Instituto de Transparencia del Estado de Aguascalientes

itea Unidad de Transparencia
24 OCT. 2024
RECIBIDO
Por: [illegible] Hora: 10:55

INSTITUTO DE TRANSPARENCIA DEL ESTADO DE AGUASCALIENTES
Oficio: ITEA/DP/19/2024
ASUNTO: El que se indica.

Aguascalientes, Ags., a veinticuatro de octubre de dos mil veinticuatro.

L.A. MÓNICA CECILIA ZÚÑIGA CASTILLO
TITULAR DE LA UNIDAD DE TRANSAPRECIA
DEL ESTADO DE AGUASCLAIENTES
P R E S E N T E

Por este conducto, en atención al oficio *ITEA/UT/00131/2024,* y derivado de la solicitud de información con número *010054924000196*. Se informa lo siguiente:

Este Organismo Garante no cuenta actualmente con Documento de Seguridad, de conformidad con las nuevas actualizaciones al Reglamento Interior del Instituto de Transparencia del Estado de Aguascalientes, publicado el veinticinco de diciembre de dos mil veintitrés, esencialmente en su estructura orgánica, por lo que nos encontramos en proceso de integración y recabo de Inventario de Datos según consta en el oficio ITEA/P/068/2024.

1.- Políticas y Programas dentro del Instituto en materia de protección de datos personales.

Este Instituto ha generado programas y sistemas como es:

- El recabo de información de datos personal debe de estar contenido en los avisos de privacidad dentro del Instituto.
- Se continua con el programa de capacitaciones a los Sujetos Obligados, con la finalidad de que se alleguen de la información y se nutran las intuiciones públicas en materia de protección de datos personales.
- Se trabaja en el Generador de Avisos de Privacidad, que debe de ponerse en marcha a mas tardar el día treinta de noviembre de dos mil veinticuatro y podrá ser consultado en la siguiente liga: https://www.itea.org.mx/login.aspx
- Se trabaja en el Documento de Seguridad mismo que contendrá todas las medidas tecnológicas, físicas y administrativas para la protección de los datos personales dentro del Instituto.

2.- Análisis de riesgo y Análisis de Brecha, Este instituto se encuentra conformando el Análisis de Riesgo y de Brecha, por lo que se remite la información con la que se cuenta hasta el momento.

Análisis de riesgos

Las áreas del Instituto de Transparencia del Estado de Aguascalientes que capturan datos personales se rigen por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), estos datos debido a su importancia y vulnerabilidad deben contar con medidas de seguridad para su resguardo.

El análisis de riesgos identifica amenazas y vulnerabilidades que ponen en riesgo la seguridad de los datos personales, evaluando el impacto y la probabilidad de su ocurrencia, este determina cuál riesgo es más importante mitigar o los datos que se encuentran más expuestos.

Para identificar los riesgos se debe enfocar en algunas variables como son:

Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	Medida de Control
Robo de datos personales	Bases de datos no cifradas	Alto	Alta	Crítico	Implementar cifrado en bases de datos y discos
Acceso no autorizado a datos	Falta de control de acceso a datos sensibles	Alto	Media	Alto	Implementar políticas de acceso basado en roles (RBAC)
Pérdida de datos personales	Ausencia de respaldos regulares y encriptados	Alto	Media	Alto	Realizar copias de seguridad cifradas periódicas
Fuga de datos por empleados	Falta de capacitación en protección de datos	Alto	Media	Alto	Capacitación periódica sobre manejo de datos personales
Ataques de ransomware	Protección insuficiente contra malware	Muy alto	Media	Crítico	Instalar sistemas avanzados de detección de amenazas
Violación de políticas de privacidad	Políticas de privacidad no actualizadas	Alto	Baja	Medio	Revisar y actualizar las políticas de privacidad y uso de datos
Transferencia insegura de datos	Uso de protocolos no seguros (sin cifrado)	Alto	Media	Alto	Implementar cifrado SSL/TLS en todas las comunicaciones

- Impacto: Es el grado de daño que puede ocurrir si la amenaza compromete los datos personales.

- Probabilidad: Es la probabilidad de que una amenaza ocurra.
- Medida de Control: Es la accione recomendada para mitigar el riesgo asociado a la vulnerabilidad identificada.

Además de los factores de interés para la sociedad misma y los interesados en obtener información de Datos Personales, como son: beneficios económicos por la venta o uso de los datos personales, datos personales de fácil acceso y poca seguridad tienen mayor probabilidad de ser atacados, es por ello la importancia establecer la seguridad en un alto nivel de los datos digitales, la anonimidad del atacante, ya que es más fácil el tratar de ingresar anónimamente por medio de recovecos digitales a ingresar personalmente al lugar donde se encuentran los datos personales de forma física.

Este análisis de riesgos se desarrolla basándose en el inventario de datos personales que manejan las distintas áreas del Instituto de Transparencia del Estado de Aguascalientes, el cual se incluye en los anexos de este documento, así como su clasificación e importancia, con el fin de identificar y establecer el riesgo de la información y de esta forma aplicar o fortalecer las medidas de seguridad que se describirán en los siguientes puntos.

En base al inventario de datos personales, se considera clasificarlos en Riesgo Bajo, Riesgo Medio y Riesgo Alto derivado del margen de vulnerabilidad de cada uno de los datos y su conjunto, lo anterior basándose en el tipo de dato y el nivel de seguridad requerido para su manejo.

- **Riesgo bajo**: Se considera la información general de una persona física, por ejemplo, los Datos de identificación, académica o laboral:
  - Nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, etc.
- **Riesgo medio**: Son los datos que permiten conocer la ubicación física de la persona, por ejemplo, la dirección física, información relativa al tránsito dentro y fuera del país, o cualquier otro que permita conocer la ubicación de una persona a través de los datos que proporcione alguien más.
  - Dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.

  Se produce o puede producirse usurpación de la identidad de los interesados.

  Los datos que permitan inferir el patrimonio de una persona, saldos bancarios, estados o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito o débito, Así como usuarios de acceso, contraseñas, biométricos, firma autógrafa, digital y electrónica, fotografías, identificación oficial, antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que tenga algún proceso legal o administrativo. Los efectos son reversibles.
- **Riesgo alto**: Son los datos personales sensibles, de salud física o mental, información genética, de raza, ideología, religión, afiliación sindical, preferencia política, sexual, y otros que puedan caer en discriminación o un riesgo grave. Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución, y sus

consecuencias son irreversibles; Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales; Afecta a interesados en situación de especial vulnerabilidad, en particular niños; Causa pérdidas morales o materiales significativas e irreversibles.

A continuación, se describe los riesgos de vulneración de datos personales:

Muy Alto:

- Si el factor de riesgo está materializado y no depende de la probabilidad.
- Si hay constancia de diversas materializaciones de dicho riesgo en el último año en distintas entidades.
- Si hay constancia de una materialización de dicho riesgo en el último año en la misma entidad.
- Existen auditorías/estudios que identifican importantes vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo.

Alto:

- Cuando se materializó el riesgo en el último año en alguna entidad.
- Existen estudios que determinan que la probabilidad podría ser alta.
- Existen auditorías o estudios que identifican posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo.
- Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados o terceros independientes

Bajo:

- Antecedente de una materialización de dicho riesgo en los últimos 10 años en alguna entidad.

Para el tratamiento de los datos personales, sea sistematizado o de forma física se solicita información variada, la cual es ingresada en bases de datos cualquiera que sea su tipo, por lo que a continuación se describen los niveles de riesgo de acuerdo al tipo de dato personal:

Catálogo datos personales de sistemas de tratamiento o bases de datos del Instituto de Transparencia del Estado de Aguascalientes

AREA	ACCIÓN	DATO	RIESGO
B. SECRETARÍA EJECUTIVA	B.1.-Recibir, registrar y turnar Recursos de Revisión, Denuncias y correspondencia.	1. Correo electrónico	
		2. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada	

		para recibir notificaciones, entre otros).	
		3. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		4. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		5. Correo electrónico	
C. SECRETARÍA DE ACUERDOS	C.1.-	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
D. DIRECCION DE ADMINISTRACIÓN Y FINANZAS	D.1.- Asistencia Inventario de datos ITEA	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Datos de identificación	
		3. Huella digital	
	D.2.- Alta de nómina en el banco	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Año de nacimiento o edad	
		3. Beneficiarios	

		4. Correo electrónico	
		5. Datos de identificación	
		6. Domicilio	
		7. Nivel educativo	
		8. Salario del servidor público	
		9. Sexo	
	D.3.- Contratos y convenios	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Correo electrónico	
		3. Datos de identificación	
		4. Teléfono fijo o celular	
	D.4.-Alta en el IMSS	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Año de nacimiento o edad	
		3. Datos de identificación	
		4. Datos laborales	
		5. Salario del servidor público	
	D.5.- Incidencias Inventario de datos ITEA	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Datos de identificación	

		3. Estado de interdicción o incapacidad legal	
		4. Firma	
	D.6.- ISSSSPEA Inventario de datos ITEA	1. Antecedentes laborales	
		2. Año de nacimiento o edad	
		3. Datos laborales	
		4. Correo electrónico	
		5. Domicilio	
		6. Firma	
		7. Nivel educativo	
		8. Salario del servidor público	
		9. Sexo	
		10. Teléfono fijo o celular	
	D.7.- NOMIPAQ Inventario de datos ITEA	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Año de nacimiento o edad	
		3. Correo electrónico	
		4. Datos de identificación	
		5. Domicilio	
		6. Salario del servidor público	
		7. Sexo	
	D.8.- Personal Inventario de datos ITEA	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada	

		para recibir notificaciones, entre otros).	
		2. Antecedentes laborales	
		3. Año de nacimiento o edad	
		4. Correo electrónico	
		5. Currículum Vitae	
		6. Datos académicos	
		7. Datos de identificación	
		8. Datos de salud	
		9. Datos laborales	
		10. Domicilio	
		11. Nacionalidad	
		12. Nivel educativo	
		13. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		14. Sexo	
		15. Teléfono fijo o celular	
		16. Títulos o constancias profesionales	
		17. Títulos profesionales	
E. DIRECCIÓN DE ASUNTOS JURÍDICOS, PROTECCIÓN De DATOS PERSONALES y	E.1.- Capacitaciones y formación de personas facilitadoras del DAI	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Sexo	

GOBIERNO ABIERTO		3. Año de nacimiento o edad	
		4. Teléfono fijo o celular	
		5. Correo electrónico	
		6. Nivel educativo	
		7. Ocupación	
	E.2.- Jornadas de socialización del DAI	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Teléfono fijo o celular	
		3. Sexo	
		4. Año de nacimiento o edad	
		5. Correo electrónico	
		6. Ocupación	
		7. Nivel educativo	
		8. Origen étnico o racial	
F. DIRECCIÓN DE INFORMATICA, TECNOLOGÍAS DE LA INFORMACIÓN Y ARCHIVO	F.1.- Registro de Usuarios y Empleados para Acceso y Administración del Sistema de Inventarios	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada	

		para recibir notificaciones, entre otros).	
		4. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		5. Correo electrónico	
		6. Datos laborales	
		7. Nivel educativo	
		8. Ocupación	
		9. Currículum Vitae	
	F.2.- Generación de Accesos al Portal Nacional de Transparencia	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Firma	
		4. Nivel educativo	
		5. Ocupación	
		6. Correo electrónico	
	F.3.- Registro de Usuarios y Responsables de Sujetos Obligados para Acceso a SIEVAL	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	

		2. Correo electrónico	
		3. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		4. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		5. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		6. Correo electrónico	
	F.4.- Registro de empleados para control de asistencias	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Huella digital	
		4. Sexo	
	F.5.- Registro de empleados para control de acceso	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada	

	a instalaciones del Instituto	para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Huella digital	
		4. Sexo	
		5. Correo electrónico	
	F.6.- Registro de Correo electrónico Institucional	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Correo electrónico	
	F.7.- Gestión de Archivo de Concentración	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Correo electrónico	
		3. Teléfono fijo o celular	
		4. Datos laborales	
G. DIRECCIÓN DE EVALUACÍON Y VERIFICACION	G.1.- Verificación de cumplimiento de las	1. Correo electrónico	
		2. Teléfono fijo o celular	

	Obligaciones de Transparencia		
H. ORGANO INTERNO DE CONTROL	H.1.- Auditorias	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos laborales	
		4. Nivel educativo	
		5. Firma	
	H. 2.- Declaración Patrimonial	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Antecedentes laborales	
		3. Año de nacimiento o edad	
		4. Circunstancias socioeconómicas	
		5. Correo electrónico	
		6. Datos académicos	
		7. Datos laborales	
		8. Datos patrimoniales	
		9. Domicilio	
		10. Nacionalidad	
		11. Nivel educativo	

		12. Salario del servidor público	
		13. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		14. Teléfono fijo o celular	
	H. 3.- Entrega Recepción	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos de identificación	
		4. Datos laborales	
		5. Domicilio	
		6. Nacionalidad	
		7. Nivel educativo	
		8. Firma	
	H. 4.- Substanciación del Procedimiento de Responsabilidad Administrativa	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona	

		autorizada para recibir notificaciones, entre otros).	
		3. Datos de identificación	
		4. Datos personales contenidos en la identificación oficial presentada por la persona física	
		5. Domicilio	
		6. Datos académicos	
		7. Datos laborales	
	H. 5.- Resolución del Procedimiento de Responsabilidad Administrativa	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos de identificación	
		4. Datos personales contenidos en la identificación oficial presentada por la persona física	
		5. Domicilio	
		6. Datos académicos	
		7. Datos laborales	
	H. 6.- Recurso de Reclamación	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	

		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos de identificación	
		4. Datos personales contenidos en la identificación oficial presentada por la persona física	
		5. Domicilio	
		6. Datos académicos	
		7. Datos laborales	
	H. 7.- Recurso de Revocación	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos de identificación	
		4. Datos personales contenidos en la identificación oficial presentada por la persona física	
		5. Domicilio	
		6. Datos académicos	
		7. Datos laborales	
	H. 8.- Investigación (Denuncia)	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada	

		para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos académicos	
		4. Datos laborales	
		5. Datos de identificación	
		6. Datos personales contenidos en la identificación oficial presentada por la persona física	
		7. Domicilio	
	H. 9.- Informe de Presunta Responsabilidad Administrativa	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos académicos	
		4. Datos laborales	
		5. Datos de identificación	
		6. Datos personales contenidos en la identificación oficial presentada por la persona física	
		7. Domicilio	

	H. 10.- Recurso de Reclamación	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Segundo apellido de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		3. Datos académicos	
		4. Datos laborales	
		5. Datos de identificación	
		6. Datos personales contenidos en la identificación oficial presentada por la persona física	
		7. Domicilio	
I. JEFATURA DE COMUNICACIÓN Y DIFUSIÓN	I.1.- Representantes de los medios de comunicación que cubren actividades del Instituto de Transparencia del Estado de Aguascalientes.	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Correo electrónico	
		3. Teléfono fijo o celular	
		4. Datos de identificación	
	I.2.- Registro de participantes para el Concurso de Nueva Imagen Gráfica del ITEA	1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros).	
		2. Correo electrónico	

		3. Datos personales contenidos en la identificación oficial presentada por la persona física	
		4. Teléfono fijo o celular	
		5. Domicilio	
J. UNIDAD DE TRANSPARENCIA	J.1.- Solicitudes de información		
	J.2.- Solicitudes de derechos ARCO		
	J.3.- 0rientación y auxilio a la sociedad civil (CAS)		

El Instituto de Transparencia del Estado de Aguascalientes, identifica de los datos personales las amenazas, riesgos y vulnerabilidades respecto de las medidas de seguridad con las cuales se cubren esos riesgos; por tanto, se ha generado un análisis de brecha de las medidas de seguridad con las que el Instituto cuenta y todas aquellas nuevas que puedan implementarse.

El identificar los riesgos nos permite resolver los problemas de seguridad antes de que éstos sucedan, esto significa que debe de ejecutarse bajo un enfoque proactivo y no de manera reactiva; una vulnerabilidad se considera una debilidad en la seguridad de los datos personales; aunque en sí misma no causa daño, puede afectar a algún dato cuando se aprovecha o explota por alguna amenaza.

De las vulnerabilidades más importantes que pudieran suscitar serían el robo y/o extravío de información o copia, la pérdida o destrucción de información, el uso, acceso o tratamiento indebido y el daño, alteración o modificación sin autorización previa. Estás pueden clasificarse como sigue:

a. Amenazas Directas, que son las que amenazan directamente el cumplimiento de nuestras expectativas, las cuales pueden ser Ataques, los cuales tienen un motivo principal, ya sea económico o criminal. Accidentes, eventos naturales como sismo o lógicas como fallas en hardware de los equipos y Errores, los cuales pueden ser defectos de configuración, programación o falla de software.
b. Amenazas secundarias, son aquellas que aminoran los efectos de las medidas de seguridad con que se cuenta para eliminar las amenazas, por ejemplo, defectos en los firewalls, antivirus, etc.

c. Amenazas primarias, estas inhiben las medidas de seguridad establecidas para eliminar amenazas directas o secundarias, por ejemplo, la falta de implementación de medidas de seguridad.

El análisis de riesgo tiene como objetivo asegurar la protección de los datos personales que se traten en el Instituto de acuerdo a las actividades que se realizan en el mismo, cada vez con mayor complejidad, pues para anticiparse y prepararse para los nuevos retos del día a día, lo recomendable es tener una responsabilidad proactiva ante el tratamiento de los datos personales gestionando los riesgos y el impacto que estos podrían generar.

En ese sentido, la gestión de riesgos, consiste en implementar un conjunto de acciones definidas con el propósito de controlar la probabilidad de consecuencias o impactos que una actividad puede tener sobre los datos personales que posee el Instituto, los cuales han de ser protegidos, pues se pretende garantizar el servicio público que se otorga, por lo que debe de identificarse la naturaleza, ámbito y fines de los tratamientos de datos personales, para poder detectar los niveles de posible vulnerabilidad de la información.

Análisis de brecha

El análisis de brecha aquí se enfoca en identificar las deficiencias en las prácticas de la organización en relación con las normativas de protección de datos y las mejores prácticas del sector.

Ejemplo de Análisis de Brecha para Protección de Datos Personales:

Área de Protección de Datos	Estado Actual	Estado Deseado	Brecha Identificada
Consentimiento del usuario	Falta de consentimiento explícito en algunos procesos	Consentimiento informado y explícito para todo uso de datos	Procesos de recolección de datos sin consentimiento explícito
Cifrado de datos personales	Los datos en reposo no están cifrados	Cifrado completo de los datos tanto en tránsito como en reposo	Falta de cifrado en bases de datos que contienen datos personales
Gestión de derechos de los usuarios	No se cuenta con un sistema automatizado para atender solicitudes de acceso, rectificación y supresión de datos	Sistema automatizado para atender las solicitudes de derechos de los usuarios (ARCO)	Procesos manuales y sin trazabilidad para gestión de derechos ARCO
Registro de incidentes de seguridad	No existe un registro centralizado de incidentes de datos personales	Registro automatizado de todos los incidentes de seguridad	Falta de un sistema de registro y reporte de incidentes de seguridad

Área de Protección de Datos	Estado Actual	Estado Deseado	Brecha Identificada
		relacionados con datos personales	
Transferencia de datos a terceros	Falta de controles para auditar transferencias de datos personales a terceros	Controles estrictos para transferencias seguras y auditables	Transferencias de datos a terceros sin controles de seguridad
Política de retención de datos	No existe una política clara de retención y eliminación de datos personales	Implementar una política clara de retención y eliminación de datos	Datos personales almacenados indefinidamente sin justificación

Explicación:

- **Estado Actual**: Describe la situación actual de la organización respecto a la protección de datos personales.
- **Estado Deseado**: Lo que se busca lograr según las normativas o mejores prácticas.
- **Brecha Identificada**: Indica la diferencia entre lo que se tiene y lo que se requiere, revelando las áreas de mejora.

Las medidas con las que actualmente cuenta el Instituto de Transparencia del Estado de Aguascalientes son:

- Se tiene una capacitación básica sobre el tratamiento de datos personales. Asistencia a los talleres de capacitación sobre el uso adecuado de los datos personales.

- La existencia de trazabilidad y posibilidad de identificar quien tuvo acceso a los datos y los tratamientos realizados.
- Se cuenta con Aviso de Privacidad integral y simplificado del ITEA.
- Los equipos personales cuentan con contraseñas de seguridad.
- Prohibición del uso en el Instituto de software ilegal o no autorizado.
- Monitorización del tráfico y las actividades en la red del Instituto para descubrir cualquier comportamiento anómalo, tales como virus, descarga de contenido inapropiado, fugas de información, etc.
- Uso de firewall para filtrar ataques al sistema.
- Generar respaldo de información de los equipos del Instituto en el servidor de la misma.
- El SITE cuenta con las medidas de seguridad para la su protección y resguardo.
- Uso de contraseñas para el acceso a los sistemas informáticos.
- Servidor resguardado en el SITE del Instituto.
- Borrado seguro de la información que reside en los equipos de cómputo.

- Inclusión de cláusula de confidencialidad de información en los contratos de servicios informáticos.
- Se cuenta un sistema de video vigilancia dentro de todas las áreas.
- Se requiere permiso del superior jerárquico para sacar quipos informáticos del Instituto.

Las medidas que aún falta de implementar en el Instituto de Transparencia del Estado de Aguascalientes son:

- Los equipos personales cuentan con contraseñas de seguridad: Se implementan reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades.
- Emisión de guía con recomendaciones para la creación y mantenimiento de contraseñas seguras, así como medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender, ejemplo cerrar cesión, bloquear equipo automáticamente cuando no se usa por periodos de tiempo, etc.
- Se habilitarán en los equipos del Instituto un perfil de usuario y el perfil de Administrador de los equipos está a cargo del Departamento de Sistemas Informáticos y Plataforma Digital.
- Bitácora de control de software contra virus y software malicioso.
- El SITE cuente con accesos controlado.
- Eliminación de fuentes de humedad, cuidado de temperatura interna del SITE y uso de protocolos en caso de desastres naturales.
- Ubicación del ciclo de vida de los datos personales para la destrucción y borrado de datos personales.
- Contratar protección avanzada contra ransomware.

3.- En este Instituto se realizan las siguientes acciones para el cumplimiento de medidas de seguridad dentro de este Sujeto Obligado.

- Reduciendo los riesgos a los que se exponen los datos personales
- Manteniendo y protegiendo los activos del órgano garante.
- Reforzando los controles y medidas de seguridad
- Identificando y mejorando los controles de acceso en el diseño de sistemas.
- Controles de acceso: Limitar el acceso a los datos a los usuarios autorizados
- Cifrado: Cifrar los datos para protegerlos
- Contraseñas: Utilizar contraseñas robustas y no compartirlas con terceros
- Firewalls: Utilizar firewalls para bloquear el acceso a la red de usuarios no autorizados
- Actualizaciones: Realizar actualizaciones de seguridad
- Copias de seguridad: Realizar copias de seguridad
- Navegación segura: Navegar de manera segura

- Protección de dispositivos: Proteger el acceso a dispositivos y cuentas
- Protección de correo electrónico: Proteger el correo electrónico
- Aviso de Privacidad: Contar con un Aviso de Privacidad
- Regulación del archivo de trámite, a fin de que cuente con todo lo necesario en caso de contar con datos personales, sin que esto signifique realizar una clasificación de información.

Sin más por el momento, agradezco las atenciones que sirva prestar al presente y aprovecho la ocasión para enviarle un cordial saludo.

A T E N T A M E N T E

24/OCT/24.

LIC. EDUARDO DE JESÚS GALLEGOS SILVA
JEFE DEL DEPARTAMENTO DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO DE TRANSPARENCIA DEL ESTADO DE AGUASCALIENTES.

C.C.P. Archivo