DOCUMENTO DE SEGURIDAD DE LA AUDITORÍA SUPERIOR

Contenido	Página

PRESENTACIÓN

El presente documento tiene como objeto describir y dar cuenta de manera general las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Auditoría Superior del Estado para garantizar la confidencialidad de los datos personales que posee, con base en los artículos 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 29 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tamaulipas.

Para tal efecto, resulta pertinente precisar que la Auditoría Superior del Estado, es el órgano técnico de fiscalización, control y evaluación gubernamental del Congreso del Estado Libre y Soberano de Tamaulipas. Cuenta con personalidad jurídica y patrimonio propio; autonomía técnica y de gestión, en el ejercicio de sus atribuciones para decidir sobre su organización interna, funcionamiento y resoluciones en los términos que dispone la Ley de Fiscalización Superior y Rendición de Cuentas del Estado de Tamaulipas, y considerado sujeto obligado, según lo señalado por el artículo 3, fracción XXII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas; y el artículo 3, fracción XXVII de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tamaulipas.

En ese orden de ideas, el objetivo que tiene esta Auditoría Superior es el de fiscalizar las cuentas públicas, y auditar los ingresos, los egresos, el manejo, la custodia y la aplicación de fondos, recursos, deuda pública, y el destino y ejercicio de los recursos obtenidos de los organismos públicos.

Bajo ese tenor, la Unidad de Transparencia de la Auditoría Superior del Estado a través de un diagnóstico de las facultades y atribuciones de las Unidades Administrativas establecidas en el marco normativo aplicable, ha identificado los procedimientos que en el ámbito de su competencia involucran el tratamiento de los datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en que tratan los datos personales, las medidas de seguridad adoptadas y las Unidades administrativas responsables de su protección. En las siguientes páginas, se abordará cada uno de los elementos que debe contener el documento de seguridad, con base en lo establecido en el artículo 29 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tamaulipas.

OBJETIVO DEL DOCUMENTO DE SEGURIDAD

El documento de seguridad describe y da cuenta de las medidas de seguridad técnicas, físicas y administrativas adoptadas por este Órgano Técnico Fiscalizador, para garantizar la confidencialidad e integridad de los datos personales que posee, con el fin de que la Auditoría Superior del Estado cumpla con el tratamiento lícito, seguro y responsable de los mismos.

Es por ello que el presente documento tendrá los siguientes objetivos:

1. Promover el marco de trabajo necesario para la protección de los datos personales en posesión de la Auditoría Superior del Estado.

2. Cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas, así como también la normatividad que derive de los mismos.

3. Establecer los elementos y actividades de dirección, operación y control de los procedimientos que impliquen el tratamiento de datos personales a efecto de protegerlos de manera sistemática y continua.

4. Promover mejores prácticas en la protección de datos personales.

ALCANCE DEL DOCUMENTO DE SEGURIDAD

En atención a los deberes de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas, el documento de seguridad es aplicable para las siguientes unidades administrativas de esta Auditoría Superior del Estado que, en el ejercicio de sus atribuciones y funciones, traten datos personales.

Las unidades administrativas involucrados son:

Unidades Administrativas de la Auditoría Superior del Estado que llevan a cabo tratamiento de datos personales
Auditoría Especial para Gobierno del Estado.
Auditoría Especial para Ayuntamientos.
Auditoría Especial de Desempeño.
Auditoría Especial de Seguimiento.
Dirección General de Administración y Finanzas.
Dirección General de Asuntos Jurídicos.
Órgano Interno de Control.
Dirección de Auditoría a Obra Pública.
Dirección de Capacitación y Profesionalización.
Dirección de Procesos y Mejora.
Dirección de Control y Evaluación.

Bajo ese tenor, Dichas unidades administrativas se encuentran bajo estricta responsabilidad de administrar y custodiar los datos personales que traten, ya sea en medios electrónicos, en espacios físicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Asimismo, en virtud de que uno de los objetivos de este Documento de Seguridad es cumplir con las obligaciones establecidas en la normatividad mencionada, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento, “quedando exceptuados de la aplicación, que correspondan al cumplimiento de las obligaciones de transparencia” a las que refieren el título Quinto de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Tamaulipas.

Asimismo, en virtud de que uno de los objetivos de este Documento de Seguridad es dar cumplimiento integral a las obligaciones establecidas en la normatividad aplicable, se atenderán en todo momento los principios, deberes y obligaciones de protección de datos personales a cargo del responsable del tratamiento de datos personales, el cual deberá elaborar la versión pública correspondiente de dicha información.

MARCO NORMATIVO

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado de Tamaulipas.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas.
- Reglamento Interior de la Auditoría Superior del Estado.

INVENTARIO DE DATOS PERSONALES

Inventario de Datos Personales por parte de esta Auditoría Superior del Estado de Tamaulipas		
Unidad Administrativa	**Procedimientos de tratamiento de datos Personales**	**Clasificación de Datos Personales**
Auditoría Especial para Gobierno del Estado.	▪ Para la fiscalización superior de las cuentas públicas.	Datos Transferidos, identificativos, laborales, patrimoniales y de procedimientos administrativos.
Auditoría Especial para Ayuntamientos.	▪ Para la fiscalización superior de las cuentas públicas.	Datos Transferidos, identificativos, laborales, patrimoniales y de procedimientos administrativos.
Auditoría Especial de Desempeño.	▪ Para la evaluación de programas o políticas entidades públicas están cumpliendo sus objetivos.	Datos Transferidos, identificativos, laborales, patrimoniales y de procedimientos administrativos.
Auditoría Especial de Seguimiento.	▪ Para el proceso de seguimiento a Auditorías.	Datos Transferidos, identificativos, laborales, patrimoniales y de procedimientos administrativos.

Dirección General de Administración y Finanzas.	▪ Procesos administrativos y laborales que gestionan el ciclo de vida del personal.	Datos identificativos, laborales, sensibles.
Dirección General de Asuntos Jurídicos.	▪ Asuntos Jurídicos, Litigios y Actuaciones procesales.	Datos Transferidos, identificativos, laborales, patrimoniales y de procedimientos administrativos.
Órgano Interno de Control.	▪ Recepción de Declaraciones Patrimoniales y Procesos de Responsabilidades Administrativas.	Datos identificativos, laborales, patrimoniales, procedimientos administrativos.
Dirección de Auditoría a Obra Pública.	▪ Para la fiscalización superior de las cuentas públicas.	Datos Transferidos, identificativos, laborales, patrimoniales y de procedimientos administrativos.
Dirección de Capacitación y Profesionalización.	▪ Para el Registro de Capacitaciones.	Datos identificativos, laborales.
Dirección de Procesos y Mejora.	▪ Para la elaboración de Procesos administrativos internos y de auditoría externa	Datos identificativos.
Dirección de Control y Evaluación	▪ Para el seguimiento y evaluación de los resultados de auditoría	Datos identificativos.

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

En términos generales, todo servidor público de la Auditoría Superior del Estado que tenga bajo su resguardo información o sistemas que contengan datos personales, tiene la obligación de protegerla y tratarla lícitamente, en estricta congruencia con la normativa aplicable y el Reglamento Interno de la propia Auditoría Superior del Estado.

Los auditores especiales, directores generales, directores y jefes de departamento de la Auditoría Superior deben asegurarse de que el personal a su cargo y con acceso físico o automatizado a los repositorios de datos personales conozcan:

I. Las normas de seguridad que deben observarse para su tratamiento;

II. Sus atribuciones respecto a los sistemas de tratamiento;

III. Las responsabilidades que tienen, junto con la firma de la carta de responsiva y confidencialidad;

IV. Las consecuencias en caso de incumplimiento de las atribuciones, resguardo o la vulneración de los datos personales.

Involucrado/a	Funciones	Obligaciones
Persona responsable titular de la Unidad Administrativa	1. Promover la capacitación del personal de las áreas adscritas a la Unidad Administrativa, en materia de protección de datos personales. 2. Participar en la integración y actualización de los documentos normativos exigidos por la ley y demás disposiciones aplicables.	1.Difundir entre el personal de las áreas que integran la Unidad Administrativa los instrumentos normativos y demás disposiciones que, en materia de datos personales, emita el Comité de Transparencia. 2.Gestionar ante la Unidad de Transparencia las solicitudes de actualización al presente Documento de Seguridad que le requieran las áreas adscritas a su Unidad Administrativa. 3.Revisar y suscribir el documento de medidas de seguridad del área, así como las actualizaciones del mismo. 4.Informar a la Unidad de Transparencia de las vulneraciones de la seguridad de los datos personales que se hayan suscitado al interior de la Unidad Administrativa. 5.Coordinar junto con la persona responsable del proceso en el que se tratan datos personales y, con el apoyo de la Unidad de Transparencia, la asesoría u orientación que se brinde a las personas titulares respecto de las vulneraciones de la seguridad de los datos personales que se susciten.
Enlace Responsable encargado del proceso de tratamiento de datos personales	1.Coordinar las acciones tendientes al cumplimiento de los principios y deberes que rigen en la materia, durante el tratamiento de los datos personales recabados por el área. 2.Dirigir la adecuada elaboración y actualización del inventario de datos personales del área. 3.Establecer los canales de comunicación con la Unidad de Transparencia, para obtener asesoría u orientación sobre el tratamiento de datos personales que realiza.	1.Suscribir las solicitudes de actualizaciones al documento de medidas de seguridad del área, a raíz del tratamiento que realice el área y solicitar su gestión a la persona que funja como enlace responsable ante el Comité de Transparencia. 2.Revisar y suscribir el documento de medidas de seguridad del área, así como las actualizaciones del mismo. 3.Supervisar la integración del informe de las vulneraciones de la seguridad de los datos personales que se hayan suscitado en el área. 4.Coordinar las acciones de contención y/o mitigación ante la

	4.Aprobar la implementación o actualización de medidas de seguridad, así como el desarrollo o adopción de esquemas de mejores prácticas, conforme a las disposiciones legales aplicables. 5.Supervisar la adecuada elaboración y actualización de los instrumentos aprobados por el Comité de Transparencia, en torno al tratamiento de los datos personales que realice el área. 6.Las demás que deriven de las resoluciones emitidas por el Comité de Transparencia	vulneración de la seguridad de los datos que trate el área. 5.Coordinar junto con la persona que funge como responsable de la Unidad Administrativa, el apoyo de la Unidad de Transparencia, la asesoría u orientación que se brinde a las personas titulares respecto de las vulneraciones de la seguridad de los datos personales que se susciten. 6. Aquellas que sean determinadas por la persona titular de la Unidad Administrativa.
Personas responsables que resguarden información de datos personales.	1. Verificar el cumplimiento de los principios y deberes que rigen en la materia, durante el tratamiento de los datos personales recabados por el área. 2. Las demás que deriven de las resoluciones emitidas por el Comité de Transparencia.	1.Elaborar informes de las vulneraciones de la seguridad de los datos personales que se hayan suscitado. 2. Aquellas que sean determinadas por la persona titular de la Unidad Administrativa a la que se encuentre adscrita.
Personas usuarias	1. ejercitar su derecho ARCO	

DEL ANÁLISIS DE RIESGOS

Una de las actividades que se realizaron en la Auditoría Superior del Estado para establecer y mantener las medidas de seguridad en el tratamiento de los datos personales, fue realizar un análisis de riesgo, donde se consideraron las amenazas y vulnerabilidades existentes para los datos personales, entendiendo por riesgo la combinación de la probabilidad de un evento y su consecuencia desfavorable.

Este análisis sirve para identificar el riesgo inherente, en el tratamiento a que son sometidos los datos personales, al desarrollar las funciones de este Órgano Técnico de Fiscalización Superior, con respecto a la integridad de las personas. Tratándose de datos personales como activo, se definirá riesgo inherente como aquellos factores que le dan un valor significativo como para que cualquier persona no autorizada pudiera beneficiarse de ellos, causando un mayor impacto en los titulares y/o en sus derechos y libertades.

Debido a lo anterior, para realizar el análisis de riesgos de los datos personales objeto de tratamiento por parte de este Órgano Técnico de Fiscalización Superior, se aplicó un instrumento de clasificación que distingue tanto su origen como su naturaleza, conforme a lo siguiente:

A. Por su origen:
I. Datos personales provenientes de los entes sujetos de fiscalización:

Son aquellos que la Auditoría Superior del Estado recibe de los entes públicos y demás sujetos fiscalizables con motivo del ejercicio de sus facultades de revisión y fiscalización superior.

II. Datos personales internos de la Auditoría Superior del Estado:
Son aquellos recabados o generados por las unidades administrativas internas, principalmente por el área de Recursos Humanos y el Órgano Interno de Control, relativos al personal que labora o ha laborado en la institución, así como a procedimientos administrativos internos, en el ámbito de sus atribuciones.

B. Por su naturaleza:
Datos Personales: Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
De lo anterior, se identificó que se trabaja con dos categorías de datos personales: datos de identificación y datos sensibles. Para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, ya sea por transferencia o que se recaben directamente, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

De lo anterior se identificó que el tratamiento de datos personales por parte de este Órgano Técnico de Fiscalización Superior se concentra en dos categorías: datos personales de identificación y datos sensibles. Para determinar el nivel de riesgo asociado a dichas categorías, se evaluó la probabilidad e impacto de que, en cualquiera de las fases de su ciclo de vida, desde su obtención, ya sea cuando son transferidos por los entes sujetos de fiscalización o cuando se recaban directamente por esta Auditoría Superior, durante su almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación, se materialicen uno o más eventos que pudieran causar un daño a las personas titulares.

Por lo tanto, se consideraron como vulnerables de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

a) La pérdida o destrucción no autorizada;

b) El robo, extravío o copia no autorizada;

c) El uso, acceso o tratamiento no autorizado, o

d) El daño, la alteración o modificación no autorizada.

ANÁLISIS DE BRECHA

Identificados los activos relacionados con los datos personales, así como el haber elaborado el análisis de riesgos, se debe proceder al análisis de brecha con las medidas de seguridad implementadas.

Las medidas de seguridad administrativas, físicas y técnicas que actualmente se aplican en la Auditoría Superior del Estado para mantener la confidencialidad e integridad de la información, protegiendo los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado e impedir la divulgación no autorizada, son las siguientes:

Medidas de seguridad administrativas:

- Actualización de avisos de privacidad.
- Para mantener la integridad y vigencia de la información se realiza la actualización periódica de documentos que se encuentren en la página web.
- La Dirección de Tecnologías de la Información, recomienda a los usuarios, eliminar documentos que se encuentren en la papelera de reciclaje del escritorio, de los equipos de cómputo, a fin de no almacenar datos personales y en caso de no seguir esta recomendación, esta información será eliminada cuando el equipo reciba mantenimiento preventivo.
- Prevenir el acceso no autorizado a los expedientes que contengan datos personales.
- No difundir o compartir documentos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.
- Exhortar al personal sobre la implementación de medidas de seguridad y confidencialidad de los datos personales.

Medidas de seguridad físicas:

- Personal sólo autorizado para el acceso a los servidores, así como bitácoras de acceso.
- Acceso a las instalaciones sólo a personas autorizadas e identificadas.
- Cámaras de vigilancia en los pasillos de la institución.
- Alarmas de seguridad en las entradas de la Institución.
- Resguardo físico de la información en archiveros con llave.

- Los equipos de cómputo reciben mantenimiento preventivo a fin de verificar que funcionen correctamente los programas y antivirus instalados.
- No dejar dispositivos electrónicos a la vista.
- El cierre de la oficina y espacios físicos en donde se resguarden los documentos que contengan datos personales.

Medidas de seguridad técnicas:

- Asignación de usuarios y contraseñas por parte de la Dirección de Tecnologías de la Información para accesos a equipos de cómputo.
- Las contraseñas utilizadas deben ser difíciles de descifrar, con el fin de proteger la información.
- Evitar compartir contraseñas.
- La instalación de sistemas informáticos sólo lo realiza personal autorizado.
- Restricción en los accesos a sistemas informáticos.
- Realización de labores de mantenimiento, preventivo y correctivo a los equipos de cómputo.
- Procurar la utilización de una cuenta de correo electrónico institucional para fines relacionados con las actividades laborales, evitando remitir datos personales.
- No difundir, transmitir o compartir documentos electrónicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

PLAN DE TRABAJO

Conforme al análisis de brecha, es importante generar acciones que permitan la seguridad de la información, por lo que a continuación se presentan las siguientes actividades que se planean realizar, a fin de continuar con la protección de datos personales:

- Asignación de enlaces por parte de los titulares de las Unidades Administrativas.
- Celebración de reuniones de trabajo con los enlaces de las unidades administrativas, a efecto de identificar alternativas de solución técnicas, físicas y administrativas a desarrollar, cuando se presente alguna vulneración de los datos personales.
- Revisión de los inventarios de datos personales.
- Implementar mecanismos de divulgación y conocimiento de las medidas de protección de los datos personales, fortaleciendo una cultura de seguridad de la información.
- Elaborar cartas de confidencialidad para todos los que tengan acceso a los datos personales.
- Mantener actualizado el Documento de Seguridad.
- Implementar mecanismos o programas tecnológicos para garantizar el blindaje frente a las amenazas que se presenten en materia de ciberseguridad.
- Revisión de las medidas de seguridad señaladas en el Documento de Seguridad.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

De manera permanente, se revisará el cumplimiento de las medidas de seguridad implementadas para la protección de los datos personales. Esta revisión estará a cargo de la Unidad de Transparencia, auxiliada por los enlaces designados de las unidades administrativas involucradas en el tratamiento de los datos personales, así como del Comité de Transparencia.

Para realizar la revisión de la aplicación de las medidas de seguridad, identificar posibles amenazas, vulnerabilidades o para evaluar la aplicación correcta o incorrecta de las mismas, se proponen los siguientes mecanismos de monitoreo:

- Identificación de amenazas por medio de una matriz de riesgo

- Realizar visitas a las unidades administrativas responsables del tratamiento de datos personales para verificar la aplicación de las medidas de seguridad aplicadas.

- Solicitar a los enlaces de datos personales, la revisión de las medidas de seguridad implementadas, así como la sugerencia de nuevas.

- Elaborar informes de vulneraciones donde los enlaces reporten al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales a través de la matriz de riesgo.

PROGRAMA GENERAL DE CAPACITACIÓN

Con el propósito de que las personas servidoras públicas de la Auditoría Superior del Estado conozcan, comprendan y se encuentren en condiciones de cumplir los principios, deberes y obligaciones en materia de protección de datos personales previstos en la normativa aplicable, se gestionará la capacitación correspondiente ante la instancia competente, para la impartición de cursos y actividades formativas conforme a la oferta institucional que se establezca.

En ese sentido, se integra al Programa Anual de Capacitación de la Auditoría Superior del Estado la inclusión de temas relativos a la protección de datos personales en posesión de sujetos obligados, transferencia de datos personales, ejercicio de los derechos ARCO y demás contenidos vinculados, cuya planeación, coordinación e implementación estará a cargo de la Dirección de Capacitación y Profesionalización, en el ámbito de sus funciones y competencias.