para garantizar la integridad, confidencialidad, autenticidad, unicidad y no repudio de la factura.</p> <p>La factura electrónica al ser la versión electrónica de las facturas tradicionales en papel, debe ser funcional y legalmente equivalente a estas últimas. De manera que el folio fiscal con el que cuenta, permite identificar la emisión de dicha factura a efecto de no duplicar información.</p> <p>En este sentido, la cifra referida sólo sirve para tener un control de las facturas emitidas y facilitar el rastreo por parte de la persona moral en caso de búsqueda del documento fuente y, en su caso, llevar a cabo su consulta y/o cancelación en la página del Servicio de Administración Tributaria (SAT).</p> <p>En tal virtud, podría considerarse que, mediante la publicidad del <i>número de folio de la factura</i>, se podría rastrear la factura emitida en la página del SAT, y en su caso, vulnerar el derecho a la protección de datos personales que se desprenden del documento fuente, en este caso, la factura emitida.</p> <p>En consecuencia, el <i>folio fiscal de la factura</i> es información de carácter confidencial con fundamento en el artículo 113, fracciones 1 y 2, de la Ley Federal de Transparencia y Acceso a la Información Pública, por lo que resulta procedente su clasificación.</p>
Fotografía	Que en las Resoluciones RRA 1774/18, RRA 1780/18 y RRA 5279/19 emitidas por la INAI señaló que la fotografía constituye la reproducción fiel de la imagen de una persona, obtenida en papel a través de la impresión en un rollo o placa por medio de cámara fotográfica, o en formato digital, que constituye la

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>reproducción de las imágenes captadas. En este sentido, la fotografía constituye el primer elemento de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual; por lo tanto, es un dato personal en términos del artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que se trata de la representación gráfica de las características físicas de una persona, el cual se debe proteger, mediante su clasificación.</p>
Género	<p>Que en la Resolución RRA 5279/19 el INAI señaló que el género describe las características de hombres y mujeres que están basadas en factores sociales; es decir, las personas nacen con sexo masculino o femenino, pero aprenden un comportamiento que compone su identidad y determina los roles de género.</p> <p>En esa consideración, el sexo es el conjunto de características biológicas y fisiológicas que distinguen a los hombres y las mujeres, por ejemplo, órganos reproductivos, cromosomas, hormonas, entre otros; mientras que el <i>género</i> comprende los roles, relaciones, responsabilidades, valores, actitudes y formas de poder construidos socialmente que se asignan al género masculino y femenino y, que a su vez, componen la identidad de género de cada persona, la cual es concebida como la manera en que cada individuo se proyecta frente a sí ante la sociedad, respecto a la pertenencia o no al sexo que legalmente le fue asignado al nacer con base en sus sentimientos y convicciones. Por lo anterior, se considera procedente su clasificación, en términos del artículo 113, fracción I, de la Ley federal de Transparencia y Acceso a la Información Pública.</p>
Huella dactilar	<p>Que el ahora INAI en su Resolución 4214/13 señaló que la huella dactilar es la impresión visible o moldeada que produce el contacto de las crestas papilares de un dedo de la mano sobre una superficie, por tanto, se considera que es una característica individual que se utiliza como medio de identificación de las personas y constituye un dato personal.</p>
Licencia de conducir	<p>Que en la Resolución 4214/13 el INAI señaló que la licencia de conducir de una persona física se trata de un documento confidencial; únicamente el número de licencia para conducir no es susceptible de clasificación, ya que a partir del mismo no podría obtenerse algún otro dato respecto de su titular.</p>
Lugar de	<p>Que en la Resolución 4214/13 el INAI señaló que el lugar de nacimiento de una persona revelaría el estado o país del cual es originario un individuo, lo que permitiría</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

nacimiento	relacionar a una persona física identificada con su origen geográfico o territorial, por lo anterior, se considera que es un dato personal.
Lugar y fecha de nacimiento	Que en la Resolución 4214/13 el INAI señaló que el lugar y fecha de nacimiento son datos de carácter confidencial, toda vez que la publicidad del primero revelaría el estado o país del cual es originario un individuo y de dar a conocer la fecha de nacimiento, se revela la edad de la persona, por lo que se afectaría la intimidad de la persona titular de los mismos.
Nacionalidad	Que el INAI estableció en las Resoluciones RRA 1024/16, RRA 0098/17 y RRA 09673/20 que la nacionalidad es un atributo de la personalidad que señala al individuo como miembro de un Estado, es decir, es el vínculo legal que relaciona a una persona con su nación de origen. En este sentido, la nacionalidad de una persona se considera como información confidencial, en virtud de que su difusión afectaría su esfera de privacidad, revelaría el país del cual es originaria, identificaría su origen geográfico, territorial o étnico. Por lo anterior, se considera procedente su clasificación, en términos del artículo 113, fracción I, de la Ley federal de Transparencia y Acceso a la Información Pública.
Nombre persona física	Que en las Resoluciones RRA 1774/18, RRA 1780/18 y RRA 11496/20 emitidas por la INAI señaló que el nombre es uno de los atributos de la personalidad y la manifestación principal del derecho subjetivo a la identidad, toda vez que no se refiere a servidores públicos; en virtud de que hace a una persona física identificada e identificable, y que dar publicidad al mismo vulneraría su ámbito de privacidad. Por lo anterior, es conveniente señalar que el nombre de una persona física es un dato personal , por lo que debe considerarse como un dato confidencial , en términos de los artículos 113 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.
Número de OCR	Que en su Resolución RRA 1024/16 , el INAI determinó que el número de credencial de elector denominado Reconocimiento Óptico de Caracteres (OCR) , contiene el número de la sección electoral en donde vota el ciudadano titular de dicho documento, por lo que constituye un dato personal en razón de que revela información concerniente a una persona física identificada o identificable en función de la información geo electoral ahí contenida, por lo que es susceptible de resguardarse en términos del artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.
	Que el INAI en su Resolución 2955/15 determinó que

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Número de seguridad social

el **número de seguridad social**, al ser un código numérico único e irrepitable que arroja información personal sobre un individuo, como lo es la alcaldía que asignó el número, el año de incorporación, así como el año de nacimiento de una persona identificada e identificable se considera un dato personal.

Número de seguridad social o número de afiliación

Que en la **Resolución RPC-RCDA 0819/12** el INAI señaló que el **número de seguridad social o número de afiliación**, es un dato personal y, por tanto, es información confidencial, debido a que los trabajadores de nuevo ingreso realizan un trámite mediante el Formato AFIL -02 denominado "Aviso de inscripción del trabajador", publicado en el Diario Oficial de la Federación el 16 de noviembre de 1999, en el cual debe incluirse, entre otra información, el nombre completo del trabajador, la Clave Única del Registro de Población; el salario base de cotización, tipo de salario, fecha de ingreso, sexo, lugar y fecha de nacimiento, ocupación, domicilio, nombre o razón social de la fuente de trabajo y el domicilio de ésta última.

De lo anterior, se advierte que el número de afiliación al Instituto Mexicano del Seguro Social se integra con datos de identificación del trabajador, y se utiliza únicamente para cuestiones relacionadas con la seguridad social, por lo que es un dato que debe clasificarse.

Número de serie del CSD Certificado de Sello Digital (CSD) - SAT

Que en la Resolución **RRA 09673/20** señaló el INAI que el **certificado de sello digital o el número de Serie del Certificado de Sello Digital**, es un documento electrónico proporcionado por el Servicio de Administración Tributaria, el cual está vinculado al certificado de la firma electrónica avanzada y, por tanto, a la identidad de su propietario, debido a que su función es habilitar al titular para emitir y sellar digitalmente facturas electrónicas.

Por medio de ellos, el contribuyente podrá sellar electrónicamente la cadena original de las facturas electrónicas que emita; garantizándose el origen de la misma, la unicidad y las demás características que se heredan de los certificados de firma electrónica avanzada.

El sello digital es el conjunto de datos asociados al emisor y a los datos del documento, por lo tanto, es único e irrepitable. Se trata del elemento de seguridad en una factura, ya que a través de él se puede detectar si un mensaje ha sido alterado y quién es el autor del documento.

El Sello Digital es una serie de caracteres que se forma como resultado de encriptar la información de la Cadena Original del Comprobante, lo que hace que el comprobante sea infalsificable ya que cualquier cambio en

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	<p>los datos, generaría un sello diferente al original.</p> <p>Para el caso que nos atañe, el Sello Digital del CFDI correspondiente a una persona física, daría cuenta del autor de documento, que es una persona de derecho privado.</p> <p>En ese sentido, de acuerdo con lo anterior, se tendría que dicho dato da cuenta de la información de una persona de derecho privado, lo cual resultaría en su clasificación. Ello de conformidad con lo establecido en el artículo 113 fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Ocupación	<p>Que en la Resolución RDA 0760/2015 el INAI señaló que la ocupación de una persona física identificada constituye un dato personal que podría reflejar el grado de estudios, preparación académica, preferencias o ideología de una persona, por lo que con respecto a los datos indicados se actualiza su clasificación como información confidencial.</p>
Origen étnico	<p>Que en la Resolución RRA 1588/16 el INAI señaló que el origen étnico es la clasificación de una persona con base en una combinación de características compartidas, tales como la nacionalidad, origen geográfico, lengua, religión, costumbres y tradiciones, por lo que se trata de un dato personal que, de divulgarse, permitiría hacer identificada o identificable a una persona, por lo que debe clasificarse como confidencial.</p>
Padecimientos y procedimientos médicos	<p>Que en la Resolución RRA 12057/19, el INAI señaló que los procedimientos médicos que se practiquen a una persona, así como los padecimientos que tenga, a todas luces darían cuenta del estado de salud de las personas a quienes correspondan, lo cual corresponde a la esfera más íntima de cada quien, por lo cual se debe considerar como información clasificada como confidencial, con fundamento en el artículo 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Patrimonio	<p>Que en la Resolución RRA 5279/19 el INAI señaló que el patrimonio es el conjunto de bienes propios de una persona o de una institución, susceptibles de estimación económica, por lo que sólo le compete a su titular, por lo que se considera como un dato personal, de conformidad con la fracción I del artículo 113 de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
	<p>Que en su Resolución RRA 1024/16, el INAI determinó que la profesión u ocupación de una persona física identificada constituye un dato personal</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Profesión u ocupación	que, incluso, podría reflejar el grado de estudios, preparación académica, preferencias o ideología. Por lo que se actualiza su clasificación como información confidencial de conformidad con el artículo 113, fracción I de la Ley de la materia, salvo el caso de que dicho dato correspondiera al responsable técnico de la elaboración del proyecto, ya que el mismo, se encuentra consignado en su cédula profesional y el mismo es considerado de acceso público, por lo que, en su caso, este no sería susceptible de clasificarse.
Reporte de buró de crédito	Que en la Resolución RDA 3142/12 el INAI señaló que mediante el Reporte de Buró de Crédito es posible que la persona tenga conocimiento de quien ha consultado su historial crediticio, verificar que dicha información esté correcta y actualizada para que, en su caso, formule las aclaraciones correspondientes, así como solicitar el apoyo de un asesor para interpretar el contenido de dicho reporte y aclarar todo tipo de dudas. Asimismo, el INAI estableció que los datos de carácter patrimonial versan sobre información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, entre otros, relativos a una persona física identificada e identificable y revela aspectos de su intimidad, ya que es producto de una decisión de carácter personal de dicha persona, por lo que el Reporte de Buró de Crédito es un dato confidencial .
Sello digital del emisor - Servicio de Administración Tributaria (SAT)	<p>Que en la Resolución RRA 7502/18, el INAI advierte que el sello digital es el conjunto de datos asociados al emisor y a los datos del documento, por lo tanto, es único e irrepetible. Se trata del elemento de seguridad en una factura, ya que a través de él se puede detectar si un mensaje ha sido alterado y quién es el autor del documento. Sirve para dar validez fiscal al documento por parte del Servicio de Administración Tributaria.</p> <p>El <i>sello digital</i> es una serie de caracteres que se forma como resultado de encriptar la información de la <i>cadena original del comprobante</i>, lo que hace que este último sea infalsificable, ya que cualquier cambio en los datos generaría un sello diferente al original.</p> <p>De acuerdo con lo señalado, y toda vez que dar a conocer los elementos de la clave de la factura electrónica permitiría identificar datos personales de quien la emitió, se concluye que dicha información debe considerarse como confidencial en términos del artículo 113, fracciones 1 y 2 de la Ley Federal de Transparencia y Acceso a la Información Pública, por lo que su clasificación resulta procedente.</p>
	Que en la Resolución RRA 09673/20 señaló el INAI que el Sello del Comprobante Fiscal Digital por Internet

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Sello del Comprobante Fiscal Digital por Internet (CFDI)	<p>(CFDI) es el resultado de firmar la cadena original que se obtiene de la factura electrónica, en la cual viene información codificada que está asociada al emisor de la factura o de cualquier otro certificado de sello digital y a los datos de la misma; es decir, funge como la firma del emisor del comprobante y lo integra el sistema que utiliza el contribuyente para la emisión del mismo.</p> <p>Además, dicho sello digital contiene datos personales del contribuyente emisor, a saber, el nombre y RFC; no obstante, si la persona descifra algoritmos informáticos, puede acceder a todos los datos personales del contribuyente.</p> <p>Derivado de lo anterior, se advierte que el sello digital del CFDI da cuenta tanto de un dato único e irrepetible con el que se otorga certeza a los actos realizados por su titular, por lo que se vincula con su credibilidad al momento de firmar un comprobante fiscal, así como del nombre y el RFC del contribuyente emisor.</p> <p>Derivado de lo anterior, resulta procedente su clasificación en términos del artículo 113, fracciones I y III de la Ley Federal de la materia</p>
Serie del certificado del emisor del Servicio de Administración Tributaria	<p>Que en la Resolución RRA 7502/18, el INAI advierte que la serie del certificado del emisor es un documento electrónico proporcionado por el Servicio de Administración Tributaria (SAT), el cual está vinculado al certificado de la firma electrónica avanzada y, por tanto, a la identidad de su propietario, en este caso una persona moral, debido a que su función es habilitar al titular para emitir y sellar digitalmente facturas electrónicas.</p> <p>Por medio de ellos, el contribuyente podrá sellar electrónicamente la cadena original de las facturas electrónicas que emita; garantizándose el origen de las mismas, la unicidad y las demás características que se heredan de los certificados de la firma electrónica avanzada.</p> <p>En ese sentido, se desprende que dicho dato contiene información de carácter confidencial relativo a una persona moral, con fundamento en el artículo 113, fracción 1, de la Ley Federal de Transparencia y Acceso a la Información Pública.</p>
Sexo	<p>Que el INAI en sus Resoluciones 1588/16 y RRA 0098/17 determinó que el sexo es considerado un dato personal, pues con él se distinguen las características biológicas y fisiológicas de una persona y que la harían identificada o identificable, por ejemplo, sus órganos reproductivos, cromosomas, hormonas, entre otros; de esta manera se considera que este dato incide directamente en su ámbito privado y, por ende, en su intimidad, por lo que debe clasificarse conforme a lo dispuesto en el artículo</p>

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

	113, fracción I, de la Ley federal de Transparencia y Acceso a la Información Pública.
Teléfono particular de persona física o moral	Que en las Resoluciones RRA 1774/18 y RRA 1780/18, RRA 09673/20 , el INAI señaló lo que corresponde al número telefónico, éste es asignado a un teléfono particular y/o celular , y permite localizar a una persona física o moral identificada o identificable, por lo que se considera como un dato personal y, consecuentemente, de carácter confidencial, ya que sólo podrá otorgarse mediante el consentimiento expreso de su titular; por ello, se estima procedente considerarlo como confidencial . Lo anterior de conformidad con lo dispuesto en el artículo 113 fracción I y III de la Ley Federal de Transparencia y Acceso a la Información Pública.
Teléfono (número fijo y de celular)	<p>Que en la Resolución RDA 1609/16 emitida por el INAI se estableció que el número de teléfono se refiere al dato numérico para la prestación del servicio de telefonía fija o celular asignado por empresa o compañía que lo proporciona, atento a una concesión del Estado y que corresponde al uso en forma particular, personal y privada, con independencia de que éste se proporcione para un determinado fin o propósito a terceras personas, incluidas autoridades o prestadores de servicio.</p> <p>El número telefónico, tendrá carácter de dato personal, cuando a través de éste sea posible identificar o hacer identificable al titular o usuario del mismo, cuando hubiere sido entregada a los sujetos obligados para un determinado propósito o hubieren sido obtenidos en ejercicio de sus funciones, análisis que resulta aplicable al presente caso.</p>

INVENTARIO DE SISTEMAS DE DATOS PERSONALES

A continuación, se presentan los sistemas de tratamiento de datos personales con los que cuenta esta Coordinación General de Asuntos Jurídicos, ordenados de acuerdo al Reglamento Interior de esta dependencia.

1. Coordinador:

- a) Secretaría Particular

2. Unidad de Administración y Finanzas:

- a) Departamento de Recursos Humanos
- b) Departamento de Recursos Financieros y Contabilidad
- c) Departamento de Recursos Materiales y servicios Generales

3. Unidad de apoyo técnico e informático:

- a) Departamento de Sistemas y Soporte

4. Subdirección de Seguimientos a los Procesos de los Subcomités de Compras y de los Comités de Adquisiciones, Arrendamientos y Servicios:

- a) Departamento de Seguimiento de Procesos Estatales y Federales A
- b) Departamento de Seguimiento de Procesos Estatales y Federales B
- c) Departamento de Seguimiento de Procesos Estatales y Federales C
- d) Departamento de Seguimiento de Procesos Estatales y Federales D

5. Subcoordinación de Asuntos Jurídicos:

- a) Dirección de Asuntos Jurídicos
- b) Departamento de Asuntos Civiles, Administrativos y Penales
- c) Departamento de Procesos Constitucionales y Derecho Social

6. Subcoordinación de Unidades de Apoyo Jurídico:

- a) Dirección de Consulta Unidades Sector 1
- b) Dirección de Consulta Unidades Sector 2
- c) Dirección de Consulta Unidades Sector 3

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- d) Departamento de Visitas y Seguimiento
- e) Unidades de Apoyo Jurídico

7. Dirección General de Normatividad y Transparencia:

- a) Departamento de Transparencia y Acceso a la Información Pública
- b) Departamento de Normatividad

8. Dirección de Seguimiento a Proyectos Legislativos:

- a) Departamento de Proyectos Legislativos
- b) Departamento de Formulación e Iniciativa Legislativa

OBLIGACIONES DEL PERSONAL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA COORDINACIÓN GENERAL DE ASUNTOS JURÍDICOS.

- a. Proteger y guardar confidencialidad respecto de los datos personales que tenga en posesión, en función de sus facultades establecidas en el Reglamento Interior de la Coordinación General de Asuntos Jurídicos.
- b. Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los Datos Personales.
- c. Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los Datos Personales en su posesión.
- d. Suprimir los datos personales, cuando hayan dejado de ser necesarios para el fin que motivó su tratamiento, conforme a las disposiciones que resulten aplicables, y una vez que concluya el plazo de conservación de los mismos.
- e. Tratar los Datos Personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
- f. Informar al Titular de datos personales, a través del Aviso de Privacidad, la existencia y características principales del tratamiento al que serán sometidos sus Datos Personales, a fin de que pueda tomar decisiones informadas al respecto.
- g. 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.
- h. Llevar una bitácora de las vulneraciones a la seguridad en la que se describan las mismas, la fecha en que ocurrieron, el motivo de ellas y las acciones correctivas implementadas de forma inmediata y definitiva.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

FUNCIONES DE LOS RESPONSABLES, ADMINISTRADORES Y ENCARGADOS DEL TRATAMIENTO DE LOS DATOS PERSONALES EN POSESIÓN DE LA COORDINACIÓN GENERAL DE ASUNTOS JURÍDICOS.

- Dar aviso al Departamento de Transparencia de los sistemas que involucren el tratamiento de datos personales en su unidad administrativa.
- Designar al Administrador del Sistema.
- Validar que la información entregada por los titulares de datos personales, sea estrictamente necesaria para cumplir con los fines legales para los cuales fueron recabados.
- Mantener actualizados los sistemas de tratamiento de datos personales que le correspondan.
- Determinar a los servidores públicos que pueden tener acceso a los datos personales, en función de sus facultades y del tratamiento que debe aplicarse a los mismos.
- Autorizar los accesos de los servidores públicos, determinar los privilegios y limitantes y llevar un registro de los mismos.
- Implementar las medidas de seguridad administrativa, física y técnica mínimas con la finalidad de evitar vulneraciones de la información.

ANÁLISIS DE RIESGOS

Los Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco, señalan en su artículo 43, que el análisis de riesgos que deberá realizar el responsable consiste en la identificación y evaluación de riesgo actual y real en el que se encuentren sus Sistemas de Datos Personales, así como, las medidas para su reducción o mitigación.

Se debe considerar también lo señalado en el artículo 60 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que a la letra dice:

Artículo 60. *Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*

- I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
- II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
- III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- V. Los factores previstos en el artículo 32 de la Ley General.

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

El análisis de riesgos contempla tres factores que en conjunto determinan el riesgo latente de los datos personales:

- Beneficio, factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- Accesibilidad, factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- Anonimidad, factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos.

Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruente para disminuir los posibles impactos a los datos personales o sensibles.

ANÁLISIS DE BRECHA

La realización de un análisis de brecha va enfocado a la seguridad de los datos personales recabados, realizando un diagnóstico de las prácticas de seguridad de la información con las que cuenta en ese momento este sujeto obligado y las que deberían de tenerse en base a las mejores prácticas.

Las mejores prácticas deben de cubrir las áreas o dominios de la seguridad de la información, para que permita evaluar de manera amplia para identificar las practicas que se deberán de llevar a cabo para un mayor cumplimiento de las obligaciones en materia de protección de datos personales, para de esta manera establecer el nivel de madurez de las practicas realizadas por el sujeto obligado y posteriormente definir las acciones que se llevaran a cabo para disminuir la brecha entre la situación actual y las mejores prácticas.

Algunos de los aspectos a evaluar y ponderar para tener una visión más completa y concreta sobre el estado actual de la seguridad de los datos personales y los aspectos existentes son:

- **Seguridad institucional.**

Control de la información compartida con terceros

- **Activos del responsable**

Asignación de responsabilidades y clasificación

- **Seguridad en recursos humanos**

Cuidar la seguridad de los recursos humanos previo a la contratación, durante y una vez que haya culminado su trabajo.

- **Seguridad física y ambiental**

Áreas seguras y protección de equipamiento

- **Operación, procedimientos y comunicación**
- **Cumplimiento con leyes y lineamientos**
- **Control de acceso a la información**

Derechos y control de acceso a aplicaciones, redes y sistemas operativos

- **Seguridad de sistemas de información**

Procesos de información

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Controles criptográficos

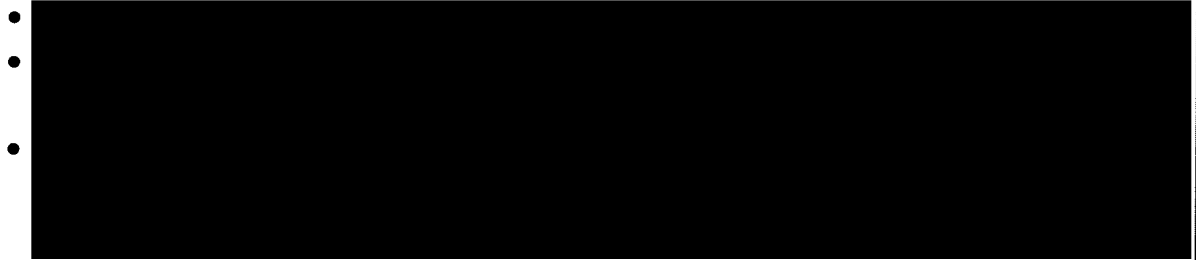
Protección de archivos de sistema

- **Incidentes de seguridad de información**

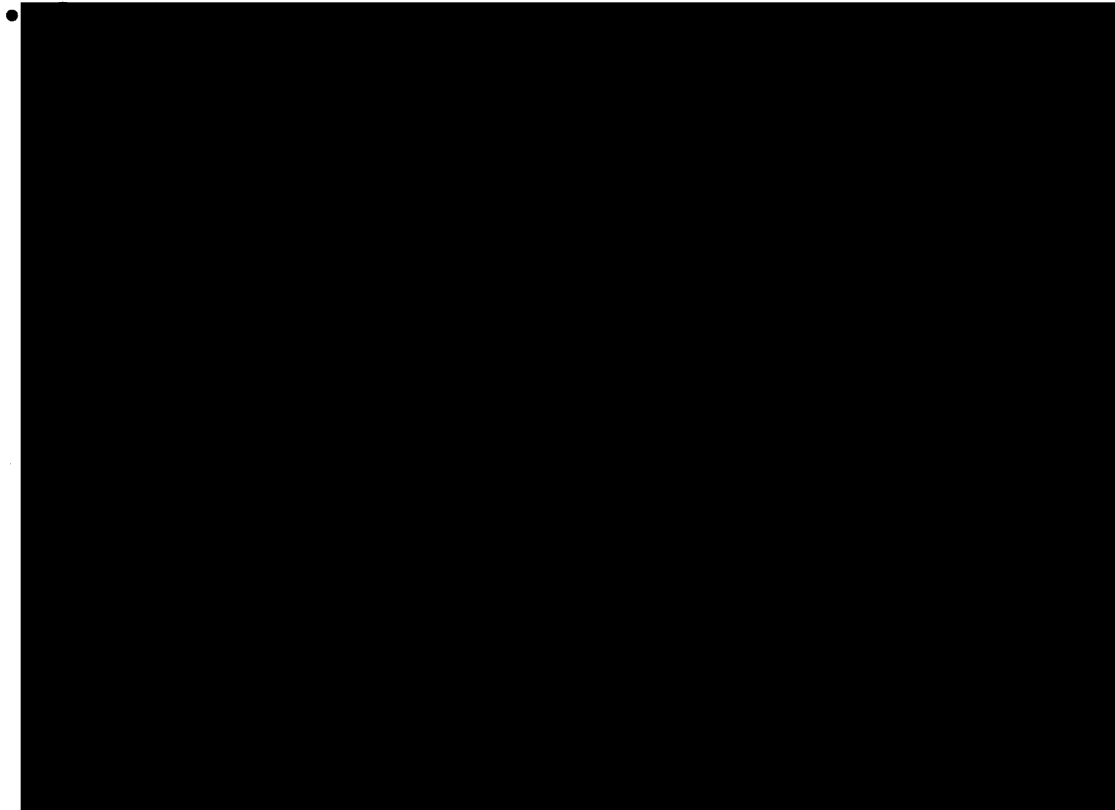
MEDIDAS DE SEGURIDAD FÍSICAS

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

- **Entorno de los datos:**



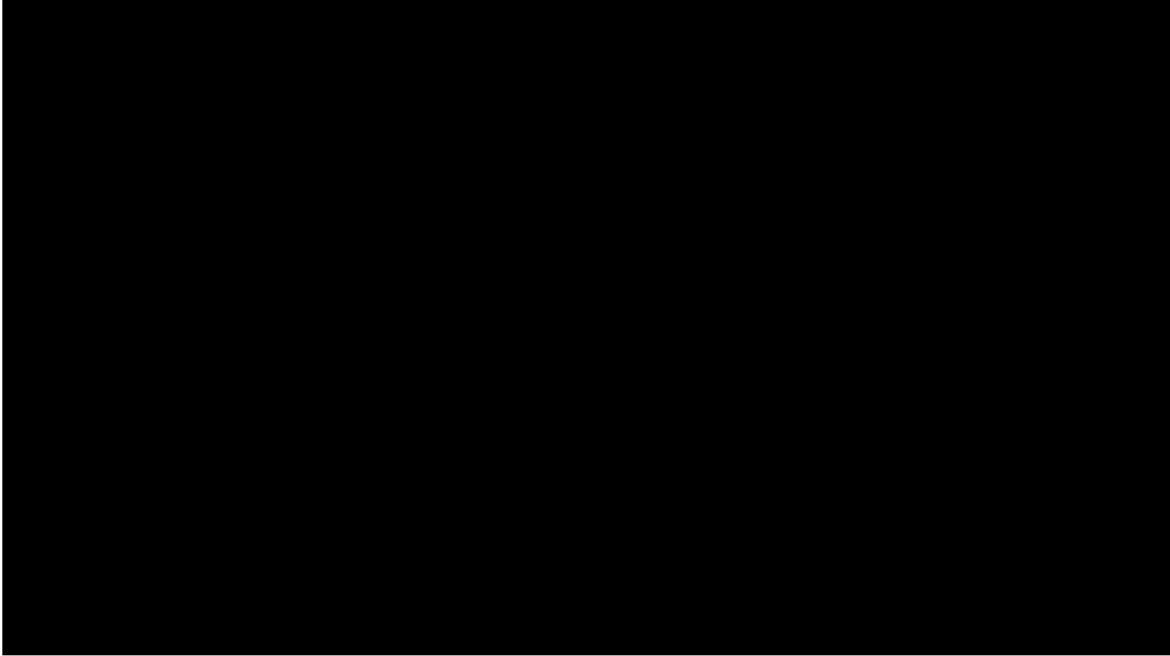
- **Procedimiento de respaldo y recuperación de datos personales:**



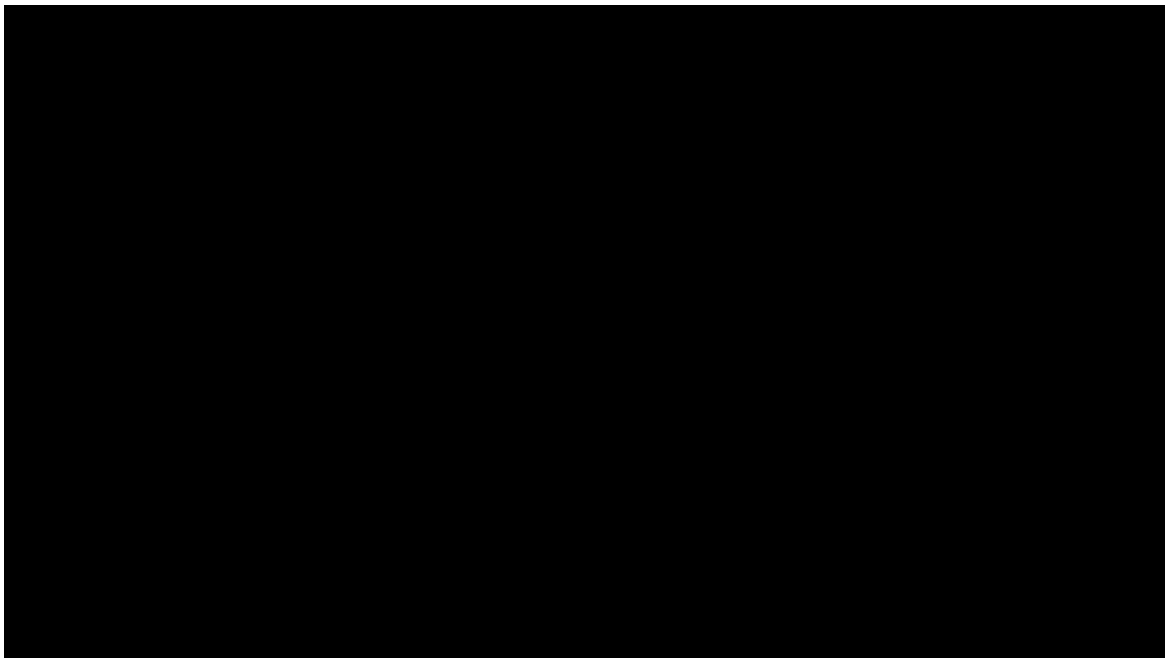
JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- Controles y mecanismos de seguridad para transferencias.

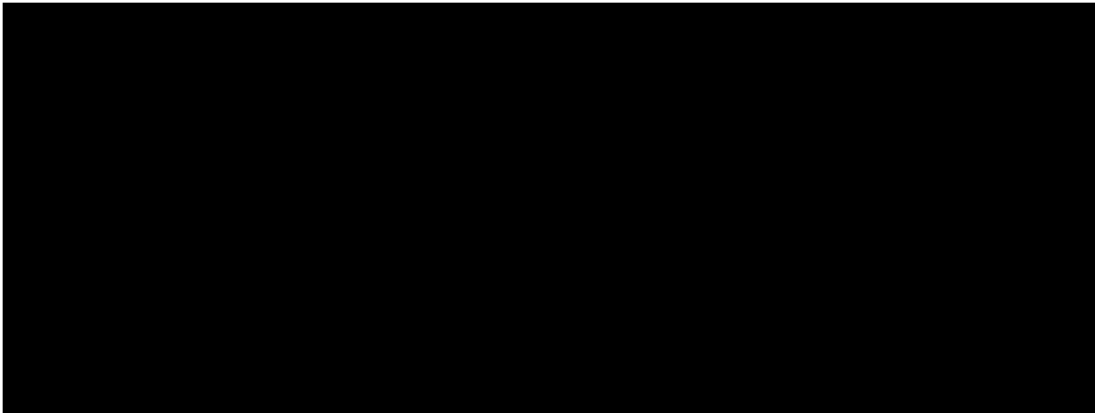


• Transmisiones mediante el traslado de soportes físicos:

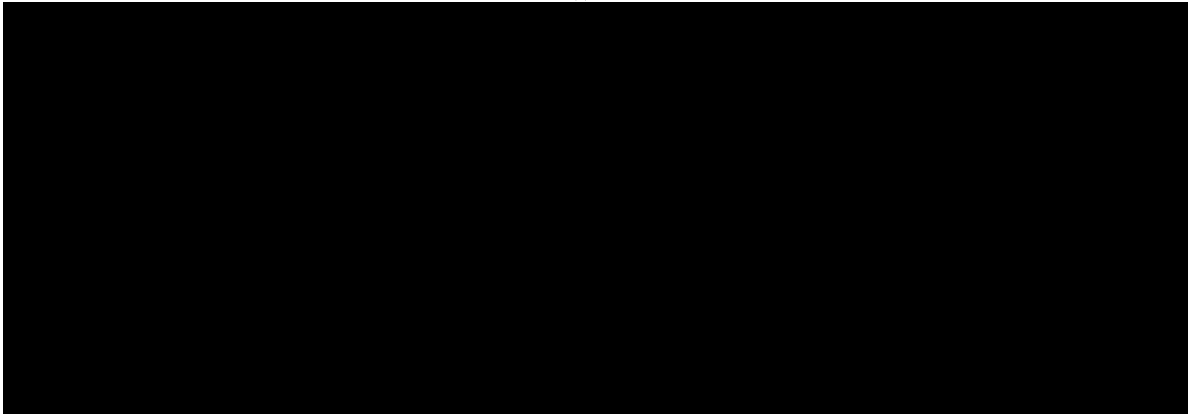


JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS



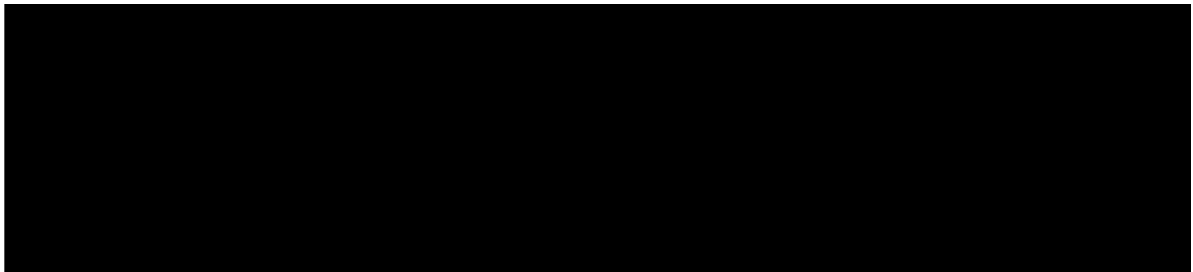
- Transmisiones mediante el traslado de soportes físicos:



TRANSFERENCIAS	TIPO DE TRASLADO
<ul style="list-style-type: none">• Interinstitucionales• Con entes privados	<ul style="list-style-type: none">• De soportes físicos• Físico de soportes electrónicos• Sobre redes electrónicas

- Técnicas de Supresión y Borrado Seguro de Datos Personales

- Métodos físicos:



JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- **Métodos lógicos:**

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

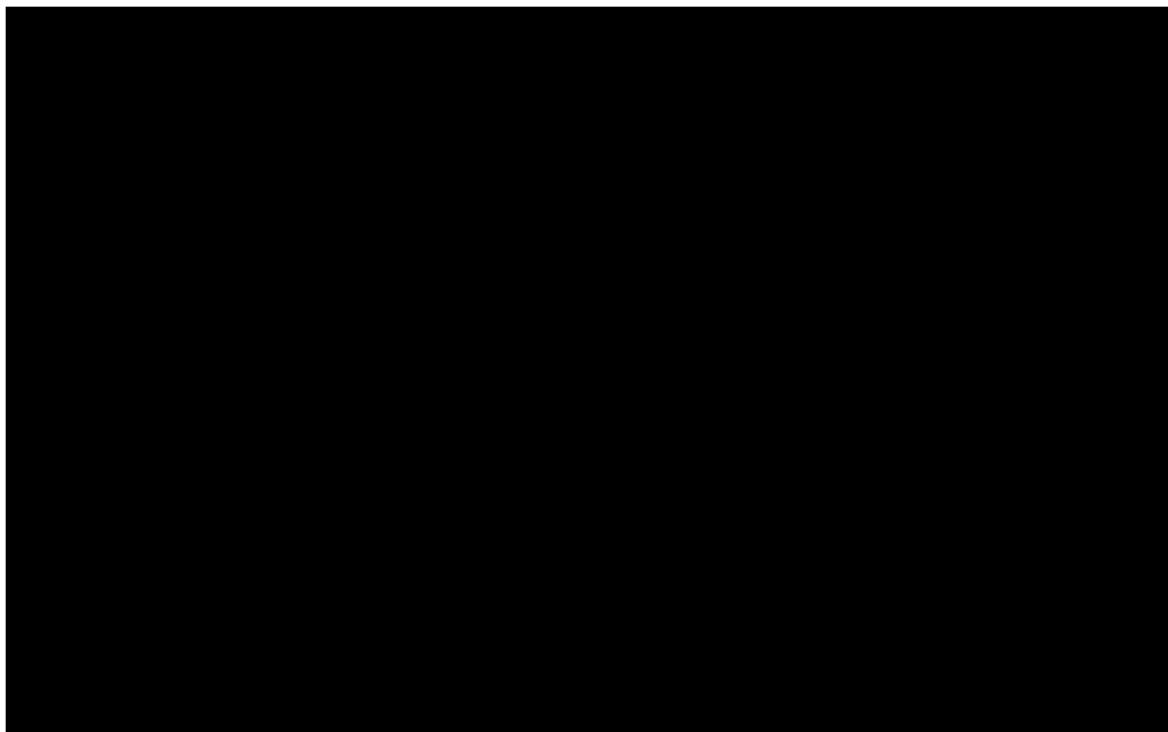
PLAN DE CONTINGENCIA PARA LA PROTECCIÓN DE LA INFORMACIÓN DE LA COORDINACIÓN GENERAL DE ASUNTOS JURÍDICOS

Clasificación de la contingencia:

Según sea el tipo de la contingencia se le puede asignar un grado de afectación:

- **Grado 1.-** son las más bajas que van desde fallas electrónicas, fallas con la conexión de internet y que pueden ser resueltas por el mismo personal de la Coordinación.
- **Grado 2.-** requiere tanto el apoyo del personal de la Coordinación, así como de personal externo (por ejemplo, en un incendio apoyo de bomberos y protección civil).
- **Grado 3.-** son contingencias que por su alcance pueden afectar severamente la operatividad de la Coordinación y se requiere además del apoyo externo.

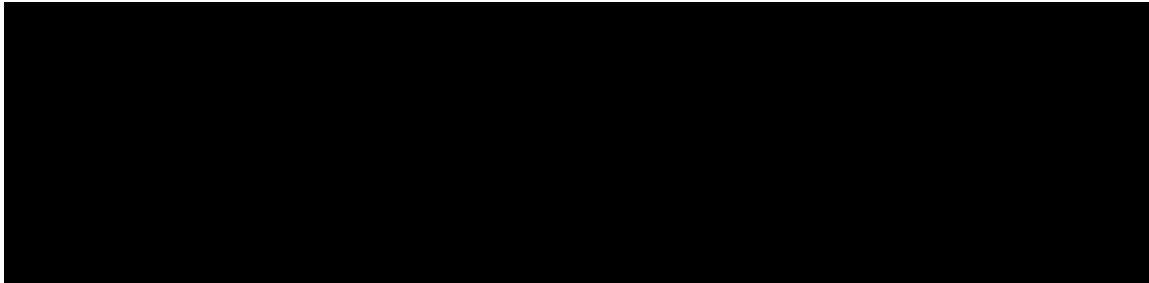
Consideraciones Principales:



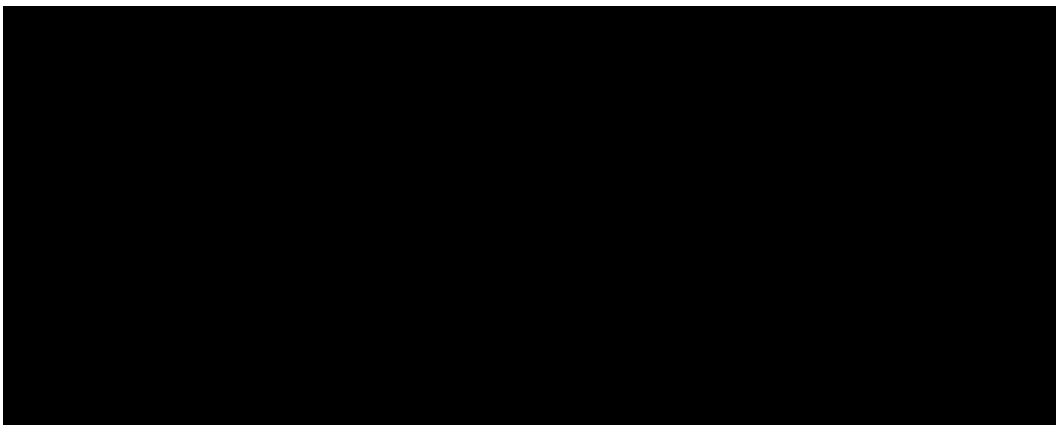
JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Lugar alternativo de trabajo

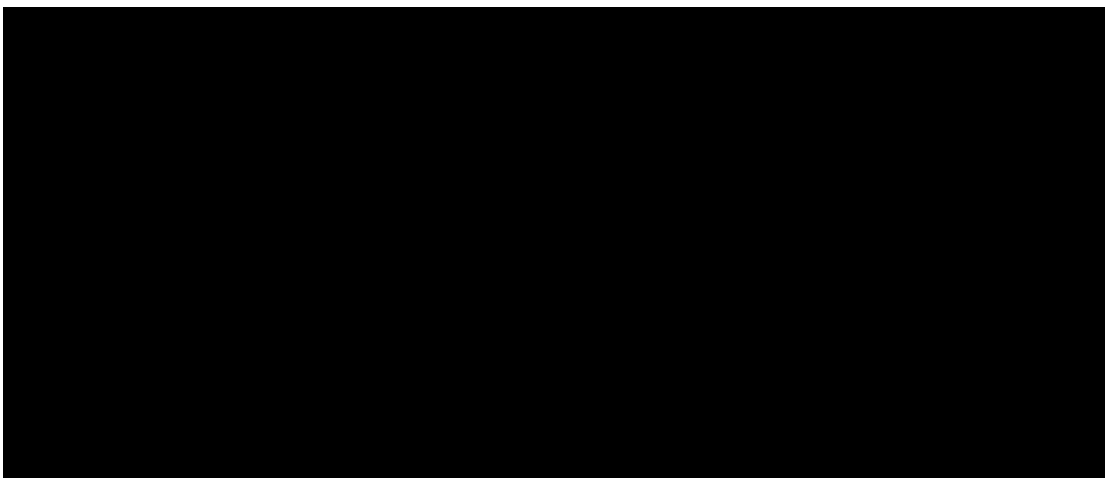


En caso de contar con un ambiente alterno debe contar con los siguientes recursos:



Medidas preventivas ante siniestros

Medidas prevención y conservación de los archivos:



COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

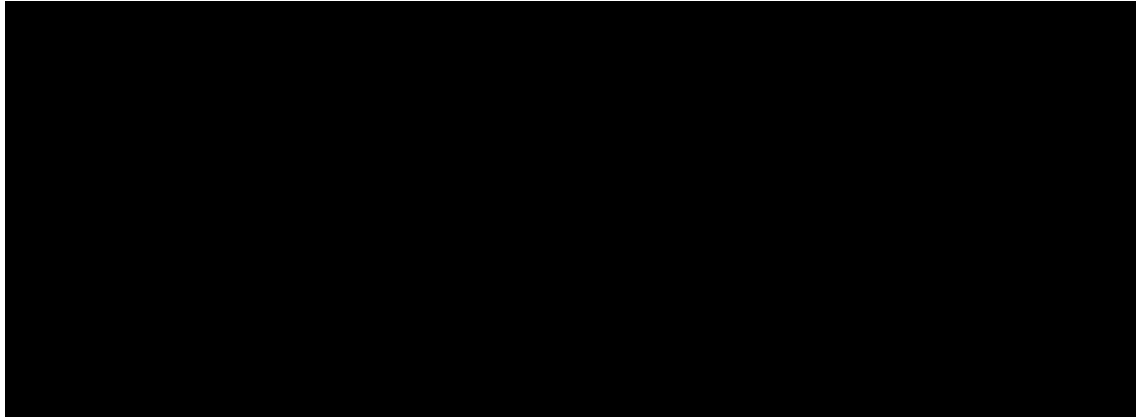
Medidas preventivas en caso de incendios:

Sobre el resguardo de la información en caso de incendio:

Durante un incendio:

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS



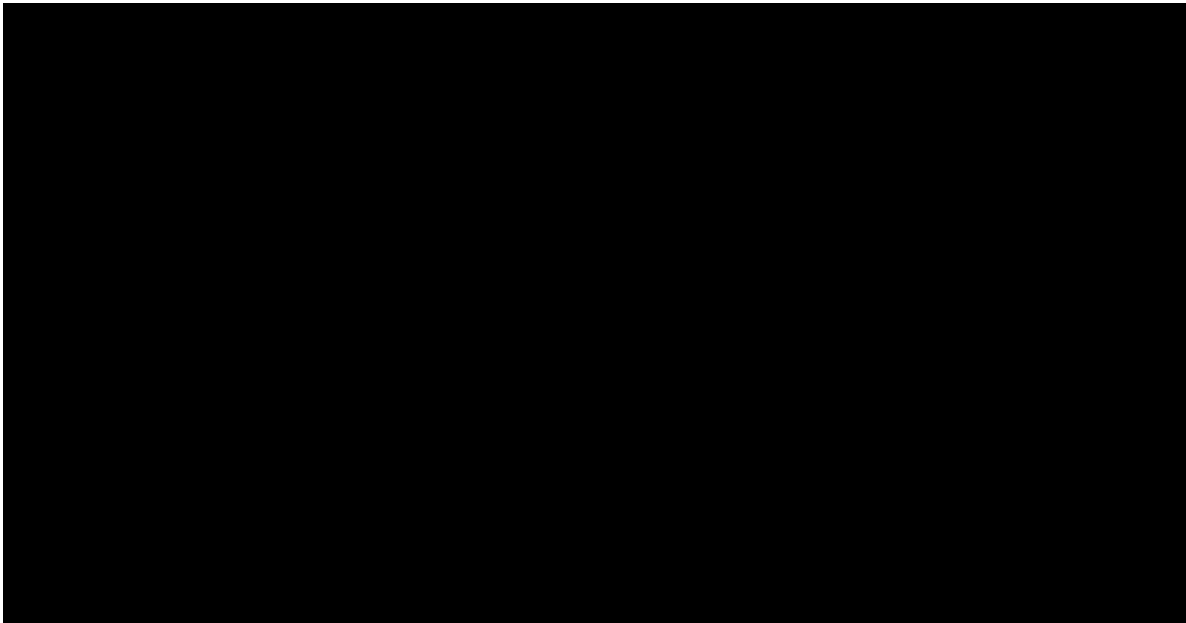
Después de incendio:



2. Terremoto:



Medidas preventivas en caso de sismo:



JURÍDICO

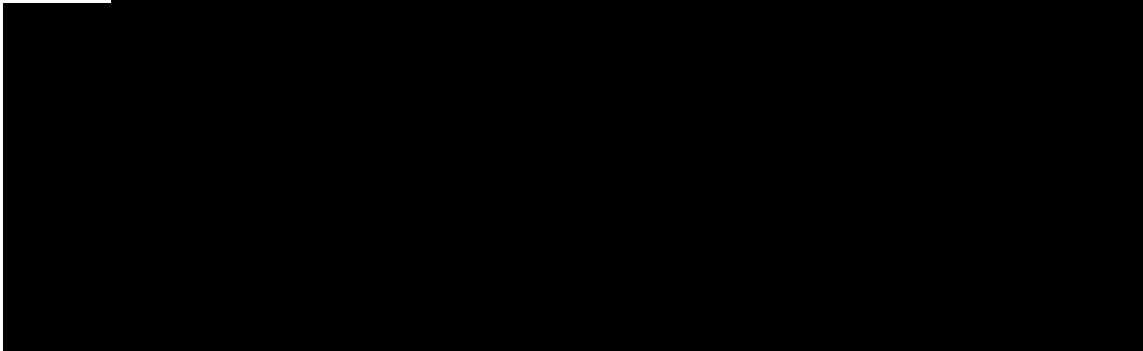
COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

Durante un sismo:

Mantener la calma y ubicarse en una zona de segura.

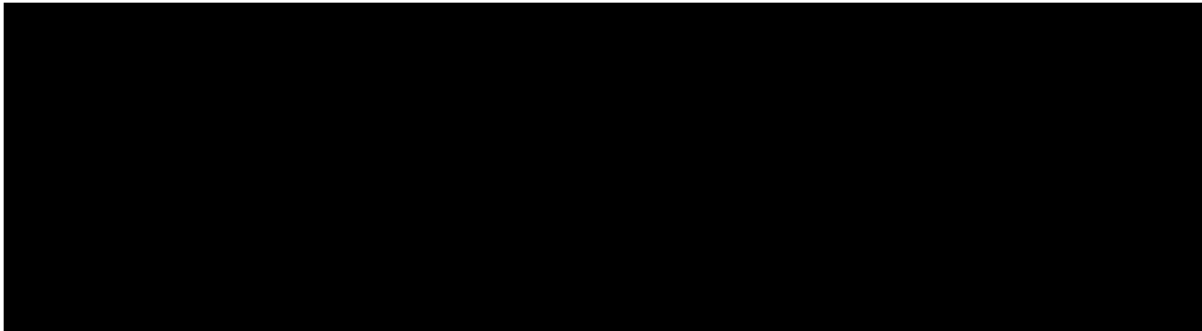
- Pararse bajo un marco de puerta con trabe o de espaldas a un muro de carga
- Adosarse a una columna o a un muro
- Alejarse de vidrios, colgaduras, etc.
- Retirarse de estanterías, etc.
- Si se está en una calle, ir a un refugio
- Si se está en un vehículo, detenerse y salir del mismo

Después de un sismo:



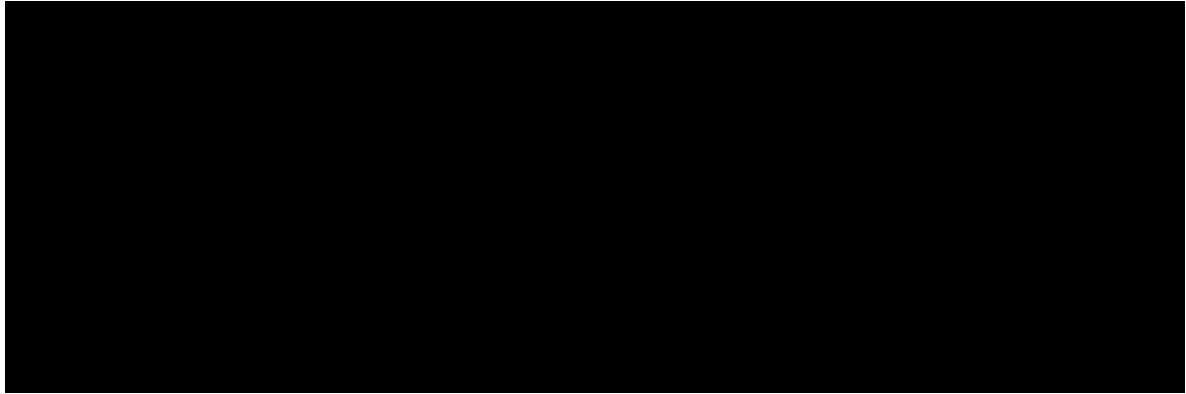
3. Inundaciones:

Medidas preventivas en caso de inundación:

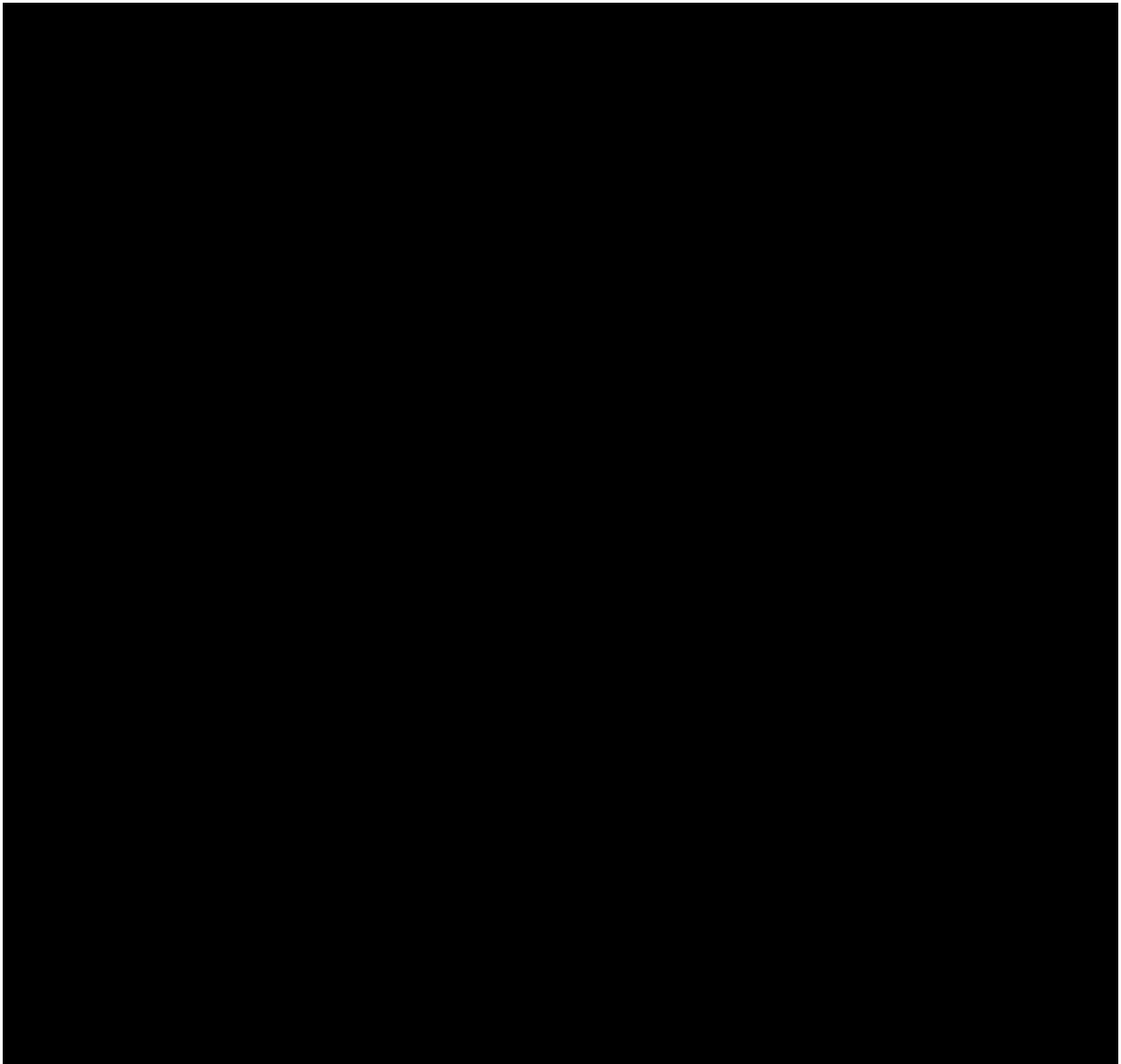


JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

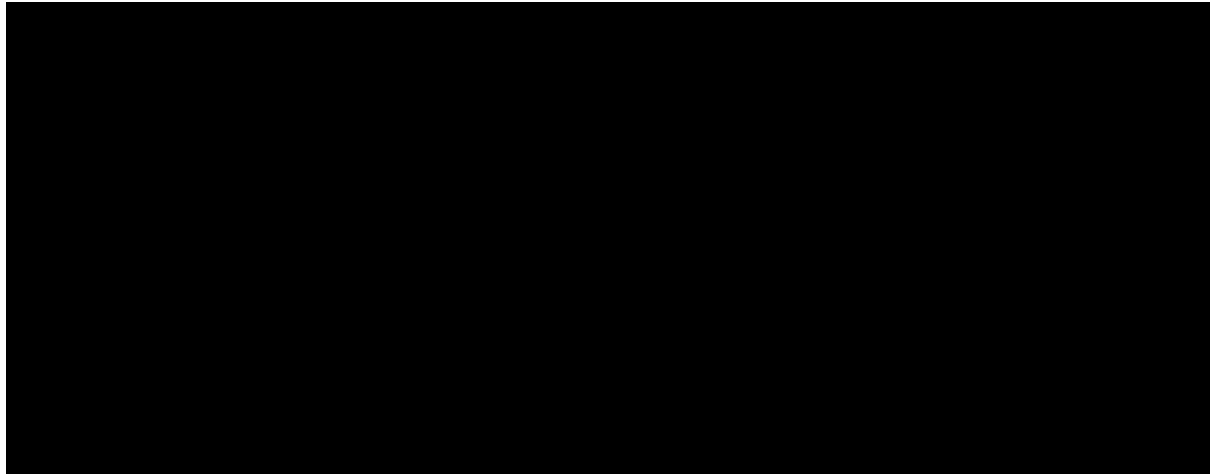


Durante una inundación:

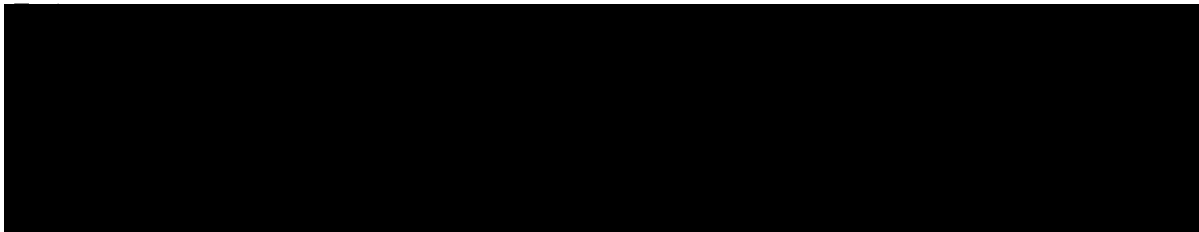


JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

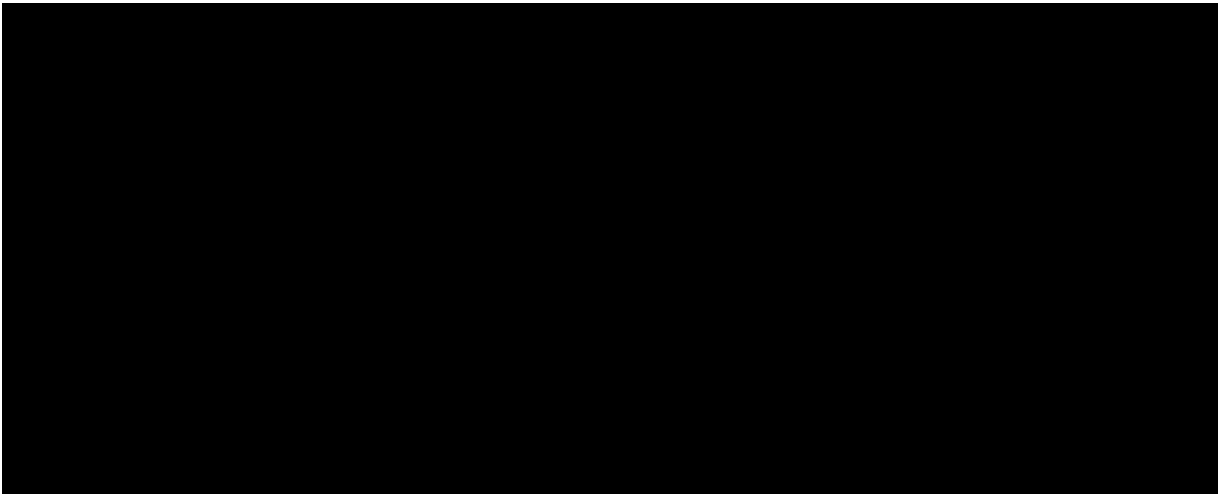


4. Robo:

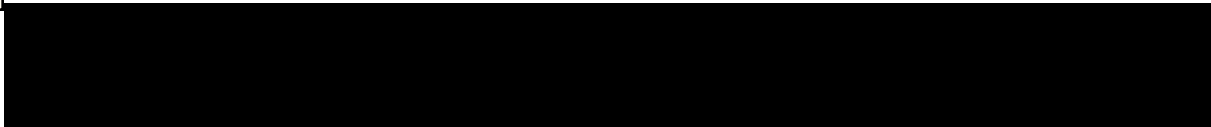


5. Amenazas informáticas:

Medidas preventivas para amenazas informáticas:



Hackeo informático



the 1990s, the number of people in the United States who are 65 years of age or older has increased by 50 percent, and the number of people 75 years of age or older has increased by 100 percent. The number of people 85 years of age or older has increased by 200 percent. The number of people 95 years of age or older has increased by 400 percent. The number of people 100 years of age or older has increased by 1,000 percent. The number of people 105 years of age or older has increased by 2,000 percent. The number of people 110 years of age or older has increased by 4,000 percent. The number of people 115 years of age or older has increased by 8,000 percent. The number of people 120 years of age or older has increased by 16,000 percent. The number of people 125 years of age or older has increased by 32,000 percent. The number of people 130 years of age or older has increased by 64,000 percent. The number of people 135 years of age or older has increased by 128,000 percent. The number of people 140 years of age or older has increased by 256,000 percent. The number of people 145 years of age or older has increased by 512,000 percent. The number of people 150 years of age or older has increased by 1,024,000 percent. The number of people 155 years of age or older has increased by 2,048,000 percent. The number of people 160 years of age or older has increased by 4,096,000 percent. The number of people 165 years of age or older has increased by 8,192,000 percent. The number of people 170 years of age or older has increased by 16,384,000 percent. The number of people 175 years of age or older has increased by 32,768,000 percent. The number of people 180 years of age or older has increased by 65,536,000 percent. The number of people 185 years of age or older has increased by 131,072,000 percent. The number of people 190 years of age or older has increased by 262,144,000 percent. The number of people 195 years of age or older has increased by 524,288,000 percent. The number of people 200 years of age or older has increased by 1,048,576,000 percent. The number of people 205 years of age or older has increased by 2,097,152,000 percent. The number of people 210 years of age or older has increased by 4,194,304,000 percent. The number of people 215 years of age or older has increased by 8,388,608,000 percent. The number of people 220 years of age or older has increased by 16,777,216,000 percent. The number of people 225 years of age or older has increased by 33,554,432,000 percent. The number of people 230 years of age or older has increased by 67,108,864,000 percent. The number of people 235 years of age or older has increased by 134,217,728,000 percent. The number of people 240 years of age or older has increased by 268,435,456,000 percent. The number of people 245 years of age or older has increased by 536,870,912,000 percent. The number of people 250 years of age or older has increased by 1,073,741,824,000 percent. The number of people 255 years of age or older has increased by 2,147,483,648,000 percent. The number of people 260 years of age or older has increased by 4,294,967,296,000 percent. The number of people 265 years of age or older has increased by 8,589,934,592,000 percent. The number of people 270 years of age or older has increased by 17,179,869,184,000 percent. The number of people 275 years of age or older has increased by 34,359,738,368,000 percent. The number of people 280 years of age or older has increased by 68,719,476,736,000 percent. The number of people 285 years of age or older has increased by 137,438,953,472,000 percent. The number of people 290 years of age or older has increased by 274,877,906,944,000 percent. The number of people 295 years of age or older has increased by 549,755,813,888,000 percent. The number of people 300 years of age or older has increased by 1,099,511,627,776,000 percent. The number of people 305 years of age or older has increased by 2,199,023,255,552,000 percent. The number of people 310 years of age or older has increased by 4,398,046,511,104,000 percent. The number of people 315 years of age or older has increased by 8,796,093,022,208,000 percent. The number of people 320 years of age or older has increased by 17,592,186,044,416,000 percent. The number of people 325 years of age or older has increased by 35,184,372,088,832,000 percent. The number of people 330 years of age or older has increased by 70,368,744,177,664,000 percent. The number of people 335 years of age or older has increased by 140,737,488,355,328,000 percent. The number of people 340 years of age or older has increased by 281,474,976,710,656,000 percent. The number of people 345 years of age or older has increased by 562,949,953,421,312,000 percent. The number of people 350 years of age or older has increased by 1,125,899,906,842,624,000 percent. The number of people 355 years of age or older has increased by 2,251,799,813,685,248,000 percent. The number of people 360 years of age or older has increased by 4,503,599,627,370,496,000 percent. The number of people 365 years of age or older has increased by 9,007,199,254,740,992,000 percent. The number of people 370 years of age or older has increased by 18,014,398,509,481,984,000 percent. The number of people 375 years of age or older has increased by 36,028,797,018,963,968,000 percent. The number of people 380 years of age or older has increased by 72,057,594,037,927,936,000 percent. The number of people 385 years of age or older has increased by 144,115,188,075,855,872,000 percent. The number of people 390 years of age or older has increased by 288,230,376,151,711,744,000 percent. The number of people 395 years of age or older has increased by 576,460,752,303,423,488,000 percent. The number of people 400 years of age or older has increased by 1,152,921,504,606,846,976,000 percent. The number of people 405 years of age or older has increased by 2,305,843,009,213,693,952,000 percent. The number of people 410 years of age or older has increased by 4,611,686,018,427,387,904,000 percent. The number of people 415 years of age or older has increased by 9,223,372,036,854,775,808,000 percent. The number of people 420 years of age or older has increased by 18,446,744,073,709,551,616,000 percent. The number of people 425 years of age or older has increased by 36,893,488,147,419,103,232,000 percent. The number of people 430 years of age or older has increased by 73,786,976,294,838,206,464,000 percent. The number of people 435 years of age or older has increased by 147,573,952,589,676,412,928,000 percent. The number of people 440 years of age or older has increased by 295,147,905,179,352,825,856,000 percent. The number of people 445 years of age or older has increased by 590,295,810,358,705,651,712,000 percent. The number of people 450 years of age or older has increased by 1,180,591,620,717,411,303,424,000 percent. The number of people 455 years of age or older has increased by 2,361,183,241,434,822,606,848,000 percent. The number of people 460 years of age or older has increased by 4,722,366,482,869,645,213,696,000 percent. The number of people 465 years of age or older has increased by 9,444,732,965,739,290,427,392,000 percent. The number of people 470 years of age or older has increased by 18,889,465,931,478,580,854,784,000 percent. The number of people 475 years of age or older has increased by 37,778,931,862,957,161,709,568,000 percent. The number of people 480 years of age or older has increased by 75,557,863,725,914,323,419,136,000 percent. The number of people 485 years of age or older has increased by 151,115,727,451,828,646,838,272,000 percent. The number of people 490 years of age or older has increased by 302,231,454,903,657,293,676,544,000 percent. The number of people 495 years of age or older has increased by 604,462,909,807,314,587,353,088,000 percent. The number of people 500 years of age or older has increased by 1,208,925,819,614,629,174,706,176,000 percent. The number of people 505 years of age or older has increased by 2,417,851,639,229,258,349,412,352,000 percent. The number of people 510 years of age or older has increased by 4,835,703,278,458,516,698,824,704,000 percent. The number of people 515 years of age or older has increased by 9,671,406,556,917,033,397,649,408,000 percent. The number of people 520 years of age or older has increased by 19,342,813,113,834,066,795,298,816,000 percent. The number of people 525 years of age or older has increased by 38,685,626,227,668,133,590,597,632,000 percent. The number of people 530 years of age or older has increased by 77,371,252,455,336,267,181,195,264,000 percent. The number of people 535 years of age or older has increased by 154,742,504,910,672,534,362,390,528,000 percent. The number of people 540 years of age or older has increased by 309,485,009,821,345,068,724,781,056,000 percent. The number of people 545 years of age or older has increased by 618,970,019,642,690,137,449,562,112,000 percent. The number of people 550 years of age or older has increased by 1,237,940,039,285,380,274,899,124,224,000 percent. The number of people 555 years of age or older has increased by 2,475,880,078,570,760,549,798,248,448,000 percent. The number of people 560 years of age or older has increased by 4,951,760,157,141,521,099,596,496,896,000 percent. The number of people 565 years of age or older has increased by 9,903,520,314,283,042,199,193,993,792,000 percent. The number of people 570 years of age or older has increased by 19,807,040,628,566,084,398,387,

PRINCIPIOS SOBRE LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

- **Finalidades Legítimas y Lealtad:** Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales.
- **Calidad:** El principio de calidad radica en que los datos personales tratados deben ser exactos, completos, pertinentes, actualizados y correctos según se requiera para el cumplimiento de la finalidad para la cual son tratados.
- **Licitud:** Implica que los responsables deben tratar los datos personales de manera lícita, conforme a lo dispuesto por la legislación mexicana y el derecho internacional aplicable, así como por la normativa que le resulte aplicable a cada responsable. El principio de licitud establece que ni los responsables ni nadie puede tratar los datos personales para actividades ilícitas, ni de forma tal que contravenga lo dispuesto por la LFPDPPP, la LGPDPPSO, ni en ningún otro ordenamiento vigente en México, o acuerdo internacional del cual el país sea parte.
- **Información:** El principio de información obliga a los responsables a informar a los titulares, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.
- **Transparencia y Consentimiento:** Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el tratamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran.
- **Pertinencia y Necesidad:** Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes, y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.
- **Tratamiento y Conservación Limitados:** Los datos personales deberían ser tratados y conservados solamente de manera legítima no incompatible con las finalidades para las cuales se recopilaron. Su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades y de conformidad con la legislación nacional correspondiente.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

- **Confidencialidad:** Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.
- **Seguridad de los Datos:** La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aun cuando éstos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.
- **Exactitud de los Datos:** Los datos personales deberían mantenerse exactos, completos y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad.
- **Acceso, Rectificación, Cancelación, Oposición y Portabilidad:** Se debería disponer de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales. Como regla general, el ejercicio de esos derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional y estar en conformidad con los estándares internacionales aplicables.
- **Datos Personales Sensibles:** Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.
- **Responsabilidad:** Los responsables y encargados del tratamiento de datos deberían adoptar e implementar medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.

DERECHOS ARCO

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, reconoce el derecho que tienen los ciudadanos para acceder, rectificar y cancelar sus datos personales, así como oponerse a su uso. A estos derechos se les conoce como derechos ARCO, y se encuentran reconocidos tanto en la LFPDPPP como en la LGPDPSO.

- **Derecho de Acceso:** Es el derecho que tienen los titulares de solicitar al responsable que sus datos personales no sean utilizados o que termine el uso de estos, siempre que exista causa legítima conforme a lo dispuesto en los ordenamientos jurídicos aplicables. Como en el derecho de cancelación, no siempre es procedente la oposición al tratamiento de los datos personales, pues pueden ser necesarios para algún aspecto legal o para el cumplimiento de obligaciones determinadas.
- **Derecho de rectificación:** Es el derecho que tienen los titulares de solicitar la rectificación o corrección de sus datos personales, cuando estos sean inexactos, incompletos o no se encuentren actualizados.
- **Derecho de cancelación:** Es el derecho que tienen los titulares de solicitar al responsable que cancelen o eliminen sus datos personales de los archivos, registros, expedientes, bases de datos o sistemas del responsable, a efecto de que se detenga el tratamiento por parte de éste, a partir de un bloqueo de estos y su posterior supresión. Es importante señalar que no en todos los casos es procedente la eliminación de tus datos personales, toda vez que puede existir alguna cuestión legal que impida su cancelación, o bien, puede que los datos personales sean necesarios para el cumplimiento de alguna responsabilidad surgida por el tratamiento.
- **Derecho de oposición:** Es el derecho que tienen los titulares de solicitar al responsable que sus datos personales no sean utilizados o que termine el uso de estos, siempre que exista causa legítima conforme a lo dispuesto en los ordenamientos jurídicos aplicables. Como en el derecho de cancelación, no siempre es procedente la oposición al tratamiento de los datos personales, pues pueden ser necesarios para algún aspecto legal o para el cumplimiento de obligaciones determinadas.

DEBERES

Además de los principios y obligaciones referidas con anterioridad, los responsables del sector público y privado deben de cumplir con los deberes de seguridad y confidencialidad, mismos que serán desarrollados a continuación:

- **Deber de seguridad:** El deber de seguridad refiere a la obligación de establecer y mantener medidas de seguridad administrativas, físicas y técnicas con el propósito de proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Las medidas de seguridad administrativas son controles que ayudan a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales; por ejemplo, dicha medida puede consistir en capacitación al personal que trata datos personales, con el objeto de evitar cualquier vulneración a los mismos. Por su parte, las medidas físicas son controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso no autorizado; por ejemplo, mantener las áreas de trabajo, mobiliario y equipos debidamente cerrados con los controles y candados suficientes.

- **Deber de confidencialidad:** El deber de confidencialidad implica que el responsable debe guardar secreto respecto de los datos personales que son tratados, es decir, que los datos personales del titular no se difundan o compartan con terceros, salvo que se cuente con el consentimiento para ello, o bien, por alguna obligación normativa que exija su difusión. Para garantizar el cumplimiento del deber de confidencialidad, los responsables tienen que establecer medidas durante todas las fases del tratamiento de los datos personales, incluso después de finalizar la relación con el titular.

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

PROGRAMA GENERAL DE CAPACITACIÓN:

La capacitación del personal de la Coordinación General es trimestral y está dividida en cinco áreas de responsabilidad con las mismas temáticas:

NIVELES DE RESPONSABILIDAD	TEMÁTICA
Departamento de Transparencia	<ul style="list-style-type: none">• Primer trimestre: Generalidades de la Ley de Protección de Datos en Posesión de Sujetos Obligados.• Segundo trimestre: Principios, funciones y deberes.• Tercer trimestre: Sistema de gestión, medidas de seguridad y acciones preventivas.
Coordinador(a), Subcoordinadores(ras) y Directores(ras)	
Secretaría Particular	
Jefes de Departamento y Jefes de Área	
Personal de base y contrato que trata datos personales	

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

PLAN DE TRABAJO

Se ha planteado implementar la totalidad de las medidas de seguridad faltantes a partir de la aprobación del presente documento de seguridad.

En ese sentido, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos como la compra de muebles incombustibles, y cestos metálicos para papeles y sustitución de los materiales plásticos e inflamables, se realizarán conforme a los tiempos administrativos de la Coordinación y el presupuesto permitido.

CONTROL	PÁRAMETROS
Fuga de información: se deben prevenir las oportunidades de fuga de información.	Todas las áreas
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Todas las áreas
Política sobre el uso de controles criptográficos: una política sobre el uso de controles para la protección de la información que debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.
Política sobre el uso de controles criptográficos: una política sobre el uso de controles para la protección de la información que debe ser desarrollada e implementada.	Todas las áreas
Eliminación de los derechos de acceso: los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiere hacer un ajuste.	Todas las áreas
Eliminación y entrega de los medios de almacenamiento: los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Todas las áreas
Elaboración del Plan de Contingencia.	Todas las áreas

JURÍDICO

COORDINACIÓN GENERAL
DE ASUNTOS JURÍDICOS

ACTIVIDAD	ÁREAS INVOLUCRADAS
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, de contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Unidad de Administración y Finanzas y el Departamento de Transparencia y Acceso a la Información Pública.
Administración de medios removibles: Deberán de documentarse e implementarse procedimientos para la gestión de medios removibles.	Departamento de Transparencia y Acceso a la Información Pública.
Uso de sistema de monitoreo: Se deben de establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Departamento de Transparencia y Acceso a la Información Pública.
Verificación del cumplimiento técnico: Se deben de verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Departamento de Transparencia y Acceso a la información Pública.
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Departamento de Transparencia y Acceso a la Información Pública y la Unidad de Administración y Finanzas

MONITOREO DE LAS MEDIDAS DE SEGURIDAD

Primer monitoreo y evaluación de los sistemas de seguridad durante el mes de diciembre y presentación de informe al pleno durante los primeros diez días de enero.

Segundo monitoreo y evaluación de los sistemas de seguridad durante el mes de julio y presentación de informe al pleno durante los primeros diez días del agosto.

RESPONSABLE DEL DESARROLLO:

Licenciada Brianda Aurora Ramírez Pérez

Jefa de Departamento de Transparencia y Acceso a la Información Pública

Tel. +52 (993) 310 07 80 Ext. 29815

transparencia_cgajtab@hotmail.com

REVISÓ:

Maestro Juan Carlos Castillo Guzmán

Director General de Normatividad y Transparencia

Tel. +52 (993) 310 07 80 Ext. 29853

juancastillo@tabasco.gob.mx

AUTORIZÓ:

Doctora Karla Cantoral Domínguez

Titular de la Coordinación General de Asuntos Jurídicos

Tel. +52 (993) 310 07 80 Ext. 29804

karlacantoral@tabasco.gob.mx

FECHA DE ELABORACIÓN:

31 de mayo de 2024