



## PLATAFORMA NACIONAL DE TRANSPARENCIA TABASCO

De conformidad con lo dispuesto en el artículo 130 de la Ley de Transparencia y Acceso a la Información del Estado de Tabasco (LTAIPET) se emite el presente Acuse de Recibo de la solicitud de información presentada ante la Unidad de Transparencia a la Información del sujeto obligado: **TRIBUNAL SUPERIOR DE JUSTICIA**

Fecha de presentación de la solicitud: **17/06/2019 23:47**

Número de Folio: **01197019**

Nombre o denominación social del solicitante: **MARIA HERNANDEZ**

Información que requiere: **DOCUMENTO DE SEGURIDAD QUE SEÑALA EL ART. 40 DE LA EY DE PROTECCION DE DATOS PERSONALES EN POSESION DE LOS SUJETOS OBLIGADOS DEL ESTADO DE TABASCO , QUE CONTENGA LOS REQUISITOS QUE ESTA LEY SEÑALA**

Otros datos proporcionados para facilitar la localización de la información:

¿Cómo desea recibir la información? **Electrónico a través del sistema de solicitudes de acceso la información de la PNT**

\*No incluir datos personales, ya que éstos serán publicados como parte de la respuesta.

\*Debe identificar con claridad y precisión de los datos e información que requiere.

\* La solicitud recibida en día hábil después de las 16:00 horas o en cualquier hora en día inhábil, se tendrá presentada a partir de las 08:00 horas del día hábil siguiente.

Los términos de todas las notificaciones previstas en esta Ley, empezarán a correr al día siguiente al que se practiquen.

Cuando los plazos fijados por esta Ley sean en días, estos se entenderán como hábiles según lo establecido en el artículo 133 de la LTAIPET.

### Plazos de respuesta:

La respuesta a toda solicitud realizada en los términos de la presente Ley, deberá ser notificada al interesado en un plazo no mayor a quince días, contados a partir del día siguiente a la presentación de aquella: **09/07/2019**. El plazo podrá ampliarse en forma excepcional hasta por cinco días, de mediar circunstancias que hagan difícil reunir la información solicitada, siempre y cuando existan razones fundadas y motivadas, las cuales deberán ser aprobadas por el Comité de Transparencia mediante la emisión de una resolución que deberá notificarse al solicitante, antes de su vencimiento según lo establecido en el artículo 138 de la LTAIPET.

En caso de requerirle que aclare, complete, indique otros elementos, corrija los datos proporcionados o bien precise uno o varios requerimientos de la información se le notificará en un plazo no mayor de 5 días hábiles: **25/06/2019**. El plazo para responder el requerimiento será hasta por 10 días según lo establecido en el artículo 131 párrafo cuarto de la LTAIPET.

Este requerimiento interrumpe el plazo que la Ley otorga para atender la solicitud, el cual iniciará de nuevo al día siguiente cuando se cumpla el requerimiento según lo establecido en el artículo 131 párrafo cuarto de la LTAIPET.

En caso de que esta Unidad de Transparencia a la Información no sea competente se le comunicará y orientará en un plazo no mayor a 3 días hábiles: **21/06/2019** según lo establecido en los artículos 142, LTAIPET.

Si los Sujetos Obligados son competentes para atender parcialmente la solicitud de acceso a la información, deberán dar respuesta respecto de dicha parte. En cuanto a la información sobre la cual es incompetente, se procederá conforme lo señala el párrafo anterior.

Ante la falta de respuesta a una solicitud en el plazo previsto y en caso de que proceda el acceso, los costos de reproducción y envío correrán a cargo del sujeto obligado según lo establecido en el artículo 140 párrafo tercero de la LTAIPET.

## **Observaciones**

Se le recomienda dar frecuentemente seguimiento a su solicitud.

\* Tratándose de solicitudes de acceso a información formuladas mediante la plataforma nacional, se asignará automáticamente un número de folio, con el que los solicitantes podrán dar seguimiento a sus requerimientos. En los demás casos, la Unidad de Transparencia tendrá que registrar y capturar la solicitud de acceso en la plataforma nacional y deberá enviar el acuse de recibo al solicitante en el que se indique la fecha de recepción, el folio que corresponda y los plazos de respuesta aplicables según lo establecido en el artículo 130 párrafo segundo de la LTAIPET.

\* Si su solicitud está relacionada con Datos Personales está obligado a acompañar a su escrito copia certificada de su identificación oficial, o en su defecto la original con copia, misma que se le devolverá previo cotejo, por lo que deberá acudir personalmente al domicilio de la Unidad de Transparencia a la Información de este Sujeto Obligado para acreditar su personalidad. Se consideran identificación oficial los documentos siguientes: Credencial de elector, cartilla militar, cédula profesional.



**DIRECTOR**

Tel. (993) 3 58 20 00 ext. 4013 y 4082  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Folio PNT: 01197019

Número de Expediente Interno: PJ/UTAIP/351/2019

Acuerdo con Oficio No.: TSJ/UT/1067/19

**ACUERDO DE DISPONIBILIDAD EN VERSIÓN PÚBLICA.**

Villahermosa, Tabasco a 09 de Julio de 2019.

**CUENTA:** Con el documento de seguridad aprobado mediante el acta de la Vigésima Sexta Sesión Ordinaria emitida por el Comité de Transparencia de este Poder Judicial. -----  
-----Conste-----

Vista la cuenta que antecede se acuerda:

**PRIMERO:** Vista la solicitud de acceso a la información pública, con número de expediente PJ/UTAIP/351/2019, recibida el diecisiete de junio de dos mil diecinueve, a las veintitrés horas con cuarenta y siete minutos, presentada vía Plataforma Nacional de Transparencia, mediante la cual se requiere: ***"...Documento de seguridad que señala el art. 40 de la Ley de Protección de Datos Personales en posesión de los sujetos obligados del estado de Tabasco, que contenga los requisitos que esta ley señala..."***, por lo que se ordena agregar a los autos, la documental de cuenta para que surta los efectos legales correspondientes.-----

**SEGUNDO:** Con fundamento en los artículos 4, 6, 49, 50 fracciones III y IV y el 138 en relación con el 133, todos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, así como el artículo 45 de su Reglamento, **se acuerda que la información solicitada ante esta Unidad de Transparencia es parcialmente pública.**-----

Por lo anteriormente expuesto, se ordena entregar a la persona interesada el documento solicitado en versión pública, así como el acta de la Vigésima Sexta Sesión Ordinaria emitida por el Comité de Transparencia de este Poder Judicial, en virtud de los argumentos aludidos por el referido órgano colegiado.-----

Es importante hacer notar, que en atención a lo dispuesto en los artículos 73 fracciones I, II y VI de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco y artículo 3 fracciones II y V, artículos 18, 19, 21, 22 y 20 de su reglamento, este sujeto obligado tiene el imperativo legal de proteger la privacidad de los datos personales, por lo que se acuerda entregar a la persona interesada, el documento requerido en versión pública, suprimiéndose los datos que son susceptibles de vulnerar y poner en riesgo a este ente público.-----



**PODER JUDICIAL  
DEL ESTADO DE TABASCO**

**DIRECTOR**Tel. (993) 3 58 20 00 ext. 4013 y 4082  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Por lo anteriormente expuesto, cabe señalar que el procedimiento para que la información se proporcionara en versión pública, fue puesto a consideración del Comité de Transparencia de este sujeto obligado y confirmado a través del acta de la Vigésima Sexta Sesión Ordinaria emitida por el Comité de Transparencia de este Poder Judicial.-----

**TERCERO:** En tal virtud, se ordena proporcionar al requirente de información, el presente Acuerdo de Disponibilidad en Versión Pública, junto con el documento solicitado.-----

En atención al artículo 6 de la Ley en la materia, la información solicitada se pone a disposición de la persona interesada en el estado en que se encuentra, en virtud de que la obligatoriedad de los sujetos obligados no comprende el procesamiento de la misma, ni el de realizar resúmenes, efectuar cálculos o practicar cualquier clase de investigación, es decir que no se tiene el imperativo legal de presentarla conforme al interés del solicitante, por lo que únicamente se proporciona información contenida en documentos previamente generados o en su caso que obren en los archivos del sujeto obligado.-----

Para sustentar lo anteriormente señalado, se cita el Criterio 009-10, emitido por el Pleno del Instituto Nacional de Transparencia y Acceso a la Información, Protección de Datos Personales, antes IFAI, mismo que se transcribe:

#### Criterio 009-10

**Las dependencias y entidades no están obligadas a generar documentos *ad hoc* para responder una solicitud de acceso a la información.** Tomando en consideración lo establecido por el artículo 42 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que establece que las dependencias y entidades sólo estarán obligadas a entregar documentos que se encuentren en sus archivos, las dependencias y entidades no están obligadas a elaborar documentos *ad hoc* para atender las solicitudes de información, sino que deben garantizar el acceso a la información con la que cuentan en el formato que la misma así lo permita o se encuentre, en aras de dar satisfacción a la solicitud presentada.

#### **Expedientes:**

0438/08	Pemex Exploración y Producción – Alonso Lujambio Irazábal
1751/09	Laboratorios de Biológicos y Reactivos de México S.A. de C.V. – María Marván Laborde
2868/09	Consejo Nacional de Ciencia y Tecnología – Jacqueline Peschard Mariscal
5160/09	Secretaría de Hacienda y Crédito Público – Ángel Trinidad Zaldívar
0304/10	Instituto Nacional de Cancerología – Jacqueline Peschard Mariscal.

Por último, es importante destacar que la actuación de este sujeto obligado se desarrolló con apego al principio de buena fe, entendido éste como un principio que obliga a todos a observar una determinada actitud de respeto y lealtad, de honradez en el tráfico jurídico y esto tanto cuando se ejerza un derecho, como cuando se cumpla un deber y por ello esta Institución en

Dr. Julio de Jesús Vázquez Ealcón



UNIDAD DE TRANSPARENCIA  
Y ACCESO A LA INFORMACIÓN

**DIRECTOR**

Tel. (993) 3 58 20 00 ext. 4013 y 4082  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

uso de sus atribuciones, atendió la solicitud conforme a su literalidad y al marco jurídico que rige el derecho de acceso a la información, además se notificó respuesta en los tiempos legales señalados para tal fin a como lo indica el numeral 138 de la Ley en la materia.-----

**Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.**

**Artículo 138.** La respuesta a toda solicitud de información realizada en los términos de la presente ley, deberá ser notificada al interesado en un plazo no mayor de quince días, contado a partir del día siguiente a la presentación de aquella. -----

**CUARTO:** En caso de no estar conforme con el presente acuerdo, hágasele saber a la persona interesada que dispone de 15 días hábiles, contados a partir del día hábil siguiente a la notificación de este proveído, para interponer por sí misma a través de representante legal, recursos de revisión ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública o ante esta Unidad de Transparencia, debiendo acreditar lo requisitos previstos en el numeral 150 de la Ley en la materia.-----

**QUINTO:** Publíquese la solicitud recibida y la respuesta dada en el Portal de Transparencia de este sujeto obligado, como lo dispone el artículo 12 de los Lineamientos Generales para el Cumplimiento de las Obligaciones de Transparencia de los Sujetos Obligados en el Estado de Tabasco, para los efectos correspondientes. -----

Notifíquese a través de la Plataforma Nacional de Transparencia, medio indicado por la persona interesada en su solicitud y en su oportunidad, archívese el presente asunto como total y legalmente concluido.-----Cúmplase.-----

Así lo acuerda, manda y firma, el Director de la Unidad de Acceso a la Información del Poder Judicial del Estado de Tabasco.-----

Esta hoja de firmas corresponde al Acuerdo de Disponibilidad de la Información de fecha 09 de julio de 2019, dictado en el expediente relativo a la solicitud de información identificada con el número de folio 01197019.-----



PODER JUDICIAL  
DEL ESTADO DE TABASCO



Dr. Julio de Jesús Vázquez Falcón

DIRECTOR



UNIDAD DE TRANSPARENCIA  
Y ACCESO A LA INFORMACIÓN

Tel. (993) 3 58 20 00 ext. 4013 y 4082  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

OFICIO No. TSJ/UT/694/19

Villahermosa, Tabasco, Mayo 21, de 2019.

ARQ. GLORIA GUADALUPE ASCENCIO LASTRA.- OFICIAL MAYOR  
LIC. GUSTAVO GÓMEZ AGUILAR.- TESORERO  
L.C.P. RODOLFO GABRIEL CUENCA RUIZ.- DIRECTOR DE CONTRALORÍA  
INTEGRANTES DEL COMITÉ DE TRANSPARENCIA  
DEL PODER JUDICIAL DEL ESTADO DE TABASCO  
P R E S E N T E S.

Por medio del presente, me permito invitarlos a ustedes, a la Vigésima Sexta Sesión Ordinaria, la cual tendrá verificativo el día Martes 21 de Mayo a las 12:00 horas, en la Sala "U" de esta Institución, por lo que hago de su conocimiento el orden del día correspondiente.

#### ORDEN DEL DÍA

- I. Lista de Asistencia.
- II. Declaratoria de quórum legal.
- III. Aprobación del documento de seguridad del Poder Judicial del Estado de Tabasco y clasificación de información en su modalidad de reserva parcial.
- IV. Clausura de la sesión.

Sin otro particular, me permito enviarles un cordial saludo.

ATENTAMENTE



C.c.p.- Archivo.







## VIGÉSIMA SEXTA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL PODER JUDICIAL DEL ESTADO DE TABASCO

En la ciudad de Villahermosa, capital del Estado de Tabasco, siendo las doce horas con cinco minutos del veintidós de mayo del dos mil diecinueve, reunidos los integrantes del Comité de Transparencia del Poder Judicial del Estado de Tabasco, los CC. Gloria Guadalupe Ascencio Lastra, Oficial Mayor y Presidenta; Gustavo Gómez Aguilar, Tesorero Judicial y Primer Vocal; Rodolfo Gabriel Cuenca Ruiz y Segundo Vocal, Director de Contraloría; así como el Dr. Julio de Jesús Vázquez Falcón, Director de la Unidad de Transparencia y Acceso a la Información y Secretario Técnico del Comité; en la sala "U" del edificio sede del Tribunal Superior de Justicia del Estado de Tabasco, con el objeto de celebrar la Vigésima Sexta Sesión Ordinaria, la Presidenta del Comité da lectura del Orden del Día para llevar a cabo la presente sesión, misma que se transcribe a continuación y que es aprobado por los todos los presentes.

### ORDEN DEL DÍA

- I. Lista de Asistencia.
- II. Declaratoria de quórum legal.
- III. Aprobación del documento de seguridad del Poder Judicial del Estado de Tabasco y clasificación de información en su modalidad de reserva parcial.
- IV. Clausura de la sesión.

**PRIMERO.** Encontrándose reunidos los integrantes del Comité de Transparencia del Poder Judicial del Estado de Tabasco, por lo que el Secretario Técnico del Comité, procede a pasar lista de asistencia, encontrándose todos aquí reunidos.

**SEGUNDO.** La Presidenta del Comité, después de recibir la lista de asistencia pasada por el Secretario Técnico, declara la existencia del quórum legal y por ende queda formalmente instalado el comité, por lo que serán válidos todos los acuerdos que aquí se tomen.

**TERCERO.** En virtud de las necesidades de este Poder Judicial, relativas a la Ley de Protección de Datos Personales, este Comité procede a la aprobación del documento de seguridad, que previamente fue generado por este órgano.





colegiado, conforme al artículo 40 de la ley referida y sus lineamientos, por lo que se procede a tomar el siguiente:

#### ACUERDO CT/073/2019

Con fundamento en los artículos 1, 3 fracción XIII, 36 y 40 de la Ley de Protección de Datos Personales en posesión de sujetos obligados vigente en la entidad, este órgano colegiado **CONFIRMA** por unanimidad de votos, la aprobación del documento de seguridad, con el propósito de garantizar el derecho de toda persona a la protección de sus datos personales y en virtud de los artículos 6 apartado A fracciones II y III, 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos y 4 bis fracciones III y IV de la Constitución Política del Estado Libre y Soberano de Tabasco.

Ahora bien, derivado de la solicitud de información registrada con folio interno PJ/UTAIP/213/2019, relativa a “...Documento de seguridad a que se refiere el artículo 40 de la Ley de Protección de Datos Personales, que contenga los requisitos que ese artículo señala...”, resulta necesario realizar la clasificación de dicho documento en su modalidad de reservada, en virtud de que contiene información relativa a la función pública que por disposición legal temporalmente queda prohibido su manejo, distribución, publicación, publicación y difusión generales, con excepción de las autoridades competentes que, de conformidad con la ley, tengan acceso a ella.

Por consiguiente, se advierte que dicho documento, contiene información relativa a las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros, en virtud de lo cual, es pertinente considerar que deban reservarse algunas secciones del documento en cuestión, toda vez que del análisis efectuado, adquieren el carácter de reservado, con fundamento en el artículo 121, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. Bajo esta concepción, es evidente que la difusión de dicha información, en nada contribuye a la rendición de cuentas o a la transparencia de la gestión gubernamental, ya que su publicación podría actualizar un daño presente, probable y específico a los principios jurídicos tutelados por la Ley de Transparencia vigente en el Estado.





Se estima que es procedente clasificar como restringida en su modalidad de reservada el documento de seguridad en lo relativo a las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros, en virtud de encontrarse en la hipótesis prevista en la fracción I del artículo 121 de la Ley de Transparencia vigente en el Estado, por lo anterior, se tienen las siguientes:

## CONSIDERACIONES

**I. Competencia.** El Comité de Transparencia del Poder Judicial del Estado de Tabasco, es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en el artículo 48, fracción II, de la Ley de Transparencia y Acceso a la Información del Estado de Tabasco, ya que tiene la facultad de confirmar las determinaciones que en materia de clasificación de información realicen los titulares de las áreas de este sujeto obligado, por lo tanto, se estima procedente la reserva de la información.

**II. Análisis.** Se advierte que en la solicitud de información se pide el documento de seguridad, respecto del cual, se informó que lo peticionado consiste en documento que actualiza dos de los supuestos de clasificación de la información, toda vez que del análisis efectuado por éste órgano colegiado, adquiere el carácter de reservado en los aspectos relativos a las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, con fundamento en el artículo 121, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

En ese sentido, se tiene en cuenta que en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento a partir de lo dispuesto en el artículo 6°, apartado A de la Constitución Política de los Estados Unidos Mexicanos, por el cual todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todos.





Sin embargo, el derecho de acceso a la información no puede caracterizarse como de contenido absoluto, sino que su ejercicio está acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello. Así, precisamente se obtiene que la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

En desarrollo de ese extremo de excepcionalidad, el artículo 113 de la Ley General de Transparencia y 121 de la Ley de Transparencia de la entidad, establecen un catálogo genérico de supuestos bajo los cuales debe reservarse la información, lo cual procederá cuando su otorgamiento o publicación encuadre en alguna de las fracciones contenidas en dichos preceptos jurídicos.

Junto a la identificación de esos supuestos y con el ánimo de proyectar a cabalidad el principio constitucional que les da sentido, la Ley General en sus artículos 103, 104, 108 y 114 exige que en la definición sobre su configuración, además de la realización de un examen casuístico y de justificación fundado y motivado, se desarrolle la aplicación de un prueba de daño, entendido esto como el estándar que implica ponderar la divulgación de la información frente a la actualización de un daño.

Ahora, en cuanto a la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, se establece lo siguiente:

**Artículo 121.** *Para los efectos de esta Ley, se considera información reservada la expresamente clasificada por el Comité de Transparencia de cada uno de los Sujetos Obligados, de conformidad con los criterios establecidos en la Ley General y en la presente Ley. La clasificación de la información procede cuando su publicación:*

*I. Comprometa la seguridad del Estado, la seguridad pública y cuente con un propósito genuino y un efecto demostrable;*

A su vez, los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas prevé:

*"Décimo octavo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al*





*poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público.*

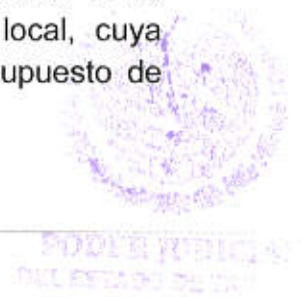
*Se pone en peligro el orden público cuando la difusión de la información pueda entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública, menoscabar o dificultar las estrategias contra la evasión de reos; o menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales.*

*Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.*

Por lo anterior, se advierte que en el caso que nos ocupa se cumple con los requisitos para que proceda la clasificación de la información solicitada en términos de lo dispuesto en el artículo 121, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco; y el Décimo Octavo de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Siguiendo ese criterio, este órgano de Transparencia, estima configurado el supuesto de reserva aludido, en tanto que sí pesa una reserva en la divulgación de las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros y en esa medida confirmar la clasificación de reserva de lo solicitado.

**III. Análisis específico de la prueba de daño.** Este Comité estima que la clasificación antes advertida también se confirma desde la especificidad que en aplicación de la prueba de daño mandata el artículo 112 de la Ley de Transparencia local, cuya delimitación, necesariamente debe responder a la propia dimensión del supuesto de reserva con el que se relacione su valoración.







Lo anterior, porque las leyes en materia de transparencia antes mencionadas, identifican un catálogo de hipótesis a partir de las cuales deberá entenderse reservada cierta información, cuya esencia, más allá de su ámbito genérico de protección, se construye a partir de elementos y objetivos diametralmente distintos, lo que por ende, incide en la valoración de la prueba de daño que sobre cada uno pueda prevalecer.

Es por ello que se procede a lo siguiente:

**Información que se reserva:** Todos los archivos físicos y electrónicos relativo a lo siguiente: *“...las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros, contenidos en el documento de seguridad...”*.

**Plazo de Reserva:** 5 años.

**Autoridades y servidores públicos responsables para su resguardo:** Gloria Guadalupe Ascencio Lastra, Oficial Mayor; Gustavo Gómez Aguilar, Tesorero Judicial; Rodolfo Gabriel Cuenca Ruiz y Segundo Vocal, Director de Contraloría todos del Poder Judicial del Estado de Tabasco.

**Parte o partes de los documentos que se reservan:** Se reservan las secciones que contienen los siguientes datos: las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros.

**Fuente y archivo donde radica la información:** Archivos físicos y electrónicos de la Oficialía Mayor, Tesorería Judicial y Dirección de Contraloría del Poder Judicial del Estado de Tabasco.







En razón de lo anterior, se acreditan los supuestos contenidos en los artículos 108 y 112 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, esto es:

**Artículo 108.** *La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder, actualiza uno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente título.*

- *Lo que aconteció con el señalamiento de que la información requerida se encuentra relacionada directamente con lo establecido en el artículo 121 fracción I de la Ley de la materia.*

**Artículo 112.** *En la aplicación de la Prueba del Daño, el sujeto obligado deberá justificar lo siguiente:*

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

El dar a conocer la integridad del Documento de Seguridad vulneraría las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales que resguarda este sujeto obligado, para llevar a cabo las funciones propias de este Tribunal y que se recaban de los interesados en recibir algún servicio.

- II. *El riesgo de perjuicio que suponía la divulgación supera el interés público de que se difunda,*

Se generaría un riesgo real ya que se daría a conocer el proceso de análisis de riesgos que considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. De igual manera 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 que en conjunto determinan el riesgo latente de los datos personales.





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

Los riesgos y daños que pudieran causar la difusión de la información referida, son superiores al derecho de acceso a la información, pues además de los daños presentes y específicos, su divulgación ocasionaría vulnerabilidades de seguridad, que resultaría en una afectación más grave al interés general, pues se está ante un límite al principio de máxima publicidad.

En conclusión, este Comité puede afirmar que la divulgación de la información que se clasifica en este documento, podría vulnerar las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros, por lo que la divulgación de la misma sería irresponsable e impropio, por lo cual se procede a tomar el siguiente:

**ACUERDO CT/074/2019**

Del estudio y análisis del presente asunto, el Comité de Transparencia de este Poder Judicial, por unanimidad de votos, **CONFIRMA** la reserva del documento de seguridad en las secciones que contienen las medidas de seguridad y ubicación de las bitácoras de acceso y operación cotidiana, de vulneraciones de seguridad, electrónicas y físicas, el análisis de riesgo de los datos en posesión de ésta institución, las condiciones de dichos datos, las medidas de seguridad faltantes, la seguridad de los datos personales, las características de los resguardos donde se encuentran los datos personales, entre otros, con fundamento en el artículo 121 fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

La información que se clasifica como reservada tendrá esa condición por un plazo de cinco años; clasificación que empieza a contar a partir de la fecha de suscripción del Acuerdo de Reserva, lo anterior, con fundamento en el artículo 109 fracción I. Asimismo se deja constancia de que los responsables de la custodia de la información que se reserva son la Oficial Mayor, el Tesorero Judicial y el Director de Contraloría del Poder Judicial del Estado de Tabasco, mismos que harán la petición para desclasificar la





información, una vez que se haya extinguido la causal de reserva o fenezca el plazo de la misma.

Elabórese el Acuerdo de Reserva y publíquese en el portal de Transparencia de este Sujeto Obligado a fin de dar cumplimiento al artículo 76 fracción XLVIII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco e inclúyase al índice de acuerdos de reserva correspondiente y notifíquese al solicitante.

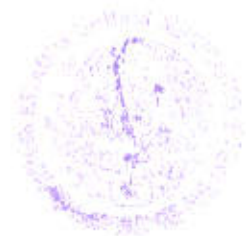
Por lo anterior, es menester generar la versión pública del documento de seguridad, suprimiendo las secciones que han sido clasificadas como reservadas en la presente sesión, permitiendo así a los ciudadanos y a cualquier otro interesado, acceder al contenido de dicho documento en cada una de sus partes, protegiendo y salvaguardando la información que no es susceptible de darse a conocer.

**CUARTO.** Finalmente, la Presidenta del Comité, manifiesta que no habiendo otro asunto que tratar, se declara clausurada la sesión siendo las trece horas con cincuenta minutos del diez de mayo del año dos mil diecinueve, redactándose la presente acta, misma que, previa lectura, fue firmada y aprobada por los presentes.

**PROTESTAMOS LO NECESARIO**

  
**Arq. Gloria Guadalupe Ascencio Lastra**  
**Oficial Mayor y Presidente**

  
**Lic. Gustavo Gómez Aguilar**  
**Tesorero Judicial y Primer Vocal**




PODER JUDICIAL  
DEL ESTADO DE TABASCO

## COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013 y 4082  
Independencia esq. Nicolás Bravo s/n  
Col. Centro. C. P. 86000. Villahermosa. Tab.

  
**L.C.P. Rodolfo Gabriel Cuenca Ruiz**  
**Director de Contraloría y Segundo Vocal**



Esta hoja de firmas forma parte del Acta de la Vigésima Sexta Sesión Ordinaria del Comité de Transparencia del Poder Judicial del Estado de Tabasco, de fecha veintidós de mayo de dos mil diecinueve.





# **DOCUMENTO DE SEGURIDAD**





## Glosario

DNS	Un Servidor DNS en informática responde a las siglas Domain Name System. Derivado de los servidores DNS se conocen los nombres en las redes, como las de Internet o las de una red privada.
DMZ	En seguridad informática, una zona desmilitarizada (conocida también como <i>DMZ</i> , sigla en inglés de <i>demilitarized zone</i> ) o red perimetral es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una <i>DMZ</i> es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que <i>en general</i> las conexiones desde la <i>DMZ</i> solo se permitan a la red externa -- los equipos ( <i>hosts</i> ) en la <i>DMZ</i> no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.
LAN	Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
N/A	No aplica

## Medidas de Seguridad Implementadas

### 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 Institucional*

Eliminado: Información Reservada Artículo 121 fracción I Ley de Transparencia y acceso a la información del Estado de Tabasco (LTAIET). Medidas de Seguridad físicas. Su publicación pondría en riesgo a este Poder Judicial pues reflejaría las posibles vulnerabilidades.

#### *Entorno de los datos*

- ✓ No se sitúan equipos en sitios altos para evitar caídas,
- ✓ No se colocan elementos móviles sobre los equipos para evitar que caigan sobre ellos,
- ✓ Se separan los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen,
- ✓ Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

## Controles de Identificación y Autenticación de Usuarios

#### *Identificación*

Eliminado: Información Reservada Artículo 121 fracción I de la Ley de Transparencia y acceso a la información del estado de Tabasco. Controles de identificación y autenticación. Su publicación pondría en riesgo a este Poder Judicial pues reflejaría las posibles vulnerabilidades.

## Procedimientos de respaldo y recuperación de datos personales

#### *Respaldo*

Se realiza una digitalización completa de la información que ingresa a través de la oficialía de partes y se almacena en discos duros. A partir de la aprobación del presente documento deberá realizarse un respaldo incremental almacenado en discos duros.



Una operación de respaldo incremental sólo copia los datos que han variado desde la última operación de respaldo de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último respaldo. Se puede adquirir una aplicación de respaldo que identifica y registra la fecha y hora de realización de las operaciones de respaldo para identificar los archivos modificados desde esas operaciones.

Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental, atendiendo, a las recomendaciones del área de Archivo.

### *Recuperación*

Los respaldos incrementales contienen fecha y hora, tanto inicial como final.

La recuperación se realiza cruzando la fecha del incidente y el último respaldo.

## **Controles y mecanismos de seguridad para las transferencias**

### *Transmisiones mediante el traslado de soportes físicos*

- a) El envío se realiza a través de los actuarios y ordenanzas adscritos a los Juzgados y Ponencias, o mediante personal autorizado por su superior jerárquico y con oficio;
- b) Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas;
- c) La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial.
- d) Toda entrega de información requiere acuse de recibo, y
- e) A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.

### *Transmisiones mediante el traslado físico de soportes electrónicos*

- a) El envío se realiza a través de los actuarios y ordenanzas adscritos a los Juzgados y Ponencias, o mediante personal autorizado por su superior jerárquico y con oficio;
- b) Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas;
- c) La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial.
- d) Toda entrega de información requiere acuse de recibo, y
- e) A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.





f) A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar cifrados.

#### *Transmisiones mediante el traslado sobre redes electrónicas*

a) A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán ser sometidos a un proceso a través del cual la información puede ser codificada para no ser accedida por otros, a menos que tengan la clave del cifrado.

#### *Transferencias*

- ☒ Interinstitucionales
- ☐ Internacionales
- ☒ Con entes privados

#### *Tipo de Traslado*

- ☒ De soportes físicos
- ☒ Físico de soportes electrónicos
- ☒ Sobre redes electrónicas

### ***Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales***

#### *Bitácoras de Acceso*

1. Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información:

- ✓ Nombre y cargo de quien accede
- ✓ Identificación del Expediente
- ✓ Fojas del Expediente
- ✓ Propósito del Acceso
- ✓ Fecha de Acceso
- ✓ Hora de Acceso
- ✓ Fecha de Devolución
- ✓ Hora de Devolución

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de Seguridad y ubicación de las bitácoras. Su publicación pondría en riesgo a la institución pues indicaría la ubicación de las bitácoras y su posible alteración.



## *Vulneraciones a la Seguridad de los Datos*

La bitácora de vulneraciones contiene la siguiente información:

1. Nombre de quien reporta el incidente
2. Cargo
3. La fecha en la que ocurrió;
4. El motivo de la vulneración de seguridad; y
5. Las acciones correctivas implementadas de forma inmediata y definitiva.

## **Técnicas de Supresión y Borrado Seguro de Datos Personales**

### *Métodos Físicos*

1. Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir.
2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

### *Métodos Lógicos*

Sobre-escritura: Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

## **Análisis de riesgos**

Eliminado. Información Reservada Artículo 121 fracción I LTAIET. Análisis de riesgo de los datos en posesión del Poder Judicial, toda vez que puede poner en riesgo a los datos personales por la divulgación del mismo.

## **Identificación de Medidas de Seguridad**

### *Medidas de Seguridad Administrativas*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Condiciones de los datos en posesión del Poder Judicial, puede poner en riesgo a los datos personales por la divulgación del mismo.

### *Medidas de Seguridad Físicas*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de seguridad para protección de los datos en posesión del Poder Judicial, puede poner en riesgo a los datos personales por la divulgación del mismo.



## *Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad.*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de seguridad para protección de los datos en posesión del Poder Judicial, puede poner en riesgo a los datos personales por la divulgación del mismo.

### **Análisis de brecha**

#### *Medidas de Seguridad faltantes por implementar*

#### *-Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de seguridad faltantes. Su publicación pondría en riesgo al Poder Judicial pues reflejaría las posibles vulnerabilidades.

#### *-Medidas de Seguridad Avanzadas para Accesos desde Red Interna*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de seguridad faltantes. Su publicación pondría en riesgo al Poder Judicial pues reflejaría las posibles vulnerabilidades.

#### *-Medidas de Seguridad Administrativas*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de seguridad faltantes. Su publicación pondría en riesgo al Poder Judicial pues reflejaría las posibles vulnerabilidades.

#### *-Medidas de Seguridad Física*

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Medidas de seguridad faltantes. Su publicación pondría en riesgo al Poder Judicial pues reflejaría las posibles vulnerabilidades.

### **Gestión de vulneraciones**

#### *Plan de respuesta*

- 1) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
- 2) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- 3) Llenado de Formato A (anexo 1), por parte de la persona que detectó la vulneración.
- 4) Llenado de Formato B (anexo 2), por parte de la Coordinación de Planeación.



- 5) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- 6) Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Coordinación de Planeación.
- 7) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.
- 8) Llenado de la bitácora de vulneraciones conforme al artículo 44 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.

### **Mecanismos de monitoreo y revisión de las medidas de seguridad**

Primer monitoreo y evaluación de los sistemas de seguridad durante acorde a las necesidades presentadas por las unidades administrativas.

### **Plan de trabajo**

Duración veinticuatro meses

Se ha planteado implementar la totalidad de las medidas de seguridad faltantes en un periodo de veinticuatro meses a partir de la aprobación del presente documento de seguridad.

En este 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 institución y el presupuesto lo permita.

Control	Parámetro
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.



# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Actividad	Áreas Involucradas
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Dirección Jurídica y Oficialía Mayor
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Coordinación de Planeación
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la institución y entidades externas.	Dirección Jurídica, Oficialía Mayor.
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Coordinación de Planeación
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Coordinación de Planeación.
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Coordinación de Planeación.

# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Actividad	Áreas Involucradas
Eliminación de los derechos de acceso: Los derechos de acceso de todos los servidores públicos, 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 requiera hacer un ajuste.	Coordinación de Planeación
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Coordinación de Planeación
Elaboración del Plan de Contingencia	Todas las Áreas

## Programa General de Capacitación

La capacitación del personal está dividida en cuatro áreas de responsabilidad con las mismas temáticas:

NIVELES DE	TEMATICA
Unidad de Transparencia	Generalidades de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados
Coordinadores Generales y Directores de Área	
Coordinadores	
Personal que trata datos personales.	Principios y Deberes
	Sistema de Gestión, Medidas de seguridad y acciones preventivas.



## **Catálogo de Sistemas de Tratamiento de Datos Personales**

### **Control de Ingreso**

#### *Sistema de Tratamiento de Control de Ingreso*

Cargo	Secretaria
Área	Oficialía Mayor
Funciones	<p>I. Recibir, controlar y almacenar la correspondencia interna propia de la Oficialía.</p> <p>II. Apoyar a la Oficialía en el seguimiento de las actividades que le corresponden.</p> <p>III. Articular y almacenar el archivo de la propia Oficialía.</p> <p>IV. Atender llamadas telefónicas, así como apoyar con la recepción y remisión de información electrónica vía correo electrónico a otras áreas de la institución.</p> <p>V. Recibir y clasificar el archivo de trámite del área, para su debido registro y control.</p> <p>VI. Atender las necesidades del personal adscrito a la Coordinación de Planeación.</p> <p>VII. Realizar el envío de la correspondencia.</p> <p>VIII. Elaborar oficios que se requieran en el área.</p> <p>IX. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la materia.</p>

### **Recepción de Documentos en Oficialía de Partes**

#### *Sistema de Tratamiento de Recepción de Documentos en oficialía de partes*

Cargo	Oficial de Partes
Área	Oficialía de Partes
Funciones	<p>Recepcionar la correspondencia que se turna a las áreas del Poder Judicial.</p> <p>Supervisar que los documentos estén en buen estado y sean dirigidos al área que corresponda.</p> <p>Verificar la captura de los datos y se hagan las anotaciones en libreta de datos de las partes involucradas por Sala, Amparo, así como los exhortos civiles y penales.</p>



## Pagos al personal

### *Sistema de Tratamiento de los Pagos al Personal*

Cargo	Jefe del Departamento de Recursos Humanos
Área	Recursos Humanos
Funciones	Mantener actualizados los expedientes del personal. Ingresar nombramientos, licencias, permisos y justificantes al sistema del personal. Revisar diariamente listas y tarjetas de asistencias del personal, de todas las unidades del Poder Judicial. Ingresar listados de guardias al Sistema de Personal. Enviar los vencimientos de nombramientos del personal a cada uno de los Plenos. Mantener actualizada la plantilla del personal y de meritorios Proporcionar copias de nombramientos del personal a las diversas áreas que lo requieran (ISSET, Contraloría y Tesorería)
<b><i>Personal autorizado para tratamiento</i></b>	
Cargo	Coordinador de Recursos Financieros
Área	Tesorería Judicial
Funciones	Realizar el pago a proveedores e imprimir las pólizas de egresos Recibir órdenes de pagos para realizar las transferencias electrónicas Entregar pólizas de egresos y de cheques Enviar recursos a los juzgados foráneos, para pagos según expedientes Entregar pólizas de cheque de envío de recursos a los juzgados foráneos a la Coordinación de Consignaciones y Pagos.
Cargo	Director Jurídico
Área	Dirección Jurídica
Funciones	Coordinar y elaborar previa solicitud de la Oficialía Mayor, los contratos y adendums de arrendamiento, donación, prestación de servicios, compraventa y comodato; así como los convenios que, en general, le sean encomendados y sean de su competencia. Mantener actualizado el padrón de contratos y convenios del verificando vigencias y términos. Emitir los criterios normativos para la celebración de los contratos y convenios vigilando y verificando que el clausulado de éstos, no sea lesivo para los intereses de la institución.



# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

	Proporcionar asesoría jurídica en el ámbito de su competencia, en materia de instrumentos jurídicos que le soliciten las diversas áreas. Mantener actualizado el padrón de contratos y convenios del verificando vigencias y términos. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la material.
<b>Tipo de datos personales pertenecientes al sistema de tratamiento de los pagos a empleados</b>	
Datos	Nombre, domicilio, correo electrónico, firma, teléfono institucional y personal, fotografía, CURP, RFC, fecha de nacimiento, INE, datos biométricos, datos de salud, nombres de familiares, actas de defunción, acta de nacimiento, datos académicos y datos laborales.
Controles de seguridad	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Seguridad de los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Tipo de Soporte	Soporte físico y electrónico.
Características del lugar de resguardo	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Programas en que se utilizan los D.P.	Microsoft Office e Intranet.
<b>Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales</b>	
Físicos	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Electrónicos	
<b>Las bitácoras de acceso y operación cotidiana</b>	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.	

# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Bitácoras Físicas	Identificación y/o lugar de almacenamiento	
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.		
Las bitácoras de vulneraciones de seguridad		
ID	Soporte	Responsable
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.		

## Padrón de Proveedores

### Sistema de Tratamiento de Padrón de Proveedores

Cargo	Jefe del Departamento de Compras
Área	Oficialía Mayor
Funciones	Apoyar en la recepción de solicitudes de bienes muebles Ayudar en la celebración de procesos licitatorios Resguardar las solicitudes de garantía de bienes Elaborar registros de proveedores en el padrón Auxiliar en la elaboración de solicitudes de cotización Elaborar cuadros comparativos
<b>Personal autorizado para tratamiento</b>	
Cargo	Coordinador de Recursos Financieros
Área	Tesorería Judicial
Funciones	Realizar el pago a proveedores e imprimir las pólizas de egresos. Recibir órdenes de pagos para realizar las transferencias electrónicas. Entregar pólizas de egresos y de cheques. Enviar recursos a los juzgados foráneos, para pagos según expedients. Entregar pólizas de cheque de envío de recursos a los juzgados foráneos a la Coordinación de Consignaciones y Pagos.
Cargo	Coordinador de Control Presupuestal
Área	Tesorería Judicial
Funciones	Diseñar y presentar propuesta anual del presupuesto general de egresos del Poder Judicial. Elaborar órdenes de pago mensuales para la ministración de los recursos.



# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

	Control y ejercicio de los recursos del Fondo Auxiliar y de los recursos federales autorizados, informar de los asuntos conciliados efectuados, así como las sentencias revisadas Elaborar los libros financieros e integrar la cuenta pública.
--	--

## *Tipo de datos personales pertenecientes al Sistema de Padrón de Proveedores*

Datos	Nombre / Domicilio/ Número de teléfono / Firma/ RFC/ Correo electrónico/ Acta constitutiva / poder notarial/ Credencial para votar/ Datos Bancarios.
Controles de seguridad	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Seguridad de los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Tipo de Soporte	Soporte físico y electrónico
Características del lugar de resguardo	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Programas en que se utilizan los Datos Personales	Microsoft Office e Intranet.

## **Auditorías de Órgano Interno de Control**

### *Sistema de Tratamiento de Auditorías de Órgano de Control*

Cargo	Director de Contraloría Judicial
Área	Contraloría Judicial
Funciones	Vigilar el cumplimiento de las normas de control interno establecidas por el Pleno del Tribunal y del Consejo de la Judicatura. Diseñar las políticas, planes de trabajo, sistemas y acciones, para el logro de su objetivo institucional de fiscalización y evaluación; Acatar y verificar su cumplimiento de las normas que expida el Consejo de la Judicatura y regulen el funcionamiento de los instrumentos y procedimientos de control administrativo del Poder Judicial;



	<p>Practicar auditorías a juzgados y unidades administrativas, informando al Pleno del Consejo el resultado de las mismas;</p> <p>Dar seguimiento a las observaciones y recomendaciones que deriven de las visitas practicadas por las áreas internas y auditorías externas;</p> <p>Emitir en los términos de las leyes y disposiciones administrativas aplicables, para su aprobación por el Consejo de la Judicatura, las normas, políticas y lineamientos que las áreas correspondientes hayan de observar en las adquisiciones, enajenaciones y baja de bienes muebles; arrendamientos, contratación de servicios y, en su caso, obras públicas del Poder Judicial;</p> <p>Establecer con base en la ley de la materia, para su aprobación por el Consejo de la Judicatura, las normas en materia de registro contable, control presupuestal y supervisar su cumplimiento;</p> <p>Evaluar el funcionamiento de los juzgados y demás áreas, en el ámbito administrativo, formulando las recomendaciones que estime conducentes al logro de las metas institucionales y de una mayor eficiencia administrativa;</p> <p>Recibir, registrar y requerir las declaraciones patrimoniales y sus modificaciones que presenten los servidores públicos del Poder Judicial, comprobando la exactitud y veracidad de ellas y comunicar al Presidente del Consejo las irregularidades que en su caso se detecten;</p> <p>Proponer a la consideración del Consejo de la Judicatura las estructuras orgánicas y ocupacionales de las áreas, así como registrar dichas estructuras a través de la expedición de manuales administrativos;</p> <p>Evaluar, proponer e instrumentar los mecanismos necesarios en la gestión pública para el desarrollo administrativo integral de las áreas, a fin de que los recursos humanos y materiales y los procedimientos técnicos de las mismas sean aprovechados y aplicados con criterios de eficacia y simplificación administrativa;</p> <p>Organizar y realizar los actos de entrega-recepción que se lleven a efecto en las Salas, los Juzgados y demás áreas del Poder Judicial, conforme la normatividad aplicable;</p> <p>Proponer para su aprobación por el Consejo de la Judicatura las normas, procedimientos y medidas de control aplicables al manejo de efectivo en los juzgados y vigilar su estricto cumplimiento;</p>
--	--



	<p>Analizar, diseñar y controlar las formas impresas de uso interno, procurando su adecuación a los sistemas y procedimientos establecidos;</p> <p>Homologar sus sistemas de verificación contable presupuestal con los existentes en el Órgano Superior de Fiscalización del Estado;</p> <p>Formar un expediente de la diligencia o auditoría que se practique, el cual deberá incluir los papeles de trabajo y documentación correspondiente.</p> <p>Mantener en sus diligencias y procedimientos la más absoluta reserva y abstenerse de comunicar a los interesados o a terceros el resultado de sus indagaciones.</p> <p>Auxiliar al Pleno del Tribunal Superior de Justicia y al Consejo de la Judicatura, en la coordinación para vigilar que la administración del presupuesto del Poder Judicial sea eficaz, honesta y ajustada a la normatividad aplicable, ejecutando las acciones operativas que se instruyan y las procedentes para tal efecto, informando el resultado a aquéllos para los efectos legales a que hubiere lugar;</p> <p>Vigilar, a través de la unidad de supervisión de obra, la debida ejecución de los programas que en la materia correspondan;</p> <p>Conocer, iniciar, tramitar los procedimientos que correspondan a personal administrativo;</p> <p>Resolver en la esfera de su competencia, los procedimientos administrativos que conozca;</p> <p>Imponer sanciones y aplicar medidas de apremio en la esfera de su competencia;</p> <p>Comunicar el inicio de los procedimientos al Pleno respectivo;</p> <p>Llevar los libros de gobierno para el registro de los procedimientos que tramite, con independencia del libro de inhabilitados;</p> <p>Revisar, elaborar y suscribir, en su caso, las cédulas de solventaciones y demás documentación que, en términos de la normatividad aplicable, deba remitirse al Órgano Superior de Fiscalización del Estado; y,</p> <p>Las demás que determinen las leyes, los reglamentos, acuerdos generales correspondientes y las que directamente le encomiende el Presidente.</p>
<b>Tipo de datos personales pertenecientes al sistema de auditorías</b>	
Datos	Nombre/Domicilio, Correo electrónico/Firma/Teléfono/INE



# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Controles de seguridad	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Seguridad de los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Tipo de Soporte	Soporte físico y electrónico
Características del lugar de resguardo	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Programas en que se utilizan los D.P.	Microsoft Office e Intranet.

## Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales

Físicos	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Electrónicos	

## Las bitácoras de acceso y operación cotidiana

Bitácoras Físicas	Identificación y/o lugar de almacenamiento
-------------------	--

Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.

## Las bitácoras de vulneraciones de seguridad

ID	Soporte	Responsable
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.		

## Declaraciones de Situación Patrimonial

### Sistema de Tratamiento de Declaraciones de Situación Patrimonial

Cargo	Director de Contraloría Judicial
Área	Contraloría Judicial
Funciones	Las señaladas en el artículo 164 de la Ley Orgánica del Poder Judicial del Estado de Tabasco.



Tipo de datos personales pertenecientes al sistema de declaraciones de situación patrimonial		
Datos	Nombre/ Domicilio/ Correo electrónico/ Firma/ teléfono personal/ fotografía/ bienes muebles / bienes inmuebles / estados bancarios / préstamos / inversiones /	
Controles de seguridad	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Seguridad de los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.	
Tipo de Soporte	Soporte físico y electrónico	
Características del lugar de resguardo	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.	
Programas en que se utilizan los D.P.	Microsoft Office e Intranet.	
Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales		
Físicos	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.	
Electrónicos		
Las bitácoras de acceso y operación cotidiana		
Bitácoras Físicas	Identificación y/o lugar de almacenamiento	
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.		
Las bitácoras de vulneraciones de seguridad		
ID	Soporte	Responsable
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.		



## Procedimientos de Responsabilidad del Órgano Interno de Control

*Sistema de Tratamiento de Procedimientos de Responsabilidad del Órgano Interno de Control*

Cargo	Director de Contraloría Judicial
Área	Contraloría Judicial
Funciones	Las señaladas en el artículo 164 de la Ley Orgánica del Poder Judicial del Estado de Tabasco.
<b>Tipo de datos personales pertenecientes al sistema</b>	
Datos	Nombre / Domicilio/ Correo electrónico/ Firma / CURP/INE.
Controles de seguridad	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Seguridad de los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Tipo de Soporte	Soporte físico y electrónico
Características del lugar de resguardo	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Programas en que se utilizan los D.P.	Microsoft Office e Intranet.
<b>Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales</b>	
Físicos	Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Características de los resguardos donde se encuentran los datos personales. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Electrónicos	
<b>Las bitácoras de acceso y operación cotidiana</b>	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.	



# COMITÉ DE TRANSPARENCIA



Tel. (993) 3 58 20 00 ext. 4013  
Independencia esq. Nicolás Bravo s/n  
Col. Centro, C. P. 86000, Villahermosa, Tab.

Las bitácoras de vulneraciones de seguridad		
ID	Soporte	Responsable
Eliminado: Información Reservada Artículo 121 fracción I LTAIET. Nombre de la bitácora. Podría encontrarse dicha bitácora y alterarse.		

## Anexo 1 Formato A

Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA	
FECHA DEL INCIDENTE		
NOMBRE		
CARGO		
AREA		
RESPONSABLE DEL ÁREA		
CAUSA DE LA VULNERACIÓN		
SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATO(S) VULNERAD(O)		
CANTIDAD DE TITULARES		
SOPORTE DE LA INFORMACIÓN VULNERADA	<input type="checkbox"/> Físico <input type="checkbox"/> Electrónico <input type="checkbox"/> Mixto	
SELECCIONE EL TIPO DE VULNERACIÓN	<input type="checkbox"/> Pérdida o destrucción no autorizada <input type="checkbox"/> Robo, extravío o copia no autorizada <input type="checkbox"/> Uso, acceso o tratamiento no autorizado <input type="checkbox"/> Daño, alteración o modificación no autorizada	
TIPO DE DATOS PERSONALES COMPROMETIDOS	<input type="checkbox"/> Identificativos <input type="checkbox"/> Laborales <input type="checkbox"/> Tránsito y Movimientos Migratorios <input type="checkbox"/> Académicos <input type="checkbox"/> Procedimientos Administrativos o Judiciales <input type="checkbox"/> Patrimoniale <input type="checkbox"/> Salud <input type="checkbox"/> Ideológicos De origen      Características Personales <input type="checkbox"/> Vida Sexual	
Nombre y firma de quién reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del área



## Anexo 2 Formato B

### Vulneraciones a los Sistemas de Información y Bases de Datos

<b>CONTENIDO DE LA BITACORA</b>	<b>COMPLETE EL CONTENIDO DE LA BITACORA</b>
<b>FECHA DEL INCIDENTE</b>	
<b>NOMBRE DEL RESPONSABLE DE LA INVESTIGACIÓN</b>	
<b>CARGO</b>	
<b>AREA</b>	
<b>NÚMERO DE INVESTIGACIÓN</b>	
<b>LA INFORMACIÓN VULNERADA ESTA REGISTRADA EN EL DOCUMENTO DE SEGURIDAD</b>	<input type="checkbox"/> Sí <input type="checkbox"/> No
<b>EN CASO DE QUE LA INFORMACIÓN NO ESTUVIERA VULNERADA, SOLICITE AL RESPONSABLE DEL ÁREA UN INFORME AL RESPECTO CON EL OBJETO DE RESPONDER EL CONTENIDO DEL APARTADO A.</b>	
<b>APARTADO A</b>	
<b>FECHA EN QUE SE CREO EL SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADA</b>	
<b>FUNDAMENTO LEGAL PARA OBTENCIÓN DE LOS DATOS PERSONALES.</b>	
<b>RESGUARDO DE LOS SOPORTES USUARIOS</b>	
<b>MEDIDAS DE SEGURIDAD FISICAS TÉCNICAS Y ADMINISTRATIVAS APLICADAS</b>	
<b>LAS CAUSAS ENUNCIADAS EN EL FORMATO A</b>	
<b>LO QUE EL TITULAR DEL ÁREA CONSIDERE PERTINENTE</b>	
<b>APARTADO B</b>	
<b>ADMINISTRADOR DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)</b>	
<b>USUARIOS DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)</b>	
<b>LOS HECHOS DE MODO TIEMPO Y LUGAR ENUNCIADOS EN EL FORMATO A</b>	
<b>RESGUARDANTE SOPORTE FÍSICO O ELECTRÓNICO VULNERADO</b>	





## **Anexo 4 Plan de contingencia**

### **Plan de Contingencia para la protección de la información**

#### **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 eléctricas, fallas con la conexión de internet y que pueden ser resueltas por el mismo personal.
- ✓ **Grado 2:** requiere tanto el apoyo del personal de la institución, así como agentes externos.
- ✓ **Grado 3:** Son contingencias que por su alcance pueden afectar severamente la operatividad y se requiere además del apoyo externo.

#### **Consideraciones Principales**

- ✓ Se debe realizar una evaluación de los riesgos.
- ✓ Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- ✓ Se designe a un encargado de cada área para que apoye en cualquier desastre que ocurra y genere la contingencia, capacitándolos para el manejo de las mismas, como el uso de extintores, planes de evacuación etc.
- ✓ Es necesario hacer las pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).
- ✓ Reunión con las comisiones o brigadas de las áreas de la Municipalidad
  - (capacitación y evaluaciones)
- ✓ Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.
- ✓ Difusión del documento del plan de contingencia una vez aprobado.

## Lugar alternativo de trabajo

En caso de algún desastre mayor (terremoto o incendio) que implique pérdidas estructurales se plantea en algunos casos la posibilidad de contar con algún lugar alternativo de trabajo los sitios alternos de trabajo pueden ser: propios de la institución, de una entidad con la que hay acuerdo o reciprocidad, instalaciones alquiladas (se debe contar con presupuesto).

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

- Mesas para monitores y teclados de los servidores principales
- Sillas
- Switches
- Router para la conexión a internet
- UPS
- Teléfono
- Extinguidor
- Material y equipo de Oficina

## Medidas preventivas ante siniestros

### **Medidas de prevención y conservación de los archivos:**

- ✓ El archivo general debe situarse en el primer piso del edificio (no sótanos).
- ✓ Espacios con luz natural y sin humedad.
- ✓ Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
- ✓ Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- ✓ Los estantes de los archivos deben de estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez la acumulación de humedad y proliferación de plagas)
- ✓ Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- ✓ Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

## ***Incendios***

### **Medidas preventivas en caso de Incendios**

- ☐ Se recomienda tener un conocimiento básico de primeros auxilios.
- ☐ Para la pronta detección de un incendio se puede contar con detectores de humo.
- ☐ En caso de incendio no abrir puertas y ventanas, el aire es factor para propagación del fuego.
- ☐ Si se tienen almacenadas sustancias inflamables como gasolina, acetona, aguarrás, alcohol o thinner, se sugiere colocarlos en lugares ventilados y lejos de las flamas, fuentes de calor y aparatos eléctricos (si no los necesita, deséchelos preferentemente)
- ☐ Si el incendio es pequeño, se procurará apagarlo mediante un extintor. Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.
- ☐ No sobrecargar los contactos eléctricos, desconectando los que no se utilicen.

### **Sobre el resguardo de la información en caso de incendio:**

- ☐ Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, Disco duro, USB, bases de datos).
- ☐ Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en un repositorio).

### **Durante un incendio:**

- ☐ Ubicar los extintores cerciórese de saber usarlos y que estos sean utilizables.
- ☐ Si detecta un incendio procure mantener la calma y repórtelo inmediatamente o presione alguna señal de alarma.
- ☐ No abra puertas ni ventanas el fuego se extiende con el aire.
- ☐ Si es un incendio que no puede controlar usted mismo llame a los bomberos.
- ☐ No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible.
- ☐ Si hay gas o humo humedezca un trapo y cubra su nariz y boca.



- ▢ Si existe una puerta que deba atravesar toque con precaución la perilla; si está caliente no la abra.
- ▢ Si su ropa se enciende; tírese al piso y ruede lentamente.

## **Después del Incendio:**

Un técnico debe de revisar las instalaciones de gas y electricidad antes de utilizarlas nuevamente.

## **Sismo**

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, sin embargo si los datos almacenados se encuentran en discos duros, cd, USB, al contar con un respaldo de información incluso en un repositorio se tiene un respaldo inmediato, que permitiría recuperar la información si los otros respaldos físicos se dañaran, para inmediatamente apenas se tenga una conexión a internet y una computadora tener acceso a dichos respaldos.

## **Medidas preventivas en caso de sismo**

- ✓ No colocar muebles, equipos o cajas que bloqueen las rutas y salidas de emergencia del archivo.
- ✓ Contar con un teléfono celular de emergencia en caso de falla de líneas telefónicas fijas.
- ✓ Contar con un plan de evacuación y realizar simulacros de manera cotidiana.
- ✓ Tener a la mano una radio de baterías, linterna y los principales documentos personales.
- ✓ Contar con un botiquín de primeros auxilios.
- ✓ Si se tienen anaqueles, los objetos pesados se colocan al final.
- ✓ Localizar los lugares seguros en cada cuarto; bajo mesas sólidas y escritorios resistentes
- ✓ Ubicar los lugares peligrosos: como ventanas donde los vidrios pueden estrellarse, libreros o muebles que podrían caerse en caso de sismo.

## **Durante un Sismo**

- ▢ Mantener la calma y ubicar en una zona de segura.
- ▢ Pararse bajo un marco de puerta con trabe o de espaldas a un muro de carga.



- ▣ Adoptar posición fetal de cara al suelo, abrazándose usted mismo en un rincón, de ser posible protegerse la cabeza.
- ▣ Alejarse de ventanas, espejos y objetos de vidrio así como de objetos colgantes.
- ▣ Retirarse de objetos calientes, libreros, gabinetes, o muebles pesados.
- ▣ Si se está en un edificio evitar el uso de elevadores, si se está en la calle evitar los postes, arboles, ramas y balcones.
- ▣ Si es posible cerrar llaves del gas, desconecte la alimentación eléctrica y no encender fuego.

## **Después de un Sismo:**

- ▣ Si usted quedo atrapado, conserve la calma y trate de comunicarse al exterior golpeando un objeto.
- ▣ Evite pisar cables que hubieran quedado caídos o sueltos.
- ▣ Encienda la radio para mantenerse informado (posibles replicas).
- ▣ En caso de visible daño estructural del edificio debe ser evaluado por protección civil para evitar cualquier riesgo secundario.
- ▣ Se deben revisar las instalaciones eléctricas y de gas principalmente para evitar un desastre secundario.

## ***Inundaciones por lluvia***

### **Medidas preventivas en caso de inundación**

- ▣ Es importante realizar la revisión y reparación de la hermeticidad de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporada de lluvias esto para evitar goteras.
- ▣ Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso.
- ▣ Respetar, al menos, una altura de 10 a 15 cm de los archiveros.
- ▣ Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del local de archivo.
- ▣ Evacuar los documentos afectados hacia áreas ventiladas.
- ▣ Inmediatamente colocar papel secante en cada hoja de los expedientes.
- ▣ Si un documento se moja en su totalidad se puede realizar la congelación del mismo para su recuperación, debe realizarlo preferentemente un especialista (restauración).

## Durante una inundación

- ▣ Desconectar servicios de luz, gas y agua.
- ▣ Mantenerse alejados de árboles y postes de luz.
- ▣ Evitar tocar o pisar cables eléctricos.
- ▣ Cubrir con bolsas de plástico aparatos u objetos que puedan dañarse con el agua.

## Después de la inundación

- ▣ Se puede expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si hay suministro eléctrico garantizado en caso de emergencia, y si no hubiere, mediante esponjas, baldes, recogedores, etc.

Cerciorarse de que los aparatos eléctricos estén secos antes de utilizarlos nuevamente

- ▣ Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- ▣ Ventilar las áreas afectadas después de la inundación.

Si los documentos han sufrido daños y se encuentran mojados, se debe seguir el procedimiento de congelación para recuperarlos. A continuación se describe este procedimiento para recuperar los documentos humedecidos:

1. Se introduce la obra en una bolsa de polietileno con cierre de cremallera o termosellable. Es muy importante envolver el libro en plástico y reducir el volumen de aire para evitar la formación de condensación. Para que la congelación se realice de forma correcta, se debe dejar un amplio espacio entre los libros.
2. La cámara de congelación debe alcanzar una temperatura de -20°C. En un proceso acelerado de descenso de la temperatura el tratamiento será más efectivo. La temperatura debe ser constante y el congelador no ha de formar hielo ya que se puede acumular humedad. Se recomienda que en el momento de aplicación combinada de los tratamientos de congelación y vacío para la desinfección de documentos. Se debe Depositar la obra en la cámara de congelación hasta que esta haya alcanzado dicha temperatura, para evitar la aclimatación de los organismos.



3. El tratamiento debe durar como mínimo 72 horas, dependiendo del grosor de la obra y la temperatura del congelador. No obstante, si es necesario, se puede alargar hasta un periodo de tres semanas.
4. La obra se ha de descongelar de forma paulatina sin ser extraída del envoltorio, hasta alcanzar el equilibrio con la temperatura ambiente. Una vez descongelada y alcanzado el equilibrio, el envoltorio se puede retirar.

### ***Robo***

#### **Robo Común de equipos:**

- En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias

### ***Huelga o Manifestaciones***

#### **Manifestación o huelga:**

- Si el archivo tiene cerradura, asegúrese que quede bajo llave.

### ***Amenazas informáticas***

#### **Medidas preventivas para amenazas informáticas**

Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopadoras etc., y tener contacto con proveedores de software, hardware, y medios de soporte.

- Prevención de falla de los equipos: se debe procurar dar mantenimiento preventivo por lo menos dos veces al año, y contar con proveedores en caso de que se requiera algún remplazo inmediato.
- Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores /reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la pérdida de información importante.

## **Hackeo informático:**

Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

### **Cambiar contraseñas.**

- ▢ Debe tener al menos ocho caracteres
- ▢ No debe contener información personal como nombre real, nombre de usuario o incluso el nombre del ente público.
- ▢ Debe ser muy distinta a contraseñas previas.
- ▢ No debe contener palabras completas
- ▢ Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales

Mientras se está conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada. Por lo que se debe desconectar el cable de la red lo antes posible.

### **Posteriormente:**

- ▢ Contactar al personal de soporte para que retire del aire la página.
- ▢ Evalúe los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible.

### **Mantener la misma dirección web**

Cuando la página fue atacada la dirección usualmente no se ve afectada. Lo que generalmente se pierde es la información (textos, videos, fotos, audios) que contenía. Se sugiere restaurar el sitio con la misma dirección, para que los usuarios no se confundan.

## **Anexo 5 Manual para cifrar documentos**

### **Cómo cifrar documentos en Word o Excel**

#### **Contraseña para archivo Word**

En el caso de Word, tenemos que hacer los siguientes pasos:

- Lo primero es abrir el archivo que queramos proteger.
- Una vez abierto, vamos a Archivo. Se da clic en Información y le damos a Proteger documento, Cifrar contraseña.
- Acto seguido nos pide que pongamos una clave dos veces. En cuanto aceptemos, quedará registrada.

Si llegado el momento queremos revertir la situación, hay que seguir los pasos como antes. Una vez estemos en Cifrar contraseña, simplemente tendremos que borrarla y dar clic en aceptar. Nuestro archivo de Word quedará abierto nuevamente.

También podremos hacer que nuestro documento sea sólo de lectura, restringir la edición u otorgar permisos sólo a ciertos usuarios.

#### **Contraseña para archivo Excel**

Para quienes quieran poner una contraseña a documentos de Excel, el proceso es muy similar:

- Tenemos que abrir el documento e ir a Archivo, Información.
- Una vez aquí dar clic en permisos, proteger libro y cifrar con contraseña.
- Lo mismo que con el documento Word, nos pedirá una clave por dos veces. A partir de aquí nuestro archivo estará cifrado con una contraseña.

Para revertir la situación debemos de realizar el mismo proceso. Borrar la clave que hemos puesto y pulsar en aceptar.

Fuente: <https://www.redeszone.net/2017/12/31/podemos-cifrar-documentos-word-excel>



## **Cómo cifrar un archivo**

El cifrado de archivos ayuda a proteger tus datos mediante su cifrado. Solo una persona que disponga de la clave de cifrado correcta (por ejemplo, una contraseña) puede descifrarlos.

1. Haz clic con el botón derecho en un archivo o carpeta (o mantenlo presionado) y selecciona Propiedades.
2. Selecciona el botón Opciones avanzadas y selecciona la casilla de verificación Cifrar contenido para proteger datos.
3. Selecciona Aceptar para cerrar la ventana Atributos avanzados, selecciona Aplicar y luego selecciona Aceptar.

Fuente: <https://support.microsoft.com/es-mx/help/4026312/windows-10-how-to-encrypt->