FGR
FISCALÍA GENERAL DE LA REPÚBLICA

UTAG
UNIDAD DE TRANSPARENCIA Y APERTURA GUBERNAMENTAL

Documento de Seguridad

FISCALÍA GENERAL DE LA REPÚBLICA

Descripción de las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Fiscalía General de la República para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Oficina del Fiscal
Unidad de Transparencia y Apertura Gubernamental
2021 | AVENIDA INSURGENTES 20, ROMA NORTE, CUAUHTÉMOC, CIUDAD DE MÉXICO

INTRODUCCIÓN

La Constitución Política de los Estados Unidos Mexicanos, establece en su artículo 16, párrafo segundo, que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Particulares (LGPDPPSO), en el artículo 16, señala que el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Asimismo, en el artículo 82 de la LGPDPPSO se indica que los responsables de las bases de datos en posesión de instancias de procuración de justicia, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

De esta forma, la Ley prevé que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, las cuales deberán estar descritas en el documento de seguridad.

Este documento tiene como propósito contar con el **inventario** de los sistemas de datos personales en posesión de la Fiscalía General de la República (FGR), en sus diversas áreas administrativas, identificando el tipo de datos personales que cada uno contiene, los intervinientes, procedimientos, tecnologías aplicadas, así como todos los activos y elementos relacionados con el tratamiento de los datos personales. Asimismo, se relacionan las funciones y obligaciones de las y los servidores públicos que tratan los datos personales, a fin de determinar el nivel de participación durante el ciclo de vida de los datos.

A partir de la identificación de los activos, se realiza un **análisis de riesgos** por cada uno de los sistemas de datos personales, en los que se hace una valoración de los riesgos asociados a los mismos, atendiendo a las características del tratamiento.

Del resultado del análisis de riesgo, en el **análisis de brecha** se establecen las medidas necesarias para garantizar el nivel de seguridad y control adecuado que reduzca la exposición al riesgo. Además de la valoración del riesgo, en la selección de las medidas de seguridad, se tomaron en cuenta los costos estimados y los beneficios esperados con las mismas, de manera tal que se pueda obtener un riesgo residual aceptable.

La implementación de las medidas de seguridad se encuentra plasmada en el **plan de trabajo** establecido por cada una de las áreas. Posteriormente, se determinan los mecanismos

de monitoreo y revisión de las medidas de seguridad, a través de los cuales se evalúan y miden los resultados esperados, y en su caso implementar mejoras o sustituir los controles de seguridad que no estén funcionando.

Finalmente, se agrega el programa de **capacitación** general aprobado por el Comité de Transparencia de la FGR y presentado ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Este tiene como finalidad concientizar y capacitar al personal sobre sus obligaciones en materia de protección de datos personales atendiendo al nivel de intervención y a los perfiles de puestos.

El Documento de Seguridad debe mantenerse actualizado y ser de observancia obligatoria para todos los servidores públicos de la FGR. De igual forma, en el Documento de Seguridad se hace extensiva la responsabilidad de observancia a personas físicas o morales que presten un servicio a la FGR que implique un tratamiento de datos personales en cualesquiera de sus fases. Lo anterior debe estar claramente estipulado en las cláusulas de contratación de servicios con terceros ajenos a la institución.

Como parte del Consejo de Seguridad Nacional y del Sistema Nacional de Seguridad Pública y por la naturaleza de sus funciones sustantivas la FGR está obligada a mantener las más elevadas medidas de seguridad independientemente de la recolección de datos personales que realice, ya que su tarea toral es la procuración de justicia, y esto obliga a la institución a conducirse bajo un alto sigilo de reserva, con el fin de llevar a buen puerto la investigación y persecución de los delitos.

DEFINICIONES

Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.[1]

Amenaza: Circunstancia o condición externa, con la capacidad de causar daño a los activos explotando una o más de sus vulnerabilidades.[2]

Archivo: Al conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden.[3]

Archivo de concentración: Al integrado por documentos transferidos desde las áreas o unidades productoras, cuyo uso y consulta es esporádica y que permanecen en él hasta su disposición documental.[4]

Archivo de trámite: Al integrado por documentos de archivo de uso cotidiano y necesario para el ejercicio de las atribuciones y funciones de los sujetos obligados.[5]

Archivo histórico: Al integrado por documentos de conservación permanente y de relevancia para la memoria nacional, regional o local de carácter público.[6]

Análisis de riesgos: La evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño.[7]

Análisis de brecha: Identificar las medidas de seguridad existentes, las medidas de seguridad faltantes y si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados.[8]

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.[9]

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.[10]

Baja documental: Eliminación de aquella documentación que haya prescrito su vigencia, valores documentales y, en su caso, plazos de conservación; y que no posea valores históricos, de acuerdo con las disposiciones jurídicas aplicables.[11]

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.[12]

---

[1] http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf Consultado el 30 de julio de 2018
[2] http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf Consultado el 30 de julio de 2018
[3] Ley General de Archivos, artículo 4. (DOF 15-06-2018)
[4] *Ídem*
[5] *Ídem*
[6] *Ídem*
[7] http://inicio.inai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf Consultado el 30 de julio de 2018
[8] http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf Consultado el 30 de julio de 2018
[9] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26-01/2017)
[10] *Ídem*
[11] Ley General de Archivos, artículo 4. (DOF 15-06-2018)
[12] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26-01/2017)

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.[13]

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.[14]

Confidencialidad: Propiedad de la información para evitar su acceso, divulgación y revelación, no autorizados.[15]

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.[16]

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[17]

Datos personales 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 éste. 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.[18]

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.[19]

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.[20]

Disponibilidad: Propiedad de la información para ser accesible y utilizable cuando se requiera.[21]

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.[22]

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.[23]

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente

---

[13] *Ídem*
[14] *Ídem*
[15] http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf Consultado el 30 de julio de 2018
[16] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26-01/2017)
[17] *Ídem*
[18] *Ídem*
[19] *Ídem*
[20] *Ídem*
[21] http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf Consultado el 30 de julio de 2018
[22] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26-01/2017)
[23] *Ídem*

de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable.[24]

Incidente de seguridad: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.[25]

Integridad: Propiedad de la información para salvaguardar la exactitud y completitud de la información.[26]

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.[27]

Medidas de seguridad administrativas: 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.[28]

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. [29]

Medidas de seguridad técnicas: 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.[30]

Plazo de conservación: Periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.[31]

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.[32]

Responsable: Los sujetos obligados que deciden sobre el tratamiento de datos personales (en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos).[33]

Riesgo: Potencial o probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que éste cause un impacto negativo o daño.[34]

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.[35]

Titular: La persona física a quien corresponden los datos personales.[36]

---

[24] *Ídem*
[25] http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf Consultado el 30 de julio de 2018
[26] *Ídem*
[27] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26-01/2017)
[28] *Ídem*
[29] *Ídem*
[30] *Ídem*
[31] Ley General de Archivos, artículo 4. (DOF 15-06-2018)
[32] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26/01/2017)
[33] *Ídem*
[34] http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf Consultado el 30 de julio de 2018
[35] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3. (DOF 26/01/2017)
[36] *Ídem*

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.[37]

Tratamiento: Cualquier 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.[38]

Vulnerabilidad: Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

Vulneración de seguridad: Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento. De acuerdo con el artículo 38 de la LGPDPPSO, se consideran al menos las siguientes vulneraciones: (i) La pérdida o destrucción no autorizada; (ii) el robo, extravío o copia no autorizada; (iii) el uso, acceso o tratamiento no autorizado, o (iv) el daño, la alteración o modificación no autorizada.

[37] *Ídem*
[38] *Ídem*

MARCO JURÍDICO

Constitución Política de los Estados Unidos Mexicanos.

LEYES

Ley de la Fiscalía General de la República

Ley Federal de Archivos[39]

Ley General de Responsabilidades Administrativas.[40]

Ley Orgánica de la Administración Pública Federal.[41]

REGLAMENTOS
Reglamento del Servicio de Carrera de Procuración de Justicia Federal[42].

Reglamento de la Ley Orgánica de la Procuraduría General de la República[43].

NORMAS
Normas de organización y funcionamiento del Órgano Auxiliar de Instrucción del Consejo de Profesionalización de la Procuraduría General de la República[44].

LINEAMIENTOS
Lineamientos para analizar, valorar y decidir el destino final de la documentación de las dependencias y entidades del Poder Ejecutivo Federal.[45]

ACUERDOS VINCULANTES A LA FGR (antes PGR)
Acuerdo A/064/03 por el que se crea la Unidad Especializada para la Atención de Delitos Cometidos en el Extranjero o en los que se encuentren involucrados Diplomáticos, Cónsules Generales o Miembros de Organismos Internacionales acreditados en México, y se establecen sus funciones.[46]

Acuerdo A/004/10 por el que se establecen los lineamientos para el ofrecimiento y entrega de recompensas a personas que aporten información útil relacionada con las investigaciones y averiguaciones que realice la Fiscalía General de la República o que colaboren en la localización y detención de probables responsables de la comisión de delitos, y se fijan los criterios para establecer los montos de dichas recompensas.[47]

Acuerdo por el que se crea el Sistema de Registro de Detenidos relacionados con delitos de competencia de la Fiscalía General de la República (SIRED). [48]

[39] DOF el 23 de enero de 2012. Abrogada a partir del 15 de junio de 2019 por Decreto DOF de 15 de junio de 2018
[40] DOF el 18 de julio de 2016.
[41] DOF el 29 de diciembre de 1976. Última reforma 15 de junio de 2018.
[42] DOF el 26 de enero de 2005.
[43] DOF el 23 de julio de 2012, y su fe de erratas, publicada en el DOF el 21 de septiembre de 2012.
[44] DOF el 02 de febrero de 2004.
[45] DOF el 16 de marzo de 2016
[46] DOF el 24 de julio de 2003.
[47] DOF el 03 de febrero de 2010
[48] DOF el 24 de mayo de 2010

Acuerdo A/023/12 para regular la expedición de constancias de datos registrales de la Fiscalía General de la República y el procedimiento para realizar la cancelación o devolución de datos registrales, así como proporcionar información, constancias o certificaciones relativas a los mismos.[49]

Acuerdo A/101/13 por el que se crea la Agencia de Investigación Criminal y se establecen sus facultades y organización.[50]

Acuerdo A/001/16 publicado en el DOF, por el que se crea el Órgano Administrativo Desconcentrado Especializado en Mecanismos Alternativos de Solución de Controversias en Materia Penal de la Fiscalía General de la República.[51]

Acuerdo A/072/16, Unidad de Transparencia y Apertura Gubernamental de la Fiscalía General de la República. [52]

ACUERDO A/001/18 por el que se fortalece el Sistema de Atención Ciudadana VISITEL.[53]

Acuerdo A/013/18 por el que se crea la Fiscalía Especializada en Investigación de los Delitos de Desaparición Forzada y se establecen sus atribuciones.[54]

Acuerdo por el que se emiten las Disposiciones en las materias de Recursos Humanos y del Servicio Profesional de Carrera, así como el Manual Administrativo de Aplicación General en materia de Recursos Humanos y Organización y el Manual del Servicio Profesional de Carrera[55].

NORMATIVIDAD EN MATERIA DE PROTECCIÓN DATOS.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[56]

Lineamientos Generales de Protección de Datos Personales para el Sector Público.[57]

Ley General de Transparencia y Acceso a la Información.[58]

Ley Federal de Transparencia y Acceso a la Información Pública.[59]

MANUALES

Manual de Organización General de la Procuraduría General de la República[6061]. En términos de lo dispuesto en los transitorios Sexto, Noveno, fracciones III, IV y VI y Décimo Segundo, fracción II del Decreto por el que se expide la Ley Orgánica de la Fiscalía General de la República y su DECLARATORIA de entrada en vigor que le confiere Autonomía Constitucional.

[49] DOF el 09 de febrero de 2012
[50] DOF el 25 de septiembre de 2013. Última reforma 07 de diciembre de 2017.
[51] DOF el 15 de enero de 2016.
[52] DOF 11 de mayo de 2016.
[53] DOF 18 de enero de 2018
[54] DOF el 16 de febrero de 2018.
[55] DOF el 12 de julio de 2010. Última reforma 04 de febrero de 2016.
[56] DOF el 26 de enero de 2017.
[57] DOF el enero de 2018, última reforma 25 de noviembre de 2020.
[58] DOF el 04 de mayo de 2015; última reforma 20 de mayo de 2021.
[59] DOF el 09 de mayo de 2016. Última reforma 20 de mayo de 2021.
[60] DOF el 25 de noviembre de 2016.
[61] DOF el 25 de noviembre de 2016.

Manual de Trámites para el Otorgamiento de las Prestaciones del Personal de la Procuraduría General de la República[62], en términos de lo dispuesto en los transitorios Sexto, Noveno, fracciones III, IV y VI y Décimo Segundo, fracción II del Decreto por el que se expide la Ley Orgánica de la Fiscalía General de la República y su DECLARATORIA de entrada en vigor que le confiere Autonomía Constitucional. [63]

Manual administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicación. [64]

[62] Suscrito el 25 de octubre de 2012 y en vigor desde el 07 de noviembre de 2012.
[63] DOF el 14 de diciembre de 2018.
[64] DOF el 08 de mayo de 2014. Última reforma 04 de febrero de 2016.

OBJETIVO

El objetivo del documento de seguridad es describir y dar cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la FGR para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Las áreas administrativas de la FGR tienen el deber de identificar de manera continua las actividades de tratamiento de datos personales que realizan ligadas a los procesos establecidos para el desempeño de sus funciones, de tal forma que puedan estar en posibilidad de establecer acciones y controles de seguridad atendiendo al ciclo de vida del dato personal y a las disposiciones normativas aplicables.

Las acciones relacionadas con la seguridad de los datos personales en posesión de la FGR se encuentran plasmadas en este documento a fin de garantizar el derecho humano a la protección de los datos personales, en cumplimiento a la Ley y a los Lineamientos Generales de Protección de Datos Personales en el Sector Público.

ÁMBITO DE APLICACIÓN

El ámbito de aplicación del documento de seguridad refiere a los sistemas de datos personales que utilizan, tratan, administran, transfieren y/o preservan los servidores públicos adscritos a la FGR en el seno de sus competencias, funciones y responsabilidades.

Los servidores públicos que realizan un tratamiento de datos personales en cualquiera de sus fases están obligados a observar los principios rectores de la protección de datos personales. Estos principios son[65]:

Licitud	El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.
Finalidad	Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.
Lealtad	El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.
Consentimiento	El responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma libre, específica e informada.
Calidad	El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
Proporcionalidad	El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
Información	El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

[65] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículos del 16 al 30. (DOF 26/01/2017)

Responsabilidad	El responsable deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y al INAI.

REPORTE DE INCIDENTES TÉCNICOS

De acuerdo con los Lineamientos para la asignación y uso de los bienes y servicios de tecnologías de la información publicados en marzo de 2018 por la DGTIC, en su capítulo IV consigna que los usuarios de los bienes y servicios institucionales de TIC deberán reportar a la Mesa de Servicios Centralizada cualquier incidente o solicitud relacionada con éstos, dentro de las 24 horas posteriores al hecho.

Por cada reporte de algún incidente con los bienes y servicios institucionales de TIC, la Mesa de Servicios Centralizada, levantará un ticket a nombre del usuario, proporcionándole un número de identificación único con el que se dará seguimiento al incidente reportado hasta su solución.

Los incidentes que los usuarios reporten a la Mesa de Servicios Centralizada, de manera enunciativa son:

- Fallas técnicas del equipo de cómputo
- Fallas del correo electrónico
- Soporte técnico
- Mantenimiento correctivo de software

Para obtener el ticket de servicio, los usuarios deberán proporcionar: nombre, teléfono, correo electrónico institucional, inmueble, unidad administrativa de adscripción y puesto. Es importante destacar que para el adecuado registro de un incidente en un equipo informático deberá proporcionar marca (fabricante), modelo y el número de serie del equipo.

MEDIDAS DE SEGURIDAD

Oficina del Fiscal

Unidad de Transparencia y Apertura Gubernamental

Solicitudes de Acceso a la Información Pública y de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de Datos Personales, así como de Recursos de Revisión y Denuncias por incumplimiento de obligaciones de transparencia, que se presenten directamente ante la Unidad de Transparencia y Apertura Gubernamental o a través de la Plataforma Nacional de Transparencia.

Unidad Administrativa	Nombre del Sistema de Datos Personales	Responsable del sistema de datos personales y cargo
Unidad de Transparencia y Apertura Gubernamental (UTAG)	**Solicitudes de Acceso a la Información, Capacitación, Sistema de Portales de Obligaciones de Transparencia (SIPOT)**	[redacted] **Titular de la UTAG** [redacted] **Director de Acceso a la Información** [redacted] **Director de Protección de Datos Personales y Capacitación**

I. Inventario de datos personales	
1. Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales	**SOLICITUDES DE ACCESO Y DERECHOS ARCOP** **Físicos:** ● Escrito libre por parte del peticionario. ● Presencial en el Módulo de Atención Ciudadana de la UTAG. **Electrónicos:** ● Plataforma Nacional de Transparencia (PNT), Sistema de Solicitudes de Acceso a la Información (SISI y SISAI 2.0). ● Correo electrónico leydetransparencia@pgr.gob.mx, derechos.arco@pgr.gob.mx. **CAPACITACIÓN** **Físicos:** ● Oficios generados por las áreas que conforman la Fiscalía General de la República (FGR). ● Oficios generados por los servidores públicos de la FGR. ● Listas de asistencia, evaluaciones y encuestas de los cursos presenciales. **Electrónicos:** ● Correo electrónico miguel.fitta@pgr.gob.mx y/o norma.carrillo@pgr.gob.mx. ● Formulario web para el registro de asistencia y evaluación del curso en línea. ● Mediante reporte en archivo Excel que se solicita al INAI cada trimestre de los servidores públicos que realizan personalmente su registro al CEVINAI **SISTEMA DE PORTALES DE OBLIGACIONES DE TRANSPARENCIA (SIPOT)** **Físicos:** ● Oficios generados por las áreas administrativas, solicitando se genere usuario para el uso del SIPOT y/o uso de la herramienta Blob Storage. ● Oficios generados por las áreas administrativas que conforman la FGR solicitando apoyo para revisión de la información que se carga en la PNT. **Electrónicos:**

	● Sistema de Portales de Obligaciones de Transparencia (SIPOT) ● Archivos en formato Excel, PDF, WORD. ● CD/DVD ● Compartidos por One drive. ● Correo electrónico miguel.fitta@pgr.gob.mx y/o norma.carrillo@pgr.gob.mx.
2. Finalidades del tratamiento	**SOLICITUDES DE ACCESO Y DERECHOS ARCOP** 1. Orientar y dar seguimiento a las solicitudes manuales presentadas en el Módulo de Atención Ciudadana de la UTAG. 2. Orientar sobre el procedimiento para presentar solicitudes de información o de datos personales ante la Fiscalía General de la República, así como el procedimiento para ejercer los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (**ARCOP**). 3. Facilitar la captura de solicitudes de información o de datos personales ante la FGR. 4. Recibir y dar trámite a las solicitudes de acceso a la información y del ejercicio de los derechos ARCOP. 5. Dar seguimiento a solicitudes de información, de ejercicio de derechos ARCOP y recursos de revisión. 6. Notificar las respuestas de las solicitudes a los particulares. 7. Llevar un registro de las solicitudes de acceso a la información, respuestas, costos de reproducción y envío. 8. Verificar que los datos personales solo se entreguen a su titular o su representante legal debidamente acreditados. ***De manera adicional, los datos personales que se nos proporcione podrán ser utilizados para contar con datos estadísticos, de control, e informes sobre el servicio brindado.*** **CAPACITACIÓN** 1. Realizar el registro en el Sistema de Información de la Profesionalización (**SIP**). 2. Generar un usuario y contraseña para el uso de las Plataformas del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (**INAI**): Sistema para la Administración de la Capacitación Presencial (**SACP**) y Centro Virtual de Capacitación (**CEVINAI**). 3. Realizar el registro a los cursos del SACP y CEVINAI. 4. Generar las constancias de participación. 5. Tener el registro de los servidores públicos de nuevo ingreso a la institución para la obtención de los Reconocimientos de Institución y Comité 100% capacitados. **SISTEMA DE PORTALES DE OBLIGACIONES DE TRANSPARENCIA (SIPOT)** 1. Generar un usuario y contraseña para el uso de la PNT-SIPOT. 2. Publicación de la información en el SIPOT, cumpliendo con las obligaciones de transparencia. 3. Generar un usuario y contraseña para uso de la herramienta Blob Storage.
3. Catálogo de tipo de datos personales que se traten, indicando si son sensibles o no. **En relación con el artículo 32, fracción I y II de la LGPDPPSO.** **(ISO 27001)**	✓ ***Datos personales estándar:*** **Personas Físicas:** • Nombre completo o pseudónimo • Sexo • Fecha de nacimiento • Domicilio • Correo electrónico • Teléfono • Escolaridad • Puesto • Lugar de trabajo • Entidad federativa

	• CURP • RFC • Firma **Personas Morales:** • Nombre completo o pseudónimo • Denominación o razón social • Nombre del representante legal. • Domicilio • RFC • Correo electrónico • Teléfono **Servidores Públicos:** ***Administrativos:*** • Nombre Completo • Correo electrónico institucional • Sexo • Escolaridad • Puesto • Teléfono o extensión • Firma ***Sustantivos:*** • Correo electrónico institucional • Sexo • Escolaridad • Puesto • Teléfono o extensión • Firma ***En ciertos contextos los datos personales podrían ser considerados como un dato personal sensible.*** ✓ ***Datos personales sensibles:*** **Personas Físicas:** • Lengua indígena • Discapacidad • Nivel económico (solicitud para no cubrir el pago de reproducción y envío) • Fotografía • Datos biométricos • Estado de salud • Grupo étnico • Patrimonio • Antecedentes Penales **Personas Morales:** • Nombre completo o pseudónimo
4. Catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de	• **Medios de almacenamiento físico:** [redacted] [redacted]

los datos personales	[redacted] • **Medios de almacenamiento electrónico:** [redacted] [redacted]
5. Número de titulares en relación con el artículo 32, fracción VI y VIII en el aspecto de cuantitativo de la LGPDPPSO (ISO 27001)	**Número de titulares:** **> 500K:** Datos de más de 500,000 personas
6. Lista de servidores públicos que tienen acceso al sistema de tratamiento	**Plataforma Nacional de Transparencia** [redacted] Titular de la UTAG [redacted] Director de Área de Acceso a la Información [redacted] Directora de Gobierno Abierto [redacted] – Director de Área [redacted] – Director de Protección de Datos Personales y Capacitación [redacted] – Administrador Auxiliar [redacted] Administrador Auxiliar [redacted] – Administrador Auxiliar [redacted] Administrador Auxiliar [redacted] Administrador Auxiliar [redacted] – Administrador Auxiliar [redacted] – Administrador de Apoyo [redacted] – Administrador de Apoyo [redacted] Administrador de Apoyo [redacted] – Administrador de Apoyo [redacted] – Administrador de Apoyo [redacted] – Técnico Especializado I [redacted] – Técnico Especializado A **Archivo** [redacted] Auxiliar B [redacted] – Especialista Técnico [redacted] Especialista Técnico [redacted] – Especialista Técnico I **SIPOT** [redacted] – Director de Protección de Datos Personales y Capacitación [redacted] – Técnico Especializado D [redacted] – Directora de Gobierno Abierto [redacted] – Administrador Auxiliar [redacted] – Administrador de Apoyo **Herramienta Blob Storage**

	[redacted] – Director de Protección de Datos Personales y Capacitación [redacted] Técnico Especializado D [redacted] – Directora de Gobierno Abierto [redacted] – Administrador Auxiliar [redacted] – Administrador de Apoyo **SIP, SACP y CEVINAI** [redacted] Director de Protección de Datos Personales y Capacitación [redacted] – Técnico Especializado D
7. En su caso, nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable. **En relación con el artículo 32, fracción V de la LGPDPPSO.**	**NO APLICA.**
8. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican. **En relación con el artículo 32, fracción V de la LGPDPPSO.**	La transferencia de datos, excepcionalmente, se realiza a autoridad competente que funde y motive su solicitud por escrito, oficio o requerimiento judicial y previa verificación de la existencia de los datos solicitados. En tal caso, los terceros receptores lo son jueces, ministerios públicos, magistrados que revisten el carácter de autoridad y solicitan los datos con el fin de integrar algún elemento o dato a los expedientes ministeriales y/o judiciales a su cargo.
9. Ciclo de vida de los datos personales **en relación con el artículo 32, fracción V de la LGPDPPSO.**	***a) Obtención de los datos personales*** **SOLICITUDES DE ACCESO Y DERECHOS ARCOP** • **Por medios físicos:** [redacted]

[redacted]

- **Por medios electrónicos:**

[redacted]

[redacted]

CAPACITACIÓN

- **Por medios Físicos:**

[redacted]

- **Por medios Electrónicos:**

[redacted]

SISTEMA DE PORTALES DE OBLIGACIONES DE TRANSPARENCIA (SIPOT)

[redacted]

[redacted]

- **Por medios electrónicos:**

[redacted]

b) Almacenamiento de los datos personales

SOLICITUDES DE ACCESO Y DERECHOS ARCOP

- **De forma física:**

[redacted]

[redacted]

[redacted]

- **De forma electrónica:**

[redacted]

[redacted]

[redacted]

CAPACITACIÓN

- **De forma física:**

[redacted]

- **De forma electrónica:**

[redacted]

[redacted]

[redacted]

SISTEMA DE PORTALES DE OBLIGACIONES DE TRANSPARENCIA (SIPOT)

- **De forma física:**

[redacted]

[redacted]

[redacted]

- **De forma electrónica:**

[redacted]

[redacted]

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.

[redacted]

[redacted]

[redacted]

d) La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen:

[redacted]

e) El bloqueo[66] de los datos personales:

Se realiza únicamente cunado alguna autoridad competente que funde y motive su solicitud por escrito, oficio o requerimiento judicial y previa verificación de la existencia de los datos solicitados.

f) La cancelación, supresión o destrucción de los datos personales.

La cancelación se lleva a cabo conforme al Catálogo de Disposición Documental (CADIDO), descrito en la siguiente tabla:

Código	Niveles de Clasificación	Vigencia Documental	Técnicas de Selección	Observaciones

[66] *Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda (Art. 3, fr. IV LGPGPPSO)*

Sección y Serie Documental		Valor documental				Plazos de Conservación			Baja	Conservación	Muestreo	
		A	L	F	C	AT	AC	TOTAL				
12C	Transparencia y Acceso a la Información											
12C.1	Disposiciones en Materia de Acceso a la Información	X	X			1	6	7			X	Selección del 20% del total XX167X de expedientes de la serie Documental
12C.2	Programas y Proyectos en Materia de Acceso a la Información	X				3	3	6			X	Selección del 20% del total XX167X de expedientes de la serie Documental
12C.3	Programas y proyectos en la Materia de Transparencia y Combate a la Corrupción	X	X			3	3	6			X	Selección del 20% del total XX167X de expedientes de la serie Documental
12c.5	Sesiones del Comité de Información	X	X			3	3	6			X	Selección del 20% del total XX167X de expedientes de la serie Documental
12C.6	Solicitudes de Acceso a la Información	X	X			2	2	4	X			
12C.7	Portal de Transparencia	X	X			3	3	6	X			
12C.8	Clasificación de Información Reservada	X	X			1	1	2	X			
12C.9	Clasificación de Información Confidencial	X	X			1	1	2	X			
12C.10	Sistemas de Datos Personales	X	X			3	3	6	X			

A: Administrativo
L: Legal
F: Fiscal

	C: Contable **AT:** Archivo de Trámite **AC:** Archivo de Concentración La vigencia de AT iniciará a partir de la conclusión o cierre del expediente

II. Funciones y obligaciones de las personas que traten datos personales

Roles, funciones y obligaciones en el tratamiento de los datos personales En relación con el artículo 32, fracción V de la LGPDPPSO.

El ciclo de vida está relacionado con toda la tabla marcada en lo incisos siguientes:

Áreas relacionadas	**Tratamiento**					
	a) Obtención	**b) Almacenamiento**	**c) Uso**	**d) Divulgación**	**e) Bloqueo**	**f) Cancelación**
Módulo de Atención de la UTAG	X					
Dirección de Acceso	X	X	X	X	X	X
Dirección de Protección de Datos y Capacitación	X	X	X	X	X	X
Dirección General de Formación Profesional		X		X		
Áreas de la FGR				X		
Instituto Nacional de Transparencia				X		

III. Análisis de riesgos

1. Requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico

[redacted]

2. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida

[redacted]

3. El valor y exposición de los activos involucrados en el tratamiento de los datos personales	<table><tr><th>Activo</th><th>Amenaza</th><th>Medida de seguridad existente</th><th>Daño/Impacto</th><th>Potencial/ Probabilidad</th></tr><tr><td colspan="5"></td></tr></table>
4. Catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales	**Posibles consecuencias de una vulneración para los titulares;** Si los datos personales de las y los servidores públicos, o incluso los datos de sus beneficiarios, familiares, dependientes económicos o referencias llegan a ser expuestos, vulnerados, robados o mal utilizados, puede haber consecuencias graves en la integridad de ellos, debido a que sus datos quedan expuestos y las personas pueden llegar a usar dichos datos personales para cometer ilícitos, arbitrariedades o incluso delitos, tales como los siguientes: • **Robo de identidad** El robo de identidad ocurre cuando alguien hurta sus datos personales para cometer fraudes. El ladrón de identidad puede usar esa información para solicitar un crédito, presentar declaraciones de impuestos o conseguir servicios médicos de manera fraudulenta. Estas acciones pueden dañar su buen nombre y su crédito, además de costarle tiempo y dinero para repararlo. • **Elaboración de perfiles** Forma de tratamiento automatizado de datos personales que consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona. Sirve en particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona. • **Extorsión** La extorsión consiste en obligar a una persona a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero. En la extorsión la delincuencia utiliza la violencia psicológica para intimidar a las víctimas, por ejemplo, utilizando agresiones verbales. En otras ocasiones aprovechan la buena fe de las personas para engañarlas. En la mayoría de los casos, los delincuentes eligen al azar a la víctima, utilizando directorios telefónicos, datos personales obtenidos a través de distintas vías e incluso, tomando la información difundida de forma pública en redes sociales por la propia persona. • **Secuestro**

Privación de libertad ambulatoria a una persona o grupo de personas, exigiendo, a cambio de su liberación, el cumplimiento de alguna condición, como puede ser el pago de un rescate.

- **Homicidio doloso**

El homicidio doloso es un subtipo del delito de homicidio que se caracteriza porque el criminal busca intencionadamente el resultado de muerte de la víctima.

- **Robo**

Quitar a una persona algo que le pertenece con ánimo de lucro, por medio de la violencia o la intimidación o utilizando la fuerza.

- **Usurpación de funciones**

Se refiere al ejercicio de actos propios de una autoridad o funcionario público. Actos propios de una autoridad o funcionario público son aquellos que están comprendidos categóricamente en la disposición legal o reglamentaria que regula tales actos, y también aquellos que están comprendidos en la línea general o en el contexto de las atribuciones conferidas a la autoridad o funcionario público, sin que sea preciso que lo que se usurpa sea la función específica de un determinado cargo, es decir, basta, por ejemplo, que una persona se presente como policía, sin serlo, y realice actos correspondientes a la policía (detención), sin que sea preciso que se presente como policía judicial. El segundo requisito, esencial, de este delito consiste en atribuirse carácter oficial. Este requisito significa que quien así actúa ha de hacer ver falsamente, con actos capaces, ya sea manifestándolo oralmente, o dándolo a conocer con capacidad bastante para engañar a una persona o colectividad, que se tiene el carácter oficial para ejercer los actos propios de esa autoridad o funcionario público.

- **Falsificación de documentos**

El delito de falsificación de documentos se comete por alguno de los medios siguientes:
1 Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando una verdadera;
2 Aprovechando indebidamente una firma o rúbrica en blanco ajena, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otro, causar un perjuicio a la sociedad, al Estado o a un tercero
3 Alterando el contexto de un documento verdadero, después de concluido y firmado, si esto cambiare su sentido sobre alguna circunstancia o punto substancial, ya se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación
4 Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento
5 Atribuyéndose el que extiende el documento, o atribuyendo a la persona en cuyo nombre lo hace: un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto
6 Redactando un documento en términos que cambien la convención celebrada en otra diversa en que varíen la declaración o disposición del otorgante, las obligaciones que se propuso contraer, o los derechos que debió adquirir
7 Añadiendo o alterando cláusulas o declaraciones, o asentando como ciertos hechos falsos, o como confesados los que no lo están, si el documento en que se asientan se extendiere para hacerlos constar y como prueba de ellos
8 Expidiendo un testimonio supuesto de documentos que no existen, dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando
9 suprimiendo en la copia algo que importe una variación substancia, y Alterando un perito traductor o paleógrafo el contenido de un documento, al traducirlo o descifrarlo.
10 Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial, sin contar con la autorización de la autoridad correspondiente.

- **Acoso**

Los tipos de acoso más conocidos son el escolar, laboral y sexual, sin embargo, hay muchas otras clases. El acoso es un fenómeno que se caracteriza por la aparición de

	comportamientos y actitudes dañinas hacia una persona o grupo, normalmente de manera repetida en el tiempo. El acoso es visto como un trastorno u obsesión que sufren un grupo de personas que las lleva a realizar ciertas acciones como espiar a sus víctimas, seguirlas, llamarlas, amenazarlas y cometer actos violentos contra ellas.

IV.	Análisis de brecha en relación con el artículo 32, fracción III de la LGPDPPSO.
1. Medidas de seguridad existentes y efectivas	**a) Administrativas** [redacted] **b) Físicas** [redacted] [redacted] [redacted] [redacted]

	[redacted] **c) Técnicas** [redacted]
2. Medidas de seguridad faltantes	**a) Administrativas** [redacted] **b) Físicas** [redacted] **c) Técnicas** [redacted] •
3. Existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.	[redacted]

V. Plan de trabajo				
Acción a implementar	**Meta o resultado esperado**	**Fecha de inicio**	**Fecha de término**	**Indicadores**
Cambiar contraseñas	[redacted]	[redacted]	[redacted]	[redacted]
Respaldo de la información contenida en los equipos de cómputo	[redacted]	[redacted]	[redacted]	[redacted]

[67] Retener el riesgo: Se puede tomar la decisión de retener el riesgo sin considerar medidas adicionales si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles se pueden implementar posteriormente. Por ejemplo, el equipo de cómputo actual falla, pero se genera un respaldo de esa información al final del día, por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

Solicitar apoyo a DGTIC para la actualización de vacuna de los equipos de cómputo.	[redacted]	[redacted]	[redacted]	[redacted]

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad				
Medida de seguridad a monitorear	**Medio de verificación**	**Fecha de inicio**	**Fecha de término**	**Responsable**
Capacitación en materia de Protección de Datos Personales y sensibilización para la transparencia.	[redacted]	[redacted]	[redacted]	[redacted]
Cámaras de Seguridad	[redacted]	[redacted]	[redacted]	[redacted] Director de Protección de Datos Personales y Capacitación
Actualización de vacuna en equipos de cómputo	[redacted]	[redacted]	[redacted]	[redacted] Director de Protección de Datos Personales y Capacitación
Mantenimiento los equipos de cómputo	[redacted]	[redacted]	[redacted]	[redacted] Director de Protección de Datos Personales y Capacitación
Correcto funcionamiento del No Break	[redacted]	[redacted]	[redacted]	[redacted] Director de Protección de Datos Personales y Capacitación
Usuarios y contraseñas en los equipos de cómputo.	[redacted]	[redacted]	[redacted]	[redacted] Director de Protección de Datos Personales y Capacitación
Cerraduras de archiveros y robotines.	[redacted]	[redacted]	[redacted]	[redacted] Director de Protección de Datos Personales y Capacitación

VII. Vulneraciones	
Las vulneraciones previas ocurridas en los sistemas de tratamiento en relación con el artículo 32, fracción VII y VIII en el aspecto de	No ha ocurrido ninguna vulneración.

[68] Evitar el riesgo: Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios, se debe tomar una decisión para evitar el riesgo, retirándose de las actividades actuales o cambiando las condiciones bajo las cuales operan dichas actividades. Por ejemplo, para un riesgo causado por la naturaleza podría ser más eficiente en costo mover físicamente el site de datos a una ubicación donde no exista el mismo riesgo o que se pueda mantener bajo control.

cuantitativo de la LGPDPPSO.	

[redacted]