Transparencia y Verificación

DIRECCIÓN DE TRANSPARENCIA Y VERIFICACIÓN

1. Tratamientos.
    - Capacitaciones.

2. Servidores Públicos que Tratan Datos Personales en el Área (Funciones y Obligaciones)
    - Directora del Área.
    - Verificadores.

3. Documento de Confidencialidad

4. Medidas de Seguridad Implementadas.

A. DIRECCIÓN DE TRANSPARENCIA Y VERIFICACIÓN.

A1. Capacitaciones.
Fecha de elaboración: 05 de Junio de 2024

1. Medios de Obtención:
   I. Directamente del titular a través de listas de asistencia.

2. Tipos de Datos:
   - Datos Personales Identificativos:
     I. Nombre completo.
     II. Correo electrónico.
   - Datos Personales laborales, académicos y patrimoniales:
     I. Área administrativa.
   - Datos Personales biométricos
     I. Fotografía.

3. Formato y Ubicación de los Datos:
   I. Formato impreso ubicado en Expediente: capacitaciones a servidores públicos 2024 Archivero de la Dirección de Transparencia.

4. Finalidades de los Tratamiento:
   I. Acreditar la participación de las capacitaciones
   II. Fines estadísticos.
   (si requiere consentimiento, el tipo de consentimiento es de forma tácito).

5. Servidores Públicos con Acceso a los Datos:
   I. Directora del área.
   II. Verificadores.
   (los servidores mencionados pertenecen al área de Transparencia y Verificación, con la finalidad de Consulta y fines estadísticos).

6. Encargado: No aplica

7. Transferencia de datos: No.

8. Difusión de los Datos: No aplica.

9. Plazo de Conservación y bloqueo: No determinado.

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES AL INTERIOR DEL ÁREA

(CAPACITACIONES A SUJETOS OBLIGADOS)

NOMBRE DE LA INSTITUCIÓN: Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo

UNIDAD ADMINISTRATIVA: Dirección de Transparencia y Verificación

TITULAR DE LA UNIDAD ADMINISTRATIVA: Lic. Martha María Hernández León

RESPONSABLE (S) DEL TRATAMIENTO: Lic. Martha María Hernández León

FUNCIONES: Capacitar a los servidores públicos de los sujetos obligados.

OBLIGACIONES: Generar evidencias de las personas que fueron capacitadas con las debidas obligaciones de resguardo de los datos proporcionados.

¿FIRMÓ DOCUMENTO DE CONFIDENCIALIDAD? Si

ANEXAR DOCUMENTO DE CONFIDENCIALIDAD FIRMADO

REALIZÓ	**AUTORIZÓ**
_____	_____
Lic. Martha María Hernández León	Lic. Martha María Hernández León

CARTA COMPROMISO DE CONFIDENCIALIDAD, NO DIVULGACIÓN, RESERVA Y RESGUARDO DE INFORMACIÓN QUE CONTENGA DATOS PERSONALES

Pachuca, Hgo, a 09 de julio de 2024.

A QUIEN CORRESPONDA
P r e s e n t e

La que suscribe Lic. **Martha María Hernández León**, Directora de Transparencia y Verificación, acepto las condiciones de resguardo, reserva, custodia y protección, así como de la seguridad y confidencialidad de la información que contenga datos personales que con motivo de mis funciones y obligaciones establecidas en el Estatuto orgánico, manual de organización y manual de procedimientos, me veo obligada a desempeñar en el Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales (ITAIH), o de la que tenga conocimiento, con motivo del trabajo, empleo y/o comisión.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica e informática, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de la unidad administrativa a la cual me encuentro adscrita.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Me obligo a devolver cualquier documentación, antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto de la presente en el supuesto de que cese la relación o prestación del servicio con el Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales ITAIH por cualquier motivo.

A t e n t a m e n t e

Nombre completo: _____
Firma: _____
Puesto o Cargo: _____

CATALOGO DE MEDIDAS DE SEGURIDAD
2024

No.	MEDIDAS DE SEGURIDAD ADMINISTRATIVAS	IMPLEMENTADO SI	IMPLEMENTADO NO	OBSERVACIONES
1	Identificación y autentificación de persona autorizada para el tratamiento de datos personales;	X		
2	Aprobación de normativa interna o políticas internas de tratamiento;		X	
3	Implementación de contraseñas, claves y protocolos de seguridad;			N/A
4	Identificación de roles y perfiles;	X		
5	Realización de inventario de datos personales, análisis de riesgo y de brecha;	X		Si se cuenta con inventario
7	Monitoreo y revisión periódica de las medidas;		X	
8	Capacitación de personal;	X		
10	Elaboración de procedimientos para dar aviso al personal custodio de los datos personales sobre la presencia y acceso de personas no autorizadas;		X	
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;		X	
12	Emisión de reglamentación interna que contemple infracciones y sanciones con relación al indebido tratamiento de datos personales;		X	
13	Emisión de reglas para la baja documental en soportes físicos y electrónicos;		X	
14	Emisión de medidas para la prevención y notificación de infracciones e incidentes;		X	

15	Emisión de reglas de uso sobre dispositivos de almacenamiento externo;		X	
17	Realización de pruebas y simulacros;		X	
18	Inclusión de cláusulas o contratos de confidencialidad para el personal laboral;		X	
19	Procedimientos y canales para el ejercicio de derechos ARCO;	X		
20	Procedimientos de disociación o pseudonimización		X	

	MEDIDAS DE SEGURIDAD FÍSICAS	SI	NO	OBSERVACIONES
1	Protección de instalaciones, equipos, soportes o bases de datos personales		X	
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.	X		
3	Implementación de sistemas de vigilancia, alarmas, y de prevención y protección contra siniestros tales como incendios		X	
4	Señalamiento de áreas de acceso restringido; aparatos de identificación por medio de la voz, iris, huella, ADN, y demás datos biométricos		X	
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		X	

	MEDIDAS DE SEGURIDAD TÉCNICAS	SI	NO	OBSERVACIONES
1	Encriptación y cifrado de los datos			Los datos recabados de consevan de manera fisica
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.			