MEDIDAS DE SEGURIDAD

Catálogo de medidas de seguridad

Descripción breve

Guía para la implementación de las medidas de seguridad y el nivel de riesgo inherente

Instituto de Transparencia
[Dirección de correo electrónico]

I. Justificación

En términos de las disposiciones de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo (LEPDPPSOEH), el Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo (ITAIH) es responsable de la protección y confidencialidad de los datos personales que recaba para realizar sus funciones u ofrecer sus servicios. Por tanto, tiene la obligación de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico.

La finalidad de las medidas de seguridad enfocadas especialmente en la protección de los datos personales es evitar cualquier daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado en las actividades cotidianas de las áreas administrativas que integran el ITAIH y que pudieran afectar la confidencialidad de los mismos, dejando en estado de vulnerabilidad a sus titulares.

Para la elaboración del Catálogo de Medidas de Seguridad para los Tratamientos de Datos Personales del ITAIH (Catálogo–ITAIH), se recomienda realizar un censo informativo con aquellas áreas involucradas en el tratamiento de los datos personales (Encuesta sobre análisis de riesgo y medidas de seguridad), con la finalidad de conocer dos aspectos:

1. El nivel de riesgo a que pudieran estar expuestos los datos personales.
2. La naturaleza y alcances de las medidas de seguridad implementadas por las áreas que impactan de manera directa o indirecta en la protección de datos personales.

Asimismo, este Catálogo–ITAIH se construyó a partir de los parámetros normativos y buenas prácticas que se desprenden de la propia LEPDPPSOEH.

II. Políticas de seguridad

De conformidad con los artículos 3, fracción XXII y 47 de la LPDPPSOEH, los sujetos obligados deben implementar diversas medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales.

El ITAIH, por la propia naturaleza de sus funciones y previo a las disposiciones legales en materia de protección de datos personales, ha implementado diversos

mecanismos encaminados a la seguridad y protección de los datos personales que trata en el marco del ejercicio de sus atribuciones legales y reglamentarias.

Por ejemplo, las medidas de seguridad de carácter administrativo son aquellas relacionadas con la organización del sujeto obligado. Se refieren a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información; así como la sensibilización y capacitación del personal en materia de protección de datos personales.

Al respecto, las áreas del ITAIH tienen la obligación de generar diversos documentos relacionados con dichas medidas de seguridad. Como ejemplo, se encuentran los Manuales de Organización y Procedimientos en donde se describen los procesos, responsables y obligaciones respecto del tratamiento de datos personales; las políticas archivísticas; y, las políticas de capacitación en la materia.

Las medidas de seguridad de carácter físico son aquellas encaminadas a la protección del entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Algunas medidas previstas son las de prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; entre otros.

Sobre el particular, el ITAIH, cuenta con la Dirección de Administración y Finanzas, misma que se ocupa de brindar y supervisar los servicios de seguridad a los servidores públicos, así como de preservar los bienes muebles e inmuebles de la misma; establecer, coordinar y mantener un sistema riguroso para el control de los ingresos en los módulos de acceso para el control y registro de la identificación oficial de los servidores públicos y usuarios de los servicios que son brindados en el ITAIH.

Por último, las medidas de seguridad de carácter técnico son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Algunas medidas establecidas son las de prevenir el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; generar un esquema de privilegios; gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales, entre otras.

Sobre este tipo de medidas, el ITAIH, cuenta con la Dirección General de Tecnologías de la Información, que se encarga, entre otras cosas, de administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia; planear, diseñar, mantener y supervisar la operación de los sistemas de información y comunicación que requieran los órganos y áreas; proporcionar los servicios de mantenimiento a las redes, sistemas, equipo informático, comunicación y digitalización de los órganos y áreas del ITAIH; ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento.

Por lo anterior, es posible advertir que, en principio, el Instituto cuenta con medidas de seguridad generales de los tres tipos y acordes a los parámetros normativos de la protección de los datos personales; sin embargo, el Catálogo–ITAIH tiene como finalidad identificar las medidas de seguridad específicas que existen en cada una de las áreas administrativas en sus entornos cotidianos y encauzar la implementación de aquellas adicionales que se requieran para garantizar la efectiva protección de los datos personales.

III. Medidas de seguridad para los tratamientos de datos personales.

A partir de lo referido en los apartados anteriores y la información que se recabe a través del censo informativo, el Catálogo se integra de manera enunciativa por las siguientes medidas que las áreas habrán de implementar en función del nivel de riesgo de cada uno de sus tratamientos:

a) Medidas de seguridad administrativas

A. Declaración de confidencialidad: realizar esta declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.

B. Listado de personal: elaborar un documento que contenga la relación del personal que interviene en el tratamiento de datos personales, en donde se incluya nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.

C. Clasificación de los archivos físicos: identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.

D. Clasificación de los archivos electrónicos: identificar y etiquetar las bases de datos en soporte electrónico con el nombre del Tratamiento de Datos Personales conforme al Inventario reportado por el área.

E. Capacitación: el personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el Comité de Transparencia en el Programa Anual de Capacitación.

F. Bitácora de vulneraciones: implementar un control informativo en donde se reporten los tipos de vulneraciones con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la Unidad de Transparencia del Instituto para que tome las acciones pertinentes. Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.

G. Depuración y borrado seguro del archivo físico: Transferir y depurar el archivo físico de manera periódica, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.

H. Depuración y borrado seguro del archivo electrónico: borrar, de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo. Solicitar a Dirección General de Tecnologías de la Información que proporcione un programa para el borrado integral de la información, o en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen. Además, para la depuración y borrado seguro de las bases de datos electrónicas, se deberá levantar un acta, signada por el titular del área y remitirse copia de la misma a la UT.

I. Bitácora de consulta: establecer una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos.

J. Responsable de seguridad: designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.

K. Transferencias: realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.

b) Medidas de seguridad físicas

A. Cuidado de los bienes informáticos: Mantener en buen estado el bien informático que le haya sido asignado y no abrir los equipos o bien, introducir en ellos cualquier tipo de instrumento o software que no sean los apropiados para el trabajo y que no hayan sido validados por la Dirección de Tecnologías de la Información, tampoco alterar el orden de los cables conectados.

B. Prevenir accesos no autorizados: prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados y autorizados por el área.

C. No instalar equipos ajenos: Abstenerse de instalar equipos de cómputo que no sean propiedad del ITAIH sin permiso de la Dirección de Tecnologías de la Información. Los usuarios que requieran hacer uso de la red interna del ITAIH deben usar solamente las direcciones IP asignadas por el área administrativa correspondiente. En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, éste debe ser revisado previamente por el antivirus. En el caso de encontrarse infectado el dispositivo, el usuario debe extraer inmediatamente sin consultar, modificar o copiar información alguna.

D. Traslado de equipos de cómputo: observar el procedimiento dispuesto por la Dirección de Administración, relativo al uso y aprovechamiento de los bienes y servicios informáticos, para el traslado de equipos de cómputo fuera de las instalaciones.

Cada usuario será responsable del resguardo del equipo de cómputo que se le haya proporcionado para el desempeño de sus funciones, de conformidad con las necesidades propias del órgano de su adscripción

E. Archivero con candado: Resguardar las bases de datos en archivo físico en un archivero con candado o con llave de seguridad, cuyo acceso sólo será permitido al personal autorizado.

F. Candados de seguridad para equipos de cómputo: fijar con candados de seguridad los equipos de cómputo que contengan bases de datos personales.

G. Zona de confidencialidad: definir una zona de confidencialidad en donde se resguardarán los archivos físicos o equipos de cómputo que contengan las bases de datos, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado.

c) Medidas de seguridad técnicas

A. Cuidado de la contraseña personal: abstenerse de compartir contraseñas personales de la red institucional, las contraseñas, tokens, identificadores o cualquier mecanismo utilizado para la autenticación en un recurso informático.

B. Actualización de contraseñas: cambiar las contraseñas cada tres meses por lo menos, a efecto de evitar robo de identidad. En caso de olvido o sospecha de divulgación de una contraseña o mecanismo de autenticación, los usuarios deberán realizar el cambio de los mismos en los sistemas informáticos.

C. Reportar fallas: notificar al área correspondiente cualquier fallo, error, sospecha, violación o incumplimiento a las políticas de seguridad de la información.

D. No instalar softwares: abstenerse de descargar en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia.

E. Contraseñas robustas: construir contraseñas con rol de administrador de forma robusta, atendiendo a los siguientes criterios: Contar con una longitud mínima de 12 caracteres. Incluir, por lo menos, dos letras mayúsculas, dos letras minúsculas, dos símbolos especiales (punto, coma, guion, etcétera) y un número; evitar el uso de palabras comunes o datos personales; renovarlas de manera periódica; las contraseñas no podrán repetirse en al menos 10 iteraciones; almacenarlas de forma cifrada y en archivos electrónicos distintos en los que se almacenan datos de aplicaciones.

F. Respaldo de información: realizar respaldos de la información que resida en el equipo de cómputo asignado. La Dirección de Tecnologías de la Información, a solicitud del usuario, asesorará y apoyará a los usuarios en el procedimiento para considerando las necesidades propias del área.

IV. Nivelación de las medidas de seguridad de acuerdo al nivel de riesgo inherente.

Las medidas de seguridad que deberán adoptarse deben tomar como referencia el nivel de riesgo inherente de cada dato que conforma el sistema de tratamiento. Para ello se requiere primeramente llevar a cabo la identificación de activos.

Identificar activos.

Un activo se define como todo bien o recurso que puede ser necesario para implementar y mantener una operación de tratamiento de datos personales en cualquier etapa de su ciclo de vida.

En este sentido, los activos que tienen valor y requieren resguardarse son los datos personales, recordando que estos activos conviven con otros activos, como servicios, aplicaciones (*software*), equipos (*hardwarw*), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

De este modo podemos identificar dos tipos de activos:

- Activos de información. Información relativa a los datos personales e información de procesos en los que interviene el flujo de datos personales, actividades involucradas en el tratamiento de estos.
- Activos de apoyo. En los cuales residen los activos de información: hardware, software, redes y telecomunicaciones o personal, estructura organizacional, infraestructura adicional.

Para la identificación de activos se recomienda:

a. Detectar todos los activos de información y de apoyo del sistema de tratamiento que pueden afectar la confidencialidad, integridad y disponibilidad de los datos personales en resguardo de su institución. Dentro de estos activos podrá incluir información documentada en papel o formato electrónico, aplicaciones, bases de datos, personal, *hardware*, *software*, infraestructura tecnológica, instalaciones y servicios o procesos externos.

b. Determinar el valor del activo en función de los tres principios fundamentales de seguridad de la información: confidencialidad,

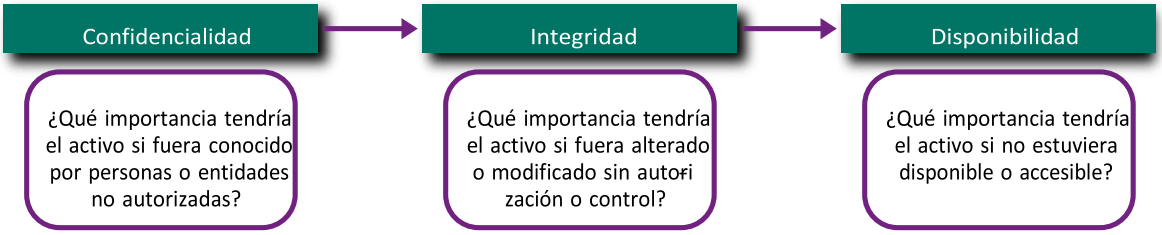
integridad y disponibilidad, aplicándose una escala, por ejemplo, del 1 al 3, donde 1 es el valor más bajo y 3 el más alto. Esta valoración resulta necesaria para conocer el riesgo inherente de cada dato que conforma el sistema de tratamiento.

c. Calcular el valor del activo. Por ejemplo, sumando los valores asignados a la confidencialidad, integridad y disponibilidad, empleándose los siguientes rangos para obtener el valor (cualitativo y cuantitativo) final. En este punto deberá identificar el valor de su inventario. Considere que, si su tratamiento incluye datos sensibles, éstos deberán ser considerados con el valor más alto, debido a su naturaleza.

Valor Cualitativo	*Valor Cuantitativo*
Bajo	1-3
Medio	4-6
Alto	7-9

Tabla 1. Ejemplo de escalas cuantitativas y cualitativas.

Para determinar adecuadamente la valoración de los activos y su asociación con cada principio de seguridad de la información, se establecen las siguientes preguntas:



Una vez establecido el valor por cada propiedad de la seguridad de los datos, debe obtenerse un valor único, por ejemplo, sumando los tres valores y estableciendo el valor cualitativo único de acuerdo con la tabla.

EJEMPLO:

	Confidencialidad	Integridad	Disponibilidad		
Currículum Vitae en papel: contiene nombre completo, dirección particular, teléfono particular, experiencia laboral, historia académica.	3 Justificación: La divulgación o conocimiento por personas no autorizadas podrían traer consecuencias para el titular, en tanto que se podría hacer mal uso de su información personal, pudiendo incluso dañar su integridad.	2 Justificación: La alteración o modificación de los datos contenidos puede traer consecuencias legales para el titular, en tanto que podría alterarse su historia académica o experiencia laboral.	1 Justificación: No tenerlos disponibles no afecta de modo importante a la operación del sujeto obligado, salvo en ocasiones particulares.	6	Medio

Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo

Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo

CATALOGO DE MEDIDAS DE SEGURIDAD

No.	MEDIDAS DE SEGURIDAD ADMINISTRATIVAS	IMPLEMENTADO		OBSERVACIONES
		SI	NO	
1	Identificación y autentificación de persona autorizada para el tratamiento de datos personales;			
2	Aprobación de normativa interna o políticas internas de tratamiento;			
3	Implementación de contraseñas, claves y protocolos de seguridad;			
4	Identificación de roles y perfiles;			
5	Realización de inventario de datos personales, análisis de riesgo y de brecha;			
7	Monitoreo y revisión periódica de las medidas;			
8	Capacitación de personal;			
10	Elaboración de procedimientos para dar aviso al personal custodio de los datos personales sobre la presencia y acceso de personas no autorizadas;			
11	Emisión de reglas sobre la introducción de equipos de cómputo, accesorios y gadgets, o de conexión inalámbrica a áreas restringidas de tratamiento de datos personales;			
12	Emisión de reglamentación interna que contemple infracciones y sanciones con relación al indebido tratamiento de datos personales;			
13	Emisión de reglas para la baja documental en soportes físicos y electrónicos;			
14	Emisión de medidas para la prevención y notificación de infracciones e incidentes;			
15	Emisión de reglas de uso sobre dispositivos de almacenamiento externo;			
17	Realización de pruebas y simulacros;			
18	Inclusión de cláusulas o contratos de confidencialidad para el personal laboral;			
19	Procedimientos y canales para el ejercicio de derechos ARCO;			
20	Procedimientos de disociación o pseudonimización			

Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo

	MEDIDAS DE SEGURIDAD FÍSICAS	SI	NO	OBSERVACIONES
1	Protección de instalaciones, equipos, soportes o bases de datos personales			
2	Utilización de candados, cerrojos, cerraduras, tarjetas de identificación, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de puertas, gavetas, cajones, archiveros, etc.			
3	Implementación de sistemas de vigilancia, alarmas, y de prevención y protección contra siniestros tales como incendios			
4	Señalamiento de áreas de acceso restringido; aparatos de identificación por medio de la voz, iris, huella, ADN, y demás datos biométricos			
5	Resguardo de datos personales a través de infraestructura que garantice condiciones adecuadas de humedad, polvo, iluminación solar y temperatura y evite el deterioro por plagas, consumo de alimentos, y otros factores presentes en el entorno			

	MEDIDAS DE SEGURIDAD TÉCNICAS	SI	NO	OBSERVACIONES
1	Encriptación y cifrado de los datos			
2	Realización de copias de seguridad, resguardos o backups;			
3	Almacenamiento en dos ubicaciones diferentes			
4	Atención de fallas de equipo electrónico y de cómputo;			
5	Indicación de software autorizado			
6	Des habilitación o cancelación de dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.);			
7	Des habilitación o cancelación de puertos de comunicación (USB, paralelo, serial, etc.);			
8	Des habilitación o cancelación de dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc.);			
9	Realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo			
10	Brindar soporte técnico de equipos, sistemas, programas de software, etc.			
11	Instalación de firewalls, antivirus, watchdogs, mecanismos para evitar la pérdida y filtración de datos (data loss prevention)			
12	Segregación de funciones mediante perfiles de acceso			
13	Mecanismos de control de acceso			
14	Monitorización del uso de datos personales			
15	implementación de técnicas de disociación o pseudonimización.			