GUÍA BÁSICA PARA LA TRANSFERENCIA PRIMARIA DE ARCHIVOS QUE CONTIENEN DATOS PERSONALES

PROPÓSITO

Esta Guía tiene como propósito dotar a aquellas áreas del Instituto Tecnológico Superior de Xalapa (ITSX) que en ejercicio de las atribuciones o funciones conferidas por la normativa institucional recaban y dan tratamiento a datos personales, de un parámetro mínimo de actuación y de medidas de seguridad básicas de carácter administrativo y tecnológico, que debidamente implementadas aseguran la transferencia primaria eficaz de los archivos que contienen datos personales bajo su responsabilidad, y que han cumplido la primera fase de su ciclo de vida.

Este parámetro mínimo de actuación y la medidas de seguridad básicas tienen como referencia el principio de proporcionalidad establecido en la *Ley de General de Protección de Datos Personales en poder de los sujetos obligados*, que obliga a los responsables a tratar únicamente los datos personales que resulten adecuados, relevantes y estrictamente necesarios para aquella finalidad que justifica su tratamiento, evitando, en la medida de lo posible, recabar datos no relevantes para el tratamiento o realizar tratamientos que no se justifiquen; por otro lado, procuran garantizar el principio de lealtad, que ordena en favor del titular de los datos personales privilegiar en todo momento la protección del interés por el que otorgó sus datos y su expectativa razonable de privacidad, garantizada en buena medida por la confidencialidad de los propios datos.

Para los propósitos de esta Guía, debe entenderse por transferencia toda derivación de archivos que hagan las áreas del ITSX poseedoras de datos personales al Archivo de Concentración en atención a los plazos fijados en el Catálogo de Disposición Documental aprobado por el Grupo Interdisciplinario.

Conforme a los principios contenidos en la Ley de General de Protección de datos Personales en poder de los sujetos obligados, es necesario que los responsables de los tratamientos de datos personales *re valoren* la necesidad o pertinencia de transferirlos ya que, sin las medidas adecuadas, aumenta el riesgo de divulgación de información confidencial; en caso de ser necesario, indispensable u obligatorio (como en el caso de documentos que han cumplido su ciclo de vida), los servidores públicos responsables deberán adoptar las medidas de seguridad recomendadas en esta Guía, así como aquellas

que en su criterio contribuyan a preservar la confidencialidad, sin que ello implique obstaculizar la transferencia primaria de archivos, pues se trata de asegurar la transferencia de archivos que contienen datos personales, no de suspenderla o cancelarla.

Es importante señalar que el principio de responsabilidad recae, esencialmente y formalmente, en las áreas y órganos del ITSX que recaban, tratan y conservan los datos personales conforme a sus atribuciones o funciones específicas; y operativamente en los servidores públicos responsables de tales áreas, incluidos los responsables de los archivos de trámite; las medidas de seguridad aquí propuestas atienden al cumplimiento de dicho principio, detectando riesgos potenciales en la transferencia de archivos que contienen datos personales y dotando a las áreas y servidores públicos responsables de mecanismos de seguridad adecuados para su aseguramiento.

MARCO JURÍDICO

- Ley General de Archivos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Decreto que crea el Instituto Tecnológico Superior de Xalapa, Veracruz.
- Reglamento Interno del Instituto Tecnológico Superior de Xalapa, Veracruz.
- Lineamientos para Catalogar, Clasificar y Conservar los Documentos y la Organización de Archivos.
- Lineamientos generales para orientar sobre la creación o modificación de ficheros o archivos que contengan datos personales, los que deberán ser acatados por los sujetos obligados por la Ley de Transparencia y Acceso a la Información Pública del Estado de Veracruz de Ignacio de la Llave.
- Lineamientos para la Tutela de los Datos Personales en el Estado de Veracruz.

TRANSFERENCIA DE DATOS PERSONALES EN ARCHIVOS FÍSICOS

La transferencia de datos personales de manera física desde las áreas del ITSX al archivo de concentración es una actividad cotidiana y necesaria para el desarrollo de las atribuciones y funciones que les confiere la normativa interna; esta actividad administrativa despliega diversas áreas de oportunidad encaminadas a que las transmisiones físicas de datos personales se realicen bajo medidas de protección que aseguren la confidencialidad de los datos que se transfieren.

Ejemplos de transmisiones de archivos físicos con contenido de datos personales son:

- listas de asistencia;
- datos de contactos o de vehículos;
- currículums vitae y solicitudes de ingreso;
- expedientes de personal;
- contratos y otros documentos jurídicos;
- solicitudes de admisión y exámenes de ingreso;
- trámites de inscripción o reinscripción;
- expedientes del alumnado;
- documentos oficiales expedidos en favor del alumnado (títulos, constancias, liberaciones, etc.);
- pólizas u otros documentos contables o fiscales.

En estos casos, los datos personales pueden reflejarse en un documento anexo o en el propio texto de los oficios a través de los cuales se transfieren; sin embargo, conforme a las disposiciones de la Ley General de Archivos, la transferencia de documentos físicos al Archivo de Concentración, resulta en una obligatoriedad conforme a los plazos establecidos en el Catálogo de Disposición Documental, y tratándose de expedientes relacionados con el alumnado, el personal o terceros prestadores de servicios o proveedores de bienes, resulta evidente que serán transferidos datos personales, por lo que se requiere seguir procesos que aseguren la confidencialidad de los mismos.

Es en este contexto que se presentan las medidas más recomendables para la transmisión de datos personales en forma física:

1. Los expedientes que contienen datos personales deben transferirse cerrados, cancelados y sellados, lo que asegura que su revisión, en caso de ser necesaria, la realice solamente el personal del área responsable de su tratamiento; se recomienda forrar el expediente con papel Kraft, e implementar controles de seguridad físicos, como la colocación de sellos o firmas autógrafas de tal forma y en lugares que aseguren tanto al responsable del Archivo de Concentración, como al responsable del Archivo de Trámite de la unidad administrativa que transfiere, que el paquete donde se encuentra la información no ha sido quebrantado durante el traslado o su conservación.

2. Se recomienda incluir en al menos uno de los lados del expediente, la advertencia de que contiene información confidencial que no puede ser reproducida, compartida o conservada por ningún medio, y que, una vez que cumpla su ciclo de vida, ésta deberá ser completamente eliminada de conformidad con lo establecido en la respectiva Ficha Técnica de Valoración Documental y el Catálogo de Disposición Documental. Esta medida puede quedar reflejada, como ejemplo, en un etiquetado como el siguiente:

> **CONFIDENCIAL**
>
> **La información contenida no deberá ser copiada, reproducida, compartida o conservada por ningún medio y una vez cumpla su ciclo de vida, deberá ser eliminada conforme a lo previamente determinado**

3. En las unidades de transferencia (cajas) en las que sean transferidos archivos con datos personales, deben ser adheridos además de la carátula correspondiente, letreros como el ejemplificado en el punto anterior.

4. En las transferencias de archivos que contienen datos personales, el personal autorizado (responsables de archivo de trámite y de concentración) debe custodiar en todo momento el traslado de la información, asegurándose que se contenga en contenedores físicos (unidades de traslado) adecuados hasta su destino.

5. Ninguna persona distinta al personal autorizado (responsables de archivo de trámite y de concentración) puede suplir la responsabilidad del traslado de archivos que contienen datos personales.

Estas medidas administrativas evitarán que los datos personales queden expuestos en el proceso de la transferencia hacia el archivo de concentración, brindando certeza a los titulares de los datos de que la confidencialidad de estos no será vulnerada.

TRANSFERENCIA DE DATOS PERSONALES EN ARCHIVOS ELECTRÓNICOS

Algunas transmisiones de datos personales se realizan de manera electrónica, a través del envío de archivos adjuntos en correos electrónicos, usando sistemas o aplicaciones institucionales, o mediante el uso de contenedores físicos de datos electrónicos, tales como discos duros, medios ópticos (CD, DVD, memorias USB o SD), a través de los cuales se transmiten archivos que contienen datos personales.

Por ejemplo, la información del estudiantado relativa a la gestión administrativo-académica o la trayectoria escolar es gestionada, en su mayaría a través del Sistema Institucional establecido para ello o mediante correos electrónicos.

Existen varias medidas tecnológicas para proteger datos personales que se comparten a través de archivos electrónicos. Una medida básica y de fácil implementación es la encriptación de los archivos.

Encriptar o cifrar los archivos es un procedimiento que impide que la información sea visible y servible para los usuarios no autorizados a conocerla. Para ello, es posible establecer una contraseña de acceso a los archivos.

1. Encriptar archivos Office

Para encriptar los archivos elaborados en programas de Office (Word, Excel, Power Point), es necesario seguir los siguientes pasos:

Paso 1. Abrir el documento. Ir a "Archivo" y luego a "Información".
Paso 2. Dar clic en "Proteger documento/libro".
Paso 3. Seleccionar "Cifrar con contraseña".
Paso 4. Escribir la contraseña y luego confirmarla.
Paso 5. El documento ha quedado protegido con contraseña.

2. Encriptar archivos con herramienta 7-zip

Para encriptar los archivos en cualquier formato (por ejemplo, en PDF) es necesario llevar a cabo el siguiente procedimiento:

Paso 1. Abrir el explorador de archivos y seleccionar el(los) archivo(s) a encriptar.
Paso 2. Dar clic secundario (botón derecho del ratón en la mayoría de los casos) y seleccionar la opción de 7zip- > Añadir al archivo....
Paso 3. Seleccionar formato de archivo a comprimir (7-zip, tar, etc.).
Paso 4. En el apartado de "encriptación" escribir la contraseña en los dos campos indicados para ello.

Paso 5. Dar clic en "Aceptar". 7-zip empaqueta y crea un archivo con el nombre seleccionado para el mismo, el cual se ha protegido correctamente mediante contraseña.

Con este procedimiento se logran proteger archivos tipo PDF, sin necesidad de tener la licencia de Adobe Acrobat Professional. Para encriptar archivos a través de esta herramienta, se requiere contar con el programa 7-zip, el cual debe solicitarse formalmente al Departamento de Tecnologías de la Información (DTI).

3. Recomendaciones para elegir contraseñas de encriptación

Cualquier contraseña o clave de acceso a utilizarse, deberá construirse de forma robusta, conforme a lo siguiente:

1. Contar con una longitud de mínimo 9 caracteres.
2. Incluir por lo menos: una letra mayúscula, una letra minúscula, un símbolo especial y un número.
3. Evitar el uso de palabras comunes o datos personales.

Las claves de acceso son intransferibles, pudiéndose compartir única, exclusiva y formalmente al responsable del Archivo de Concentración con la finalidad de que, dado un caso fortuito, fuerza mayor o de absoluta emergencia, puedan ser visualizados; pero, sobre todo, para qué llegado el término de su ciclo de vida, la información pueda ser eliminada en los términos del Catálogo de Disposición Documental.

Se recomienda que la contraseña que se elige para encriptar los archivos electrónicos se comparta en un correo electrónico distinto a aquel en el que se remitieron los archivos que contienen datos personales, ello para disociar la protección del archivo con la medida de seguridad adoptada o, incluso, mejor aún, a través de otro medio de comunicación entre el emisor y el receptor.

4. Transmitir archivos a través de OneDrive

Otra forma de transmitir de forma segura archivos electrónicos con datos personales es a través del uso de OneDrive. Este programa, aunque no contempla la opción de encriptar archivos electrónicos, permite controlar qué personas pueden acceder o editar los archivos compartidos. Para ello, se debe realizar el siguiente procedimiento:

Paso 1. Ingresar, mediante el programa OneDrive, a la carpeta o archivo que se desea compartir.
Paso 2. Dar clic secundario (botón derecho del ratón en la mayoría de los casos) y seleccionar la opción de Compartir.
Paso 3. Escribir los correos electrónicos de los destinatarios y seleccionar las personas que tendrán acceso al vínculo.
Paso 4. Determinar si se permitirá edición de los usuarios a los que se les comparte el vínculo en caso de archivos editables.
Paso 5. Dar clic en "Aplicar". La herramienta de OneDrive genera una liga que se podrá copiar y colocar en el correo electrónico requerido para dar conocimiento de a quien se le comparte el recurso.

Es importante aclarar que los usuarios deben estar migrados a Office365. En caso contrario, solicitar al DTI dicha migración a través de la mesa de servicios.

MEDIDAS DE SEGURIDAD DEL ARCHIVO DE CONCENTRACIÓN

Sólo el responsable del Archivo de Concentración puede tener acceso, para el proceso de eliminación, a los archivos que contienen datos personales.

El resguardo de las contraseñas electrónicas es absoluta responsabilidad del responsable del Archivo de Concentración.

En la ubicación topográfica que corresponda a las unidades de transferencia que contienen datos personales, deberá señalarse que se contienen datos personales, para ello puede usarse el ejemplo del punto 2 del apartado Transferencia de Datos Personales en Archivos Físicos.

En los procesos de eliminación de archivos que contienen datos personales, tanto físicos como electrónicos, además del Responsable del Archivo de Concentración y del responsable del archivo de trámite de la Unidad Administrativa responsable del tratamiento de los datos personales a ser eliminados, deberá contarse con la asistencia de la Coordinación de Archivos y la Unidad de Transparencia, pudiéndose habilitar personal específicamente para el acto; todos los concurrentes deberán verificar la eliminación total de los datos personales, lo cual quedará consignado en el Acta respectiva.

CONCLUSIÓN

Esta Guía es de carácter informativo y orientada a conseguir que la transferencia de datos personales se realice de manera segura.

Las sugeridas son medidas básicas que garantizan, cuando menos, que la información no quede expuesta a personas ajenas al área responsable del tratamiento de los datos personales y al responsable del Archivo de Concentración.

Todos los usuarios son responsables de la información que generen, utilicen y transfieran, a través de los medios informáticos que utilicen, así como de implementar y supervisar los controles para protegerla durante su manejo considerando la clasificación y gestión de la información de acuerdo con sus atribuciones y funciones.

Los responsables de los archivos de Trámite y de Concentración deberán firmar el documento denominado Deber de Confidencialidad ante el Comité de Transparencia del Instituto.