DOCUMENTO DE SEGURIDAD

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

CONTENIDO

1. INTRODUCCIÓN
2. OBJETIVO
3. MARCO JURÍDICO
4. GLOSARIO
5. INVENTARIO DE LOS DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO
6. INVENTARIO DE SISTEMAS DE DATOS PERSONALES
7. FUNCIONES Y OBLIGACIONES
8. MEDIDAS DE SEGURIDAD IMPLEMENTADAS PARA GARANTIZAR LA PROTECCIÓN DE LOS DATOS PERSONALES
    a. Medidas de Seguridad Físicas
    b. Controles de identificación y autenticación de usuarios
    c. Controles y mecanismos de seguridad para las transferencias
        i. Transmisiones mediante el traslado de soportes físicos
        ii. Transmisiones mediante el traslado físico de soportes electrónicos
        iii. Transmisiones mediante el traslado sobre redes electrónicas
        iv. Vulneraciones a la seguridad de los datos personales
    d. Técnicas de supresión y borrado de datos personales
        i. Métodos físicos
        ii. Métodos lógicos
9. ANÁLISIS DE RIESGOS
10. ANÁLISIS DE BRECHA
11. PLAN DE TRABAJO
12. MECANISMOS DE REVISIÓN Y MONITOREO DE LAS MEDIDAS DE SEGURIDAD
13. PROGRAMA GENERAL DE CAPACITACIÓN
14. PLAN DE CONTINGENCIA
15. CIERRE

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

DOCUMENTO DE SEGURIDAD PARA LOS SISTEMAS DE DATOS PERSONALES EN POSESIÓN DEL COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE TABASCO

INTRODUCCIÓN

La información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la organización; por lo que el presente documento contiene las disposiciones en materia de protección de datos personales de las unidades administrativas del Colegio de Estudio Científicos y Tecnológicos del Estado de Tabasco, que los servidores públicos deben conocer y aplicar en términos de sus funciones y de conformidad con lo establecido por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el 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 del Colegio de Estudios Científicos y Tecnológicos del Estado de Tabasco. Por lo que se tiene a bien expedir su Documento de Seguridad para la Protección de los Datos Personales que, en el ejercicio de las funciones conferidas en su normatividad vigente, recabe, obtenga o genere; lo anterior, bajo los siguientes contenidos:

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

MARCO JURÍDICO

- **CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS**

- **CONSTITUCIÓN POLÍTICA DEL ESTADO LIBRE Y SOBERANO DE TABASCO**

- **LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA**

- **LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DE TABASCO**

- **LEY GENERAL DE RESPONSABILIDADES ADMINISTRATIVAS DE LOS SERVIDORES PÚBLICOS**

- **LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE TABASCO**

- **LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS**

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

GLOSARIO

Para los efectos del presente Documento de Seguridad, se entenderá por:

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

DNS: Un Servidor DNS en informática responde a las siglas *Domain Name System*. Gracias a los servidores DNS conocemos los nombres en las redes, como las de Internet o las de una red privada;

LAN: Una red de área local o LAN (por las siglas en inglés de *Local Área Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio;

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, trata datos personales a nombre y por cuenta del responsable;

Instituto: Instituto de Transparencia para el Pueblo del Estado de Tabasco;

CECyTE: Colegio de Estudios Científicos y Tecnológicos del Estado de Tabasco;

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco;

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco;

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**;**

Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los Datos Personales;

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, y clasificación borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de Datos Personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los Datos Personales y de los recursos involucrados en su tratamiento. De manera enunciativa, más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones, físicas, áreas críticas recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y
d) Proveer a los equipos que contienen o almacenan Datos Personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

Medidas de Seguridad Técnicas: conjunto de acciones y mecanismos que se valen de la tecnología relacionado con hardware y software para proteger el entorno digital de los Datos Personales y los recursos involucrados en su tratamiento. De manera enunciativa, más no limitativa, se deben considerar las siguientes actividades:

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

a) Prevenir que el acceso a las Bases de Datos o a la información, así como los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, desarrollo y mantenimiento del software y hardware; y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de Datos Personales;

Plataforma Nacional: La Plataforma Nacional de Transparencia;

Remisión: Toda comunicación de Datos Personales realizada exclusivamente entre el responsable y Encargado, dentro o fuera del territorio mexicano;

Responsable: Los Sujetos Obligados a que se refiere la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco, que deciden y determinan los fines, medios y demás cuestiones relacionadas con determinado tratamiento de Datos Personales;

Sistema Estatal: El Sistema Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales;

Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

Supresión: La baja archivista de los Datos Personales conforme a la normatividad archivista aplicable, que resulte en la eliminación, borrado o destrucción de los Datos Personales bajo las Medidas de Seguridad previamente establecidas por el responsable;

Titular: La persona física a quien corresponden los Datos Personales;

Transferencia: Toda comunicación de Datos Personales dentro o fuera del Territorio mexicano, realizada a persona distinta del Titular, del responsable o del encargado;

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los Datos Personales, relacionadas de manera enunciativa mas no limitativa, con la obtención , uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de Datos Personales; y

Unidad de Transparencia: Instancia a la que hace referencia el Capítulo V de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

INVENTARIO DE LOS DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

En atención a la fracción I del artículo 40 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tabasco, se realizó el inventario de los datos personales y de los sistemas de tratamiento, que en el ejercicio de sus funciones recaba, obtenga o genera el CECyTE.

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.

Categorías de datos personales según su naturaleza:

a) Nivel estándar: Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona identificada o identificable, tal como: nombre, teléfono, edad, sexo, R.F.C., C.U.R.P., 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

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

aquellos 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 del Colegio de Estudios Científicos y Tecnológicos del Estado de Tabasco, 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:

IDENTIFICABLES	***CARACTERÍSTICAS FÍSICAS***
• Nombre completo • Fecha de nacimiento • Lugar de nacimiento • Domicilio • Número telefónico (móvil y/o fijo) • Número de seguridad social • Correo electrónico personal • Estado civil • Firma autógrafa • Firma electrónica • Registro Federal de Contribuyentes • Clave Única de Registro de Población • No. de cartilla militar • No. de licencia de manejo • Credencial para votar con fotografía • Pasaporte • Edad • Nombre de familiares, dependientes y beneficiarios • Fotografía	• Estatura • Complexión
BIOMÉTRICOS	***SALUD***
• Huella dactilar • Reconocimiento facial	• Certificados médicos • Licencias médicas • Constancias médicas • Dictamen médico • Resumen médico • Diagnóstico y prescripción médica • Resultados de estudios médicos • Prescripción médica
INFORMÁTICOS	***PATRIMONIALES***
• Correo electrónico	• Bienes muebles e inmuebles • No. de cuenta bancaria • Fianzas • Servicios contratados • Seguros • Descuentos no oficiales • Información fiscal.
LABORALES	***ACADÉMICOS***
• Capacitación • Domicilio laboral	• Trayectoria académica • Grado de estudios

• Referencias laborales • Referencias personales • Currículum vitae • Actas circunstanciadas • Incidencias • Experiencia laboral	• Título • Cédula Profesional • Certificado de estudios • Reconocimientos
PROCEDIMIENTOS SEGUIDOS EN FORMA DE JUICIO	***DE TRÁNSITO O MIGRATORIO***
• Nombre del actor • Nombre del demandado • Nombre del apoderado • Domicilio del apoderado • Procesos administrativos de ejecución • Procedimientos administrativos de investigación, responsabilidades y auditorías	• Nacionalidad
ESPECIALMENTE SENSIBLE	***NATURALEZA PÚBLICA***
• Filiación sindical • Actas de defunción • Religión	• Nombramientos

INVENTARIO DE SISTEMAS DE DATOS PERSONALES

A continuación, se presentan los sistemas de tratamiento de datos personales con los que cuenta el CECyTE Tabasco.

- ***Dirección Académica***

No.	***Nombre del sistema***
1	Contratación de docentes
2	Reporte de visitas, entrevistas, citatorios, justificantes, cartas compromiso y pláticas psicológicas con alumnos
3	Lista de Asistentes a Eventos
4	Control de horas de descarga
5	Lista de salidas escolares de los alumnos de los Planteles Educativos del CECyTE
6	Planeación Didáctica
7	Biblioteca y Círculos de Lectura
8	Recolección de datos para Estudio Socioeconómico.

- ***Dirección Financiera***

No.	***Nombre del sistema***
1	Pago de cheques
2	Procesos de licitaciones
3	Plantilla de personal
4	Reloj Checador

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

- ***Dirección de Vinculación***

No.	Nombre del sistema
1	Convenios de colaboración con instituciones públicas y privadas
2	Lista de asistentes a eventos
3	Concentrado de viajes nacionales e internacionales
4	Seguimiento de Egresados
5	Encuesta digital para seguimiento de egresados
6	Uso de voz e imagen en actividades de difusión del CECyTE Tabasco

- ***Dirección de Planeación***

No.	Nombre del sistema
1	Inscripciones, Trámite de Titulación y Cédula Profesional
2	Plataforma digital XXII

- ***Subdirección de Informática***

No.	Nombre del sistema
1	Carpetas compartidas.
2	Recepción de equipos de cómputo y revisión de contenido de sistemas operativos e informáticos.

- ***Unidad de Asuntos Jurídicos***

No.	Nombre del sistema
1	Concesiones y Contratos.

- ***Unidad de Transparencia***

No.	Nombre del sistema
1	Solicitudes de Información Pública y Protección de Datos Personales.

- ***Unidad del Sistema para la Carrera de Maestras y Maestros***

No.	Nombre del sistema
1	Convocatorias para docentes

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

FUNCIONES Y OBLIGACIONES

Los servidores del CECyTE que traten los datos personales, tendrán las siguientes funciones y obligaciones

Funciones:

a) Verificar que el sistema de datos personales se encuentre completo y sin alteraciones.
b) Llevar un registro de los servidores públicos, que previa autorización, acceden al sistema de datos personales.
c) Actualizar la relación de usuarios que acceden al sistema de datos personales.
d) Informar al responsable sobre transmisiones parciales o totales del sistema de datos personales y llevar el registro.
e) Informar al responsable del sistema de datos personales sobre los incidentes que ocurran y llevar el registro.

Obligaciones:

a) Proponer mecanismos para asegurar que los datos personales en posesión de la unidad administrativa a la que pertenece, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.
b) Garantizar la seguridad de los datos personales y evitar su alteración, pérdida, transmisión y acceso no autorizado

MEDIDAS DE SEGURIDAD IMPLEMENTADAS PARA GARANTIZAR LA PROTECCIÓN DE LOS DATOS PERSONALES

1. 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; refiriéndose 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 sistema de datos personales y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

El CECyTE con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas que pongan en riesgo la seguridad de los sistemas de datos personales, cuenta con los siguientes controles para espacios seguros y seguridad del equipo:

Entorno Institucional: El CECyTE cuenta con la puerta principal de vidrio asegurada, seguidamente se encuentra una puerta a base de herrería que cuenta con una cerradura, las personas que ingresan en horario laboral al edificio, se registran en el libro de gobierno; en cada oficina donde se encuentran resguardados los sistemas de datos personales se cuenta con puertas que contienen cerradura, y los archiveros en donde se concentra la información física y los equipos de cómputo que resguardan la información electrónica cuentan con llave, mismo que cada encargado tiene la responsabilidad de resguardar; estos archivos electrónicos que se encuentran resguardados en los diferentes equipos de cómputo y contienen una medida de seguridad que permite que solo la persona autorizada pueda tener acceso a ellos ya que los equipos cuentan con nombre de usuario y su contraseña.

Entorno de los datos: No se sitúan equipos en sitios altos para evitar caídas; no se colocan elementos móviles pesados o que contengan líquidos sobre los equipos para evitar que caigan sobre ellos; se separan los equipos de las ventanas para evitar que caigan por ellas, qué objetos lanzados desde el exterior los dañen o que por efectos de las lluvias y filtraciones estas puedan mojarse; el CECyTE está dotado de equipo para la extinción de incendios conforme a los requerimientos de (Protección Civil); se cuentan con módulos de trabajos que garantizan la estabilidad de los equipos para prevenir que estos sufran daño por un caso fortuito o de fuerza mayor. Así mismo el acceso a los equipos en los que se alojan las bases de datos está restringido, mediante claves de acceso, al personal que captura y utiliza operativamente tales datos.

2. Controles de Identificación y Autenticación de Usuarios

Identificación y autenticación. Los controles de identificación y autentificación de los usuarios que acceden a los sistemas de datos personales del Colegio, son los siguientes:

El CECyTE ha establecido un proceso de identificación y autenticación a los servidores públicos que tienen acceso a los sistemas de datos personales, esto con la finalidad de que el servidor público pruebe que está autorizado para tener acceso a dicho sistema. Para poder ingresar a cualquier servicio de la red es necesario pasar por tres procesos: Autenticación, se refiere al procedimiento a través del cual la

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

persona coloca su identificación sin equivocarse, es decir coloca el usuario y contraseña. Autorización, es el procedimiento a través del cual el sistema aprueba el acceso de la persona previamente identificada, si una persona no autorizada intenta tener acceso al sistema, este se bloquea y no permite su acceso.

3. Controles y mecanismos de seguridad para las transferencias

Transmisiones mediante el traslado de soportes físicos:

a) El envío se realiza a través de los notificadores autorizados siempre y cuando esta transferencia atienda a un requerimiento o mandato de autoridad jurisdiccional;
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, previa acreditación con identificación oficial; así como a la autoridad jurisdiccional que la haya solicitado.
d) Toda entrega de información requiere acuse de recibo; y

Transmisiones mediante el traslado físico de soportes electrónicos

a) El envío se realiza a través de los notificadores autorizados siempre y cuando esta transferencia atienda a un requerimiento o mandato de autoridad jurisdiccional;
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, previa acreditación con identificación oficial; así como a la autoridad jurisdiccional que la haya solicitado.
d) Toda entrega de información requiere acuse de recibo; y
e) A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar cifrados.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Transmisiones mediante el traslado sobre redes electrónicas

a) A partir de la emisión 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:

- A otros sujetos Obligados, siempre y cuando sea atendiendo un mandamiento de autoridad jurisdiccional.

Tipo de Traslado:

- De soportes físicos
- Físico de soportes electrónicos

Vulneraciones a la Seguridad de los Datos Personales

La bitácora de Vulneraciones a los Sistemas de Datos Personales del Colegio, contiene los siguientes datos:

- Número del sistema
- Fecha de Vulneración
- Hora de vulneración
- Naturaleza del incidente
- Descripción detallada de las circunstancias en torno a la vulneración ocurrida
- Categorías de los datos personales
- Sistemas de datos personales comprometidos
- Datos Personales comprometidos
- Recomendaciones al titular de las medidas para proteger sus intereses
- Acciones correctivas implementadas de forma inmediata y definitiva
- Medios para obtener más información al respecto

4. Técnicas de supresión y borrado seguro de Datos Personales

Métodos Físicos: La supresión se realiza de la siguiente manera:

a) Se realiza la trituración mediante corte cruzado o en partículas: Este consiste en cortar el documento en formas vertical y horizontal generando fragmentos diminutos imposibles de unir.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

b) Se realiza la destrucción de los medios de almacenamiento electrónicos mediante desintegración: consiste en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos: Esto se realiza de la siguiente manera:

a) Sobre-escritura: se realiza sobrescribiendo información nueva en la superficie de almacenamiento utilizables, es decir en el mismo lugar de la información existente a fin de hacer imposible su lectura; lo anterior, haciendo uso de las diferentes herramientas de software que para tales efectos existen.

No tendrá lugar la supresión de los sistemas de datos personales cuando exista una disposición expresa en una Ley que exija su conservación.

ANÁLISIS DE RIESGOS

El Análisis de Riesgo es la evaluación cuantitativa y cualitativa sobre la posibilidad de que un sistema de datos personales pueda sufrir una pérdida o daño; por lo anterior, el análisis de riesgos de los sistemas de datos personales en posesión del CECyTE Tabasco, se realizó basado en la metodología BAA, publicada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

El análisis de riesgo de cada una de las Unidades Administrativas del CECyTE, que cuentan con sistemas de datos personales, fue realizado con base basado en la siguiente clasificación:

Tipo de Dato	Nivel de Riesgo Inherente
Ubicación en conjunto con patrimoniales	Reforzado
Información adicional de tarjeta bancaria	Reforzado
Titulares de alto riesgo	Reforzado
Salud	Alto
Origen, creencias e ideológicos	Alto
Ubicación	Medio
Patrimoniales	Medio
Autenticación	Medio
Jurídicos	Medio
Tarjeta bancaria	Medio
Personales de identificación	Bajo

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

ANÁLISIS DE BRECHA

El análisis de brecha para la seguridad de los datos personales en posesión del CECyTE, es la herramienta para identificar la distancia que existe entre las medidas recomendadas en el Plan de Trabajo y las medidas implementadas para cada uno de los tratamientos reportados, este documento toma como referencia la "Metodología de Análisis de Riesgo BAA (Beneficio, Accesibilidad y Anonimidad del atacante)".

El campo denominado "Control" describe las medidas de seguridad faltantes en el ITAIP y el "Parámetro" describe las medidas a implementar para cubrir esas deficiencias.

Medidas de Seguridad Avanzadas para Accesos desde Red Interna:

Control	Parámetro
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Cada Área Administrativa deberá contar mínimo con un dispositivo de almacenamiento removible, con capacidad suficiente que permita el respaldo la información de forma periódica que permita tener limpia las pantallas de los equipos de cómputo.
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos.
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Considerar contraseñas para los dispositivos de red diferentes a las provistas por defecto. WIFI: establecer contraseña.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Medidas de Seguridad Administrativas

Control	Parámetro
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad	Revisiones anuales, considerando como estándares de seguridad los controles de la lista del análisis de riesgo.
Concienciación, educación y entrenamiento de seguridad de la información: Todos los servidores públicos deben recibir concienciación. Asimismo, debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Elaborar un plan de capacitación que contenga temas de medidas de seguridad de los sistemas de datos personales.
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad.
Eliminación de los derechos de acceso: Los derechos de acceso de todos los servidores públicos 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.	Realizar un procedimiento para que, una vez terminada la relación laboral entre el servidor público y el ente, el primero no tenga acceso a los sistemas electrónicos desde un equipo externo.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Es necesario que cada Unidad Administrativa tenga su propio inventario de sus sistemas de datos personales, para mayor control de estos.
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones	Protocolos Seguros Cifrado del medio Autenticación Disociación de información cuando los datos pasen a un entorno de mayor anonimidad
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

Medidas de Seguridad Física

Control	Parámetro
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	No se cuenta con espacios suficientes que permita la distribución física de los servidores públicos.
Control de acceso en la entrada principal de los Servidores Públicos del CECyTE, mediante identificación	Entregar a los Servidores públicos del CECyTE identificación oficial que los acredite como servidores públicos del ente, mismo que deberán portar visiblemente.
Eliminación de los derechos de acceso: Los derechos de acceso de todos los servidores públicos a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato,	Retirar al servidor público que termine su relación laboral con el CECyTE, toda fuente de acceso a las instalaciones donde se encuentra el resguardo físico de los sistemas de datos personales, tales como llaves de oficina de

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

acuerdo o cuando se requiera hacer un ajuste.	archiveros y retirar identificación oficial.
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	Cifrar la información, implementar algún programa que permita encriptar la información para evitar que personas no autorizadas puedan acceder a los sistemas de datos personales. De igual manera se deberá utilizar en la transmisión de datos.
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removible.	No se cuenta con dispositivos de almacenamiento móviles y por lo que se tendrá que dotar a los servidores públicos de dichos dispositivos; estos serán resguardados en un lugar seguro y será administrado por el Encargado de los SDP.
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Debe mediar autorización por escrito.
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	Realizar revisiones aleatorias de las bitácoras de acceso para identificar accesos no autorizados. Considerar una frecuencia semestral.
Definir e implementar listas de control de acceso	Tener un inventario de servidores públicos que cuentan con autorización para el acceso a la información electrónica.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

PLAN DE TRABAJO

En medida de la disponibilidad financiera, se ha planteado implementar las medidas de seguridad faltantes en un periodo de veinticuatro meses a partir de la emisión 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, trituradoras de papel, cestos metálicos para papeles y sustitución de los materiales plásticos e inflamables, se realizarán conforme a los tiempos administrativos del Colegio y el presupuesto lo permita.

Del mes 1 al 24 se deben de cumplir con lo siguiente:

CONTROL	PARÁMETRO	ÁREAS ADMINISTRATIVAS RESPONSABLES
Fuga de información: se deben de prevenir las oportunidades de fuga de información	Detectar las áreas vulnerables	Todas
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Identificar	Todas
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	Subdirección de informática
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Firma de resguardos de los medios de almacenamientos removibles	Todas
Plan de contingencia: se elaborará un plan de contingencia para la protección de la información en posesión del Colegio y se difundirá en el interior del mismo.	Que el personal del Colegio cuente con los conocimientos básicos de medidas a tomar ante un caso	Todas

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

	fortuito o de fuerza mayor.	
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Acuerdo de responsabilidad	Todas
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Realizar revisiones	Subdirección de Informática
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 requiera hacer un ajuste.	Cambiar claves de acceso en los equipos cuando se requiera hacer un ajusto por movimiento de personal	Subdirección de Informática
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Eliminar el sistema de datos personal de manera segura cuando se haya cumplido el objetivo por el cual fue creado.	Todas
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.	Establecer mecanismo de monitoreo	Unidad de Tecnologías
Capacitación: elaborar un programa de capacitación enfocado a las medidas de seguridad para la protección de los sistemas de datos personales.	Integrarlo al programa general de capacitación.	Unidad de Transparencia

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

MECANISMOS DE REVISIÓN Y MONITOREO DE LAS MEDIDAS DE SEGURIDAD

A partir de la emisión del presente documento, se deberán implementar mecanismos de revisión y monitoreo y estos se deben realizar de manera anual, y en caso que sea necesario, se realizará un informe de su resultado.

PROGRAMA GENERAL DE CAPACITACIÓN

El programa general de capacitación del CECyTE, en materia de protección de datos personales, se basa en los principios, deberes y obligaciones que señala la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco, misma que en su artículo 1°establece que es un ordenamiento de carácter público y de observancia general en el Estado de Tabasco.

En consecuencia dicho ordenamiento legal señala que “El Responsable deberá implementar los mecanismos previstos en el artículo 35 de la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de Datos Personales en su posesión al Titular y al Colegio, para lo cual deberá observar la Constitución Política Federal, la Constitución Local y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normatividad mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.”

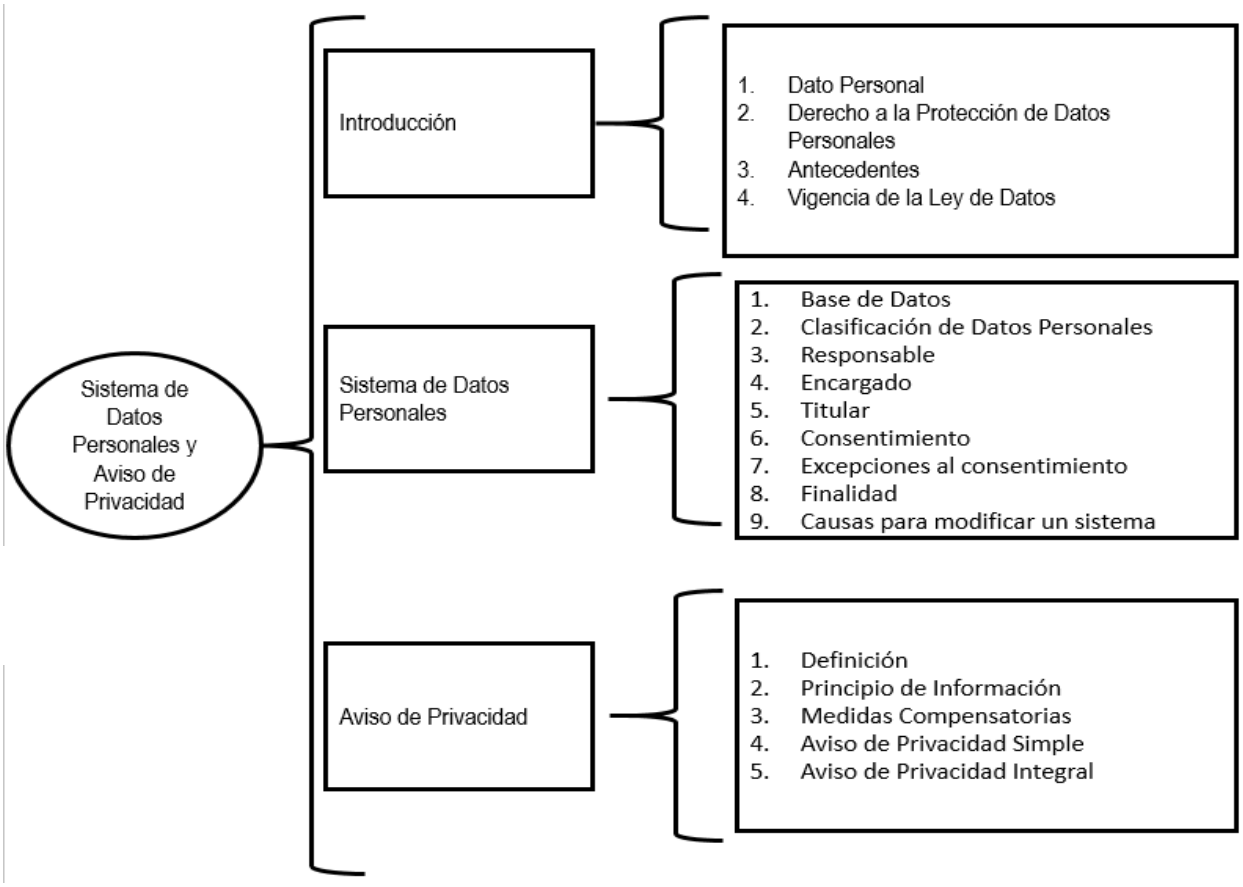
En cumplimiento a lo anterior, se elaboró un Programa General de Capacitación en el que se establecen las acciones a tomar para que este Colegio como responsable del tratamiento de datos personales que custodia, pueda cumplir con los deberes y obligaciones, así como el respeto a los principios establecidos en la multicitada Ley en la materia.

De igual forma es importante mencionar que nuestra Ley de Protección de Datos Personales en Posesión de Sujetos Obligados vigente para el Estado de Tabasco, establece como un DEBER, para los responsables, cargo que ostenta este Colegio, el establecimiento de medidas de seguridad para la protección de los sistemas de datos personales con los que se cuente, todas las acciones que se establezcan e implementen en ese tenor, deberán hacerse constar en el llamado documento de seguridad. Precisamente uno de los requisitos del mencionado documento de seguridad es el establecimiento de este Programa General de Capacitación.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Por ello, con el presente Programa General de Capacitación se establecen las acciones a tomar para que este Colegio, como responsable del tratamiento de datos personales que custodia, pueda cumplir con sus deberes y obligaciones, así como el respeto a los principios establecidos en la ya citada Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Tabasco.

En ese orden de ideas, la Unidad de Transparencia de este Colegio, se dio a la tarea de analizar y dividir los temas normados en dicha ley, teniendo por resultado la creación de los siguientes temas de capacitación.



Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

PLAN DE CONTINGENCIA

Clasificación de la contingencia:

Según sea el tipo de la contingencia se le pude 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 del Colegio.

✓ Grado 2: Requiere tanto el apoyo del personal del Colegio, 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 del Colegio 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).

✓ 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 perdidas estructurales se plantea en algunos casos la posibilidad de contar con

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

algún lugar alternativo de trabajo los sitios alternos de trabajo pueden ser: propios de la organización, 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
- Útiles 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.

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.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

- Si se tienen almacenadas sustancias inflamables como gasolina, acetona, aguarrás, alcohol o tiner, se sugiere colocarlos en lugares ventilados y lejos de las flamas, fuentes de calor y aparatos eléctricos.
- 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, bases de datos, la nube únicamente si es segura).
- 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 la nube).

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 abrir.
- 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.

Terremoto

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, sin embargo si los datos almacenados se encuentran en

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

discos duros, cd, USB, al contar con un respaldo de información incluso en la nube 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.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

Después de un Sismo

- Si usted quedó 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.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

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:

Robo

- En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias, así como un botón de pánico por medio de una App instalada en el celular.

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, fotocopiadoras 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 perdida de información importante.
- Cambiar contraseñas.

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

- 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.

CIERRE

El presente Documento de Seguridad constituye el instrumento mediante el cual se documentan y establecen, de manera integral, las medidas de seguridad de carácter administrativo, físico y técnico implementadas por el **Colegio de Estudios Científicos y Tecnológicos del Estado de Tabasco**, para la protección de los Datos Personales que se encuentran bajo su responsabilidad, con el propósito de garantizar su confidencialidad, integridad y disponibilidad, así como prevenir su daño, pérdida, alteración, destrucción o tratamiento, uso o acceso no autorizado.

Lo anterior, de conformidad con lo dispuesto por la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco**, particularmente en las disposiciones relativas al deber de seguridad, a la implementación y mantenimiento de medidas de seguridad, al sistema de gestión y al Documento de Seguridad, así como demás disposiciones jurídicas y administrativas aplicables en la materia.

En ese sentido, las medidas, controles, mecanismos y acciones previstas en el presente Documento deberán observarse por las personas servidoras públicas y demás personas que, con motivo de sus funciones o atribuciones, intervengan en cualquier etapa del ciclo de vida de los Datos Personales, desde su obtención, uso, almacenamiento y conservación, hasta su bloqueo y, en su caso, supresión, atendiendo en todo momento a los principios, deberes y obligaciones establecidos en la legislación aplicable.

Asimismo, el presente Documento de Seguridad deberá ser objeto de **monitoreo, revisión y mejora continua**, a efecto de verificar la eficacia de las medidas implementadas y, en su caso, determinar las acciones preventivas, correctivas y de mejora que resulten necesarias para fortalecer la protección de los Datos Personales y reducir los riesgos asociados a su tratamiento.

De igual manera, deberá mantenerse actualizado cuando se produzcan modificaciones sustanciales en los tratamientos de Datos Personales que impliquen un cambio en el nivel de riesgo, cuando los resultados del monitoreo y revisión del sistema de gestión determinen la necesidad de realizar adecuaciones, cuando

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx

ocurra alguna vulneración a la seguridad o cuando se implementen acciones correctivas o preventivas derivadas de ésta, en términos de la legislación aplicable.

La observancia del presente Documento de Seguridad será responsabilidad de las áreas administrativas, unidades y personas servidoras públicas que participen en el tratamiento de Datos Personales, dentro del ámbito de sus respectivas atribuciones y funciones, sin perjuicio de las responsabilidades administrativas, civiles, penales o de cualquier otra naturaleza que pudieran derivarse del incumplimiento de las disposiciones aplicables.

Por lo anterior, el **Colegio de Estudios Científicos y Tecnológicos del Estado de Tabasco** refrenda su compromiso institucional de adoptar y mantener las medidas necesarias para garantizar el derecho fundamental a la protección de los Datos Personales, fortaleciendo una cultura institucional orientada a la prevención de riesgos, la seguridad de la información, la responsabilidad en el tratamiento de los Datos Personales y el cumplimiento permanente del marco jurídico aplicable.

En virtud de lo expuesto, el presente Documento de Seguridad se emite para los efectos administrativos y jurídicos conducentes y permanecerá vigente hasta en tanto sea modificado, actualizado o sustituido conforme a las necesidades institucionales y a las disposiciones legales aplicables. -

Boulevard Del Centro 302, Fracc. Electricistas, C.P. 86030, Centro, Tabasco. Tel.: 993 358 0810, ext.: 2026 uaip@cecytab.edu.mx www.cecytab.edu.mx