GUÍA PARA LA REVISIÓN Y CUMPLIMIENTO DE LOS PRINCIPIOS, DEBERES Y OBLIGACIONES SEÑALADOS EN LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS Y SUS LINEAMIENTOS.

INTRODUCCIÓN

La presente guía tiene por objeto establecer los procedimientos para cumplir con la regulación y protección de los datos personales en posesión de la Fiscalía General de la República en concordancia con los principios y deberes señalados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad que resulte aplicable.

Esta guía será de observancia general para todas las áreas responsables y personas servidoras públicas, al igual que para cualquier tratamiento de datos personales que obren en soportes físicos, electrónicos y mixtos dentro de las áreas responsables de la Fiscalía,

Todas las áreas responsables y personas servidoras públicas de la Fiscalía que intervengan en el tratamiento de datos personales, deberán garantizar la protección en el manejo de los mismos, por lo que no podrán comunicarlos a terceros, salvo en los casos previstos por la Ley General y demás normatividad que resulte aplicable en la materia; así mismo, no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de datos personales, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable; o bien que ello atienda a una obligación legal o a un mandato judicial, esto de conformidad con lo dispuesto en el artículo 22, fracción III de la Ley General.

Las áreas responsables y personas servidoras públicas de la Fiscalía que posean, por cualquier título, bases que contengan datos personales, deberán hacerlo del conocimiento de la Unidad de Transparencia y Apertura Gubernamental (**UTAG**), quien coadyuvará para mantener el registro actualizado de los sistemas de tratamiento datos personales en posesión de la Institución de conformidad con la Ley General y demás normatividad que resulte aplicable en la materia.

La aplicación e interpretación de esta guía se hará conforme a lo dispuesto en la Ley General, sus Lineamientos, así como las resoluciones y determinaciones vinculantes que emita el Instituto Nacional de Trasparencia, Acceso a la Información Pública y Protección de Datos Personales (**INAI**), favoreciendo en todo momento la protección más amplia a las personas, el derecho a la protección de datos personales y atendiendo a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Finalmente, es importante señalar que los casos no previstos por esta guía serán resueltos por el Comité de Transparencia.

GLOSARIO

Además de las definiciones contenidas en los artículos 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 2, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, para efectos de este documento se entenderá por:

Área interna: Aquella que cumple de forma directa con el documento de seguridad de un sistema de tratamiento de datos personales específico.
Área responsable: Aquella área de la Fiscalía que maneja un sistema de tratamiento y gestión de datos personales.
Áreas: Áreas de la Fiscalía General de la República.
Comité de Transparencia: Órgano colegiado de la Fiscalía General de la República, referido en el acuerdo quinto del Acuerdo A/072/16, por el que se crea la Unidad de Transparencia y Apertura Gubernamental de la Procuraduría General de la República y se conforma el Comité de Transparencia; instancia a la que hace referencia los artículos 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Documento: Documento de Seguridad.
DOF: Diario Oficial de la Federación.
Enlace de Datos Personales: Aquel que se vincula con el cumplimiento de los principios y deberes respecto a todos los sistemas de tratamiento de datos personales de las áreas responsables y sus áreas internas.
Fiscalía: Fiscalía General de la República.
INAI: Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Lineamientos: Lineamientos Generales de Protección de Datos Personales para el Sector Público.
Oficial de Protección de Datos Personales: Especialista en materia de protección de Datos Personales, que tiene la atribución de asesorar a las áreas del Sujeto Obligado y hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable.
Responsable de monitoreo: Persona responsable del monitoreo de las medidas de seguridad existentes.
Subenlace de Datos Personales: Especialista en los sistemas de tratamiento de datos personales de las áreas internas.
UTAG: Unidad de Transparencia y Apertura Gubernamental.

PRINCIPIOS Y DEBERES

- **Principios**

El tratamiento de datos personales que realicen las áreas de la Fiscalía deberá regirse por los principios, deberes y obligaciones previstos en la Ley General, sus Lineamientos y demás disposiciones que otorguen la protección más amplia a sus Titulares.

En función de dar cumplimiento a las obligaciones en materia de protección de datos, las áreas deberán dirigir sus acciones conforme a los principios de licitud, finalidad, lealtad, consentimiento, proporcionalidad, información y responsabilidad.

Cabe señalar que, de conformidad con el artículo 20 de la Ley General, en los casos en que las áreas de la Fiscalía recaben y den tratamiento a datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, la obtención del consentimiento se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable y demás disposiciones que al respecto emita la Fiscalía.

En el caso de los formatos que requisiten los menores de edad o personas en estado de interdicción, y que sean recabados de manera personal, el aviso de privacidad deberá especificarse la finalidad para la que se recaban los mismos. En todo caso, se deberá privilegiar la mayor protección hacia sus derechos a opinar o tomar sus decisiones, según sea el caso.

En cuanto al tratamiento de datos personales de personas menores de edad, el área correspondiente deberá considerar, además de la Ley General de los derechos de niñas, niños y adolescentes, lo siguiente:

a) Se deberá privilegiar el interés superior de niñas, niños y adolescentes en términos de las disposiciones legales aplicables;
b) Las niñas, niños y adolescentes tienen derecho a la protección de sus datos personales; y
c) Las personas menores de edad no podrán ser objeto de divulgaciones o difusiones ilícitas de información o datos personales, incluyendo aquélla que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación.

En consecuencia, las áreas adoptarán las medidas necesarias a efecto de que, en los expedientes de los procedimientos administrativos de cualquier índole, los datos personales de las personas menores de edad se resguarden de tal manera que se preserve su identificación y su derecho a la intimidad.
Aunado a lo anterior, los sujetos obligados sólo podrán acceder a los datos de las personas menores de edad, cuando sea estrictamente necesario para el ejercicio de sus funciones.

Ahora bien, para cumplir con el principio de responsabilidad, el área deberá acreditar el apego a los principios, deberes y obligaciones establecidos en la Ley General y demás normatividad aplicable, así como implementar los mecanismos previstos en el artículo 30 de la referida Ley. Asimismo, deberá rendir cuentas sobre el tratamiento que realiza a los datos personales en su posesión al titular y al INAI.

- **Deberes**

En función de dar cumplimiento a las obligaciones en materia de protección de datos, las áreas responsables deberán dirigir sus acciones conforme a los deberes de seguridad y confidencialidad, además deberán informar, sin dilación alguna al titular de los datos, las vulneraciones que ocurran, conforme a lo previsto en el artículo 41 de la Ley General, esto en cuanto confirme que ocurrió la vulneración y una vez que hubiere empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación.

Lo anterior, a fin de que los titulares afectados, puedan tomar las medidas correspondientes para la defensa de sus derechos.

Además, las áreas deberán hacer del conocimiento a la UTAG a través de su Enlace, las vulneraciones a que se refiere el párrafo anterior, al mismo tiempo que notifiquen a los Titulares de las áreas, a efecto de que dicha Unidad informe lo conducente al INAI.

Para dar cumplimiento con lo expresado, la UTAG implementará un Documento de Seguridad Institucional en el que quedarán documentadas y contenidas las medidas de seguridad implementadas por las áreas para proteger los datos personales contra daño, pérdida, alteración destrucción; o uso, acceso o tratamiento no autorizado, esto mediante la recopilación de los documentos de seguridad, y sus actualizaciones, elaborados por cada área.

DOCUMENTO DE SEGURIDAD

El documento de seguridad es aquel que tiene como propósito identificar los sistemas de datos personales que posee cada área de la Fiscalía, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Dicho documento deberá ser elaborado por el área que, conforme a los dispuesto en la Ley General, realice cualquier tipo de operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y deberá contener las medidas de seguridad administrativas, físicas y técnicas aplicables a sus sistemas de datos personales con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen. Así mismo, deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de las áreas, así como para las personas externas que debido a la presentación de un servicio tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

Además de lo previsto en el párrafo anterior, el documento deberá ser actualizado en caso de que ocurra alguno de los siguientes eventos:

a) En caso de que exista una implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
b) Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad; y

c) Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.

De conformidad con lo anterior, se considerarán medidas de seguridad:

a) **Administrativas**: aquellas que hacen alusión 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.
b) **Físicas:** aquellas de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
c) **Técnicas:** aquellas que abarcan el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

El documento de seguridad debe tener un contenido básico, acatando lo establecido en el artículo 35 de la Ley General, por lo cual el área de la Fiscalía que lo elabore debe cuidar que contenga, al menos, la siguiente información:

1. Inventario de los datos personales y de los sistemas de tratamiento;
2. Funciones y obligaciones de las personas o áreas que traten los datos personales;
3. Análisis de riesgo;
4. Análisis de brecha;
5. Un plan de trabajo; y
6. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

- **Inventario de datos personales y de los sistemas de tratamiento**

Para la elaboración del inventario de datos personales y de los sistemas de tratamiento se deberá incluir la siguiente información:

a) El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
b) Las finalidades de cada tratamiento de datos personales;
c) El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
d) El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
e) La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
f) En los casos aplicables, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable; y
g) En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.

Dentro del inventario se incluirá el **ciclo de vida de los datos personales**, conformado por lo siguiente:

a) La obtención de los datos personales;
b) El almacenamiento de los datos personales;

c) El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
d) La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
e) El bloqueo de los datos personales, en su caso, y
f) La cancelación, supresión o destrucción de los datos personales.

Es importante señalar que, por cancelación, supresión o destrucción de los datos personales, se hace referencia a aquella medida de seguridad mediante la cual se establecen métodos y técnicas para el borrado definitivo de los datos personales, de modo que la probabilidad de recuperarlos sea mínima[1].

- **Funciones y obligaciones de las personas o áreas que traten los datos personales**

Se definirán las funciones, y obligaciones de cada servidor público que trate datos personales por unidad administrativa, además, se comunicará a cada uno de estos la información antes señalada, y se buscará su capacitación constante en la materia.

- **Análisis de riesgo**

El análisis de riesgo se elaborará tomando en cuenta:

a) Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
b) El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
c) El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
d) Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;
e) El riesgo inherente a los datos personales tratados, contemplando su ciclo de vida, las amenazas y vulnerabilidades existentes y los recursos o activos involucrados en su tratamiento;
f) Las transferencias de datos personales que se realicen;
g) El número de titulares;
h) Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
i) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

- **Análisis de brecha**

El análisis de brecha se realizará comparando las medidas de seguridad existentes y efectivas con las faltantes en la organización del responsable, considerando lo siguiente:

a) Las medidas de seguridad existentes y efectivas;
b) Las medidas de seguridad faltantes, y
c) La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

[1] *"Guía para el Borrado Seguro de Datos Personales"*, Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), Primera Edición, junio de 2016, 36 págs.

- **Plan de trabajo**

En lo referente al plan de trabajo, éste se elaborará después de contar con el análisis de riesgo y de brecha, priorizando las medidas de seguridad más relevantes y urgentes, considerando los recursos designados; el personal interno y externo en su organización, y estableciendo fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

- **Mecanismos de monitoreo y revisión de las medidas de seguridad**

Se estipularán mecanismos de monitoreo y revisión de manera periódica de las medidas de seguridad existentes y efectivas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente:

a) Los nuevos activos que se incluyan en la gestión de riesgos;
b) Las modificaciones necesarias a los activos;
c) Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
d) La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
e) Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
f) El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
g) Los incidentes y vulneraciones de seguridad ocurridas.

El modelo del Documento de Seguridad deberá ser generado a partir de lo dispuesto en los Lineamientos de Protección de Datos Personales y las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidas por el INAI, el cual será responsabilidad de la UTAG, que a su vez estará encargada de su actualización y divulgación al interior de la Fiscalía.

En cuanto a las **vulneraciones** al sistema de tratamiento de datos personales, además de las contempladas del artículo 37 al 41 de la Ley General, se considerarán 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.

Aunado a lo anterior, las áreas en sus respectivos ámbitos de competencia deberán llevar un registro de las vulneraciones a la seguridad de los datos personales. Dicho registro será parte del mismo documento y, en el apartado correspondiente, deberán ser descritas:

1. La vulneración;
2. La fecha en la que ocurrió;
3. El motivo de la misma;
4. Las acciones correctivas implementadas de forma inmediata y definitiva; y
5. Las acciones preventivas que, en su caso, puedan ser implementadas para evitar vulneraciones posteriores.

Con la finalidad de dar cumplimiento a las obligaciones en materia de Datos Personales, las áreas de la fiscalía deberán actualizar su documento de seguridad de manera **trimestral**, haciendo del conocimiento del Oficial de Protección de Datos de la UTAG, mediante el correo electrónico correspondiente:

a) Si ha ocurrido algún cambio en la lista de servidores públicos que participan en el tratamiento de los datos personales (bajas o nuevos ingresos);
b) Los resultados del análisis de brecha realizado en el trimestre correspondiente;
c) Los avances en el plan de trabajo para la protección de los datos personales;
d) Los resultados del monitoreo y revisión de las medidas existentes y efectivas y, en su caso, de las medidas implementadas; y en su caso
e) Las vulneraciones ocurridas a los datos personales durante el trimestre correspondiente.

Las acciones antes mencionadas deberán ser realizadas por aquella persona que haya sido designado por el Enlace de Datos Personales como el responsable del monitoreo y revisión de las medidas en el documento de Seguridad.

INTERVINIENTES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Fungirán como intervinientes en el cumplimiento de la Ley General y demás normatividad que resulte aplicable en la materia:

a) Comité de Transparencia;
b) Oficial de Protección de Datos Personales (UTAG);
c) Las áreas responsables; y
d) Enlace y Subenlace de Datos Personales.

Para estos efectos, el **Comité de Transparencia**, de conformidad con lo dispuesto en el artículo 84, fracciones I, IV y V de la Ley General, coadyuvará en:

a) La aprobación del Documento de Seguridad;
b) Aprobar las actualizaciones trimestrales que la UTAG le hace llegar por parte de las áreas de la Fiscalía sobre las actividades realizadas por las áreas en materia de protección de datos personales (inventario de datos personales, análisis de riesgo, análisis de brecha, medidas de seguridad, plan de trabajo y mecanismos de monitoreo y revisión de las medidas de seguridad.);
c) Conocer el registro actualizado de las bases de datos personales de la Institución.

El **Oficial de Protección de Datos Personales**, adscrito a la UTAG, de conformidad con lo dispuesto en el artículo 85 de la Ley General y las funciones que le atribuye el artículo 122 de los Lineamientos Generales, coadyuvará de la siguiente manera:

a) Monitorear los avances o cambios legislativos en materia de privacidad y protección de datos personales;
b) Identificar, implementar y promover la adopción de esquemas de mejores prácticas;
c) Vigilar los programas de capacitación;
d) Asesorar a las áreas en materia de protección de datos personales;
e) Verificar el cumplimiento, incluida la gestión de las actividades internas de la protección de datos personales;

f) Identificar las áreas o prestadores de servicios que dentro la Fiscalía, hacen un tratamiento de datos personales;
g) Dialogar con los responsables de estos sistemas de gestión de datos para conocer e identificar los aquellos que se tratan y el tipo de tratamiento que se realiza, lo anterior con la finalidad de identificar a las diferentes personas que intervienen a lo largo del proceso;
h) Conocer de las prácticas de recopilación y gestión de datos que tienen las áreas, esto a través del Taller de Documento de Seguridad; así se podrá identificar los posibles riesgos que puedan afectar la seguridad de los datos personales y las medidas que actualmente se encuentran implementadas para su protección, con lo cual se identificará, formalizará o creará el análisis de riesgo y brecha;
i) Definir las funciones y obligaciones de las personas que realizan el tratamiento de los datos personales, con la finalidad de garantizar que éste se realice de tal manera que dé cumplimiento a los principios, deberes y obligaciones que establece el marco en materia de protección de datos; y
j) Presentar al Comité de Transparencia, cada trimestre, el desempeño de las actividades realizadas por las áreas en materia de protección de datos personales en la Fiscalía.

Las **áreas responsables**, con la finalidad de dar cumplimiento a lo establecido en la Ley General, los Lineamientos y demás normatividad aplicable, coadyubarán con lo siguiente:

a) Coordinar la atención de las observaciones, recomendaciones y/o requerimientos que resulten de las verificaciones internas realizadas por la UTAG, a través del Oficial de Protección de Datos Personales;
b) Coordinarse internamente para el envío de la información a la UTAG a través de su enlace y subenalces correspondientes; y
c) Implementar acciones de control o mecanismos administrativos, técnicos y físicos, que permitan proteger los datos personales, conforme lo establecido en la Ley General y sus Lineamientos.

Asimismo, las áreas responsables, para el debido cumplimiento de los principios y deberes respecto a todos sus sistemas de tratamiento de datos personales, deberán atender las disposiciones que emita el INAI, lo previsto en la Ley General, sus Lineamientos y demás ordenamientos que se deriven de ésta.

Para el cumplimiento de lo señalado en el párrafo anterior, se contará con el apoyo de un **área interna**, misma que coadyuvará de la siguiente manera:

a) Actualizar y validar la información registrada en el documento de seguridad, conforme a los criterios establecidos en la Ley General y demás ordenamientos que se deriven de ésta, a través de su enlace de Datos Personales;
b) Integrar la información en el(os) formato(s) establecidos;
c) Informar a través del correo electrónico cualquier incidencia o cambio ocurrido en su sistema de tratamiento de datos personales; y
d) Atender las observaciones, requerimientos y/o recomendaciones, como resultado de la verificación interna que realice la UTAG.

Por su parte, el **enlace de datos personales** coadyuvará de la siguiente manera:

a) Atender las observaciones, requerimientos y/o recomendaciones, como resultado de la verificación interna que realice la UTAG;
b) Establecer los procedimientos internos necesarios para solicitar a las áreas internas que poseen sistemas de tratamiento de datos personales en el ejercicio de sus facultades, competencias y funciones;
c) Informar a las áreas internas, cuando existan inconsistencias en la información que enviaron;
d) Informar a la UTAG, a través del correo electrónico gestion.datospersonales@fgr.org.mx cuando un área en específico no cumpla en tiempo y forma los requerimientos que le formule;
e) Informar a través del correo electrónico señalado, cuando no hay información que deba reportarse en el periodo de actualización correspondiente;
f) Recabar la información enviada por las áreas internas; y
g) Aquellas que en el devenir del procedimiento surjan y no estén normadas, previo aviso de la UTAG.

El **subenlace de datos personales,** siendo una figura de apoyo para el enlace, colaborará proporcionándole a este último la información particular sobre el sistema de tratamiento de datos del que es especialista, lo anterior con la finalidad de proporcionar al enlace el conocimiento necesario y poder determinar las brechas de seguridad que puedan existir.

Resulta importante señalar que, en caso de llegar a faltar el enlace de Datos Personales, el subenlace asumirá sus funciones, es decir, deberá reportar al Titular del área y a la UTAG, de manera trimestral, las actualizaciones en el inventario de datos, las medidas de seguridad, el plan de trabajo y los mecanismos de monitoreo de las medidas de seguridad. Lo anterior con la finalidad de que, en tanto se asigna a un nuevo enlace de protección de datos personales, no se pierda la continuidad en el trabajo realizado por el área.

PLAZOS PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

Los enlaces y subenlaces de Protección de datos personales de las diferentes áreas que elaboren su documento de seguridad deberán tomar el curso de ***Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDDPSO)*** y, posteriormente, el ***Curso de Documento de Seguridad***, ambos con una duración de 5 horas cada uno.

Una vez que hayan concluido los cursos antes mencionados, el Oficial de Protección de Datos Personales de la UTAG se encargará de impartir el ***Taller para la elaboración de Documento de Seguridad***, durante el cual, asesorará y dará acompañamiento al enlace designado durante la elaboración del documento del área correspondiente. Dicho taller constará de 20 horas a lo largo de las cuales el área entregará los avances de su documento para revisión.

Transcurridos 10 días hábiles desde la finalización del taller, el área deberá enviar la **versión final** de su documento de seguridad para que la UTAG pueda revisarlo.

La UTAG contará con un plazo de 30 días hábiles para la revisión del documento, periodo en el cual se realizarán las modificaciones que a efecto sean oportunas. Cuando se hayan hecho las correcciones y haya transcurrido el plazo antes mencionado, la UTAG presentará ante el Comité de Transparencia el documento de seguridad para obtener su aprobación.

PLAZOS PARA LA ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Como se ha mencionado en diferentes ocasiones a lo largo de esta guía, las áreas deberán mantener actualizado su documento de seguridad conforme a la normatividad aplicable, para lo cual deberán entregar un reporte, en el que se indiquen los cambios ocurridos en cuanto a las medidas de seguridad, el plan de trabajo y los mecanismos de monitoreo, lo anterior siempre y cuando hayan ocurrido; si por el contrario no se realizaron cambios, también deberán hacerlo de conocimiento.

Esta actualización se llevará a cabo de forma trimestral, por lo que, al concluir este periodo, las áreas deberán enviar su reporte y actualización a la UTAG, quien someterá dichos documentos a validación del Comité de Transparencia en la sesión que se celebre en la tercera semana del mes siguiente a la conclusión del trimestre correspondiente. Una vez que los documentos actualizados hayan sido aprobados por el Comité de Transparencia, la UTAG se encargará de integrarlos al documento de seguridad institucional.

RESPONSABILIDADES Y SANCIONES

- **Responsabilidades**

En caso de vulneración ocurrida a los datos personales que sufren tratamiento, el responsable del monitoreo deberá informar al Enlace de Datos Personales y al Titular del área, para que estos a su vez, lo hagan de conocimiento al Oficial de Protección de Datos Personales de la UTAG. Así mismo, el Oficial deberá informar sobre la vulneración al INAI para que el órgano garante en comento pueda tomar las medidas necesarias.

- **Sanciones**

Debido a que la Fiscalía General de la República es un sujeto obligado competente en instancia de seguridad, procuración y administración de justicia, la información contenida en los documentos de seguridad de sus diferentes áreas es considerada de valor alto, por lo que se debe contar con las medidas de seguridad óptimas para garantizar su protección.

El valor de la información antes mencionada encuentra su fundamento en los artículos 55[2] y 56[3] de la Ley General de Responsabilidades Administrativas, que hacen referencia a la **información privilegiada**; tomando en cuenta el ordenamiento en comento, es importante señalar que éste fija las sanciones a las que los servidores públicos pueden ser acreedores por faltas administrativas graves, las cuales pueden van desde la suspensión o destitución

[2] *Ley General de Responsabilidades Administrativas.* **Título Tercero, Capítulo II "De las faltas administrativas graves de los Servidores Públicos". Artículo 55.** Incurrirá en utilización indebida de información el servidor público que adquiera para sí o para las personas a que se refiere el artículo 52 de esta Ley, bienes inmuebles, muebles y valores que pudieren incrementar su valor o, en general, que mejoren sus condiciones, así como obtener cualquier ventaja o beneficio privado, como resultado de información privilegiada de la cual haya tenido conocimiento.

[3] *Ley General de Responsabilidades Administrativas.* **Título Tercero, Capítulo II "Sanciones para los Servidores Públicos por Faltas Graves"**. **Artículo 56.** Para efectos del artículo anterior, se considera información privilegiada la que obtenga el servidor público con motivo de sus funciones y que no sea del dominio público. La restricción prevista en el artículo anterior será aplicable inclusive cuando el servidor público se haya retirado del empleo, cargo o comisión, hasta por un plazo de un año.

del empleo, una sanción económica o la inhabilitación temporal para desempeñar funciones en el servicio público[4].

Derivado de lo anterior, en caso de que ocurra una vulneración en cualquier paso del ciclo de vida del tratamiento de los datos personales, el responsable del monitoreo deberá informarlo al enlace o bien al Titular del área, e informar al titular de los datos personales para que para que estos puedan ejecutar las acciones necesarias para mitigar dicha vulneración.

[4] *Ley General de Responsabilidades Administrativas.* **Título Cuarto, Capítulo II "De las faltas administrativas graves de los Servidores Públicos"**. Del artículo 78 al 80 Bis.