



**ANEXOS EN FORMATO ABIERTO DEL DOCUMENTO DE SEGURIDAD EN MATERIA DE
PROTECCIÓN DE DATOS PERSONALES
DE LA OFICINA DEL GOBERNADOR**

**OFICINA DEL GOBERNADOR
JEFATURA DE OFICINA DE GUBERNATURA
COMITÉ DE TRANSPARENCIA**

OG/12C.10-UT/PDP-DS/2026



Anexo 5: Formato de Reporte de Seguridad para el Mecanismo de monitoreo en la protección de datos personales.

De conformidad con lo establecido en el Mecanismo de monitoreo y supervisión en la protección de datos personales, el cual obra en el Documento de Seguridad, la Unidad de Transparencia requerirá a órgano administrativo, por cada uno de los tratamientos que realiza, la elaboración del Reporte de Seguridad de Datos Personales en el que deberán precisarse los elementos siguientes:

Reporte de Seguridad de Datos Personales	
Fecha de elaboración:	
Información General del Tratamiento	
Planteamiento	Respuesta
Instancia responsable del tratamiento.	
Denominación del tratamiento.	
Fundamento normativo del tratamiento.	
Información Requerida	
Planteamiento	Respuesta
Indique las acciones desarrolladas para la ejecución de las medidas de control existentes.	
Manifieste si existe alguna actualización o modificación respecto de las medidas de seguridad y controles implementados en el tratamiento de datos personales que realice.	

De ser así, deberán incluir una explicación de tal actualización o modificación.

Indique de manera clara la actualización de los aspectos siguientes:

- La incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.
- El surgimiento de nuevas amenazas en el tratamiento de los datos.
- La posibilidad de que las nuevas amenazas actualicen una vulnerabilidad en el tratamiento de datos respectivo.
- Casos en los que una amenaza haya sufrido alguna modificación que derive en el incremento del impacto que tendría su materialización en la seguridad de los datos personales

Anexo 6: Formato de Dictamen de Seguridad para el Mecanismo de supervisión en la protección de datos personales.

De conformidad con lo establecido en los Mecanismo de monitoreo y supervisión en la protección de datos personales, el cual obra en el Documento de Seguridad, la Unidad de Transparencia analizará los Reportes e Seguridad de Datos Personales elaborados por los órganos administrativos, supervisando los aspectos siguientes:

Formato de Dictamen de Seguridad	
Fecha de elaboración:	
Dictamen de Seguridad	
Planteamiento	Respuesta
Idoneidad y efectividad de las medidas de seguridad y control respecto del tratamiento.	
Suficiencia de controles preventivos y correctivos.	
Gestión interna de nuevas amenazas e incrementos en el impacto de probables daños.	
Nombre, cargo y adscripción de la persona servidora pública responsable del tratamiento o sistema.	
Cumplimiento de políticas, planes, procesos y procedimientos en materia de seguridad de datos personales.	
Observaciones por parte de la Unidad de Transparencia.	

Anexo 7: Formato de Reporte de Alerta de Seguridad.

De conformidad con lo establecido en el Mecanismo de actuación ante alertas y vulneraciones a la seguridad de los datos personales, el cual obra en el Documento de Seguridad, las instancias deberán emitir un Reporte de Alerta de Seguridad cuando hayan verificado la existencia de una alerta de seguridad, en el deberán precisarse los aspectos siguientes:

Reporte de Alerta de Seguridad	
Fecha de elaboración:	
Información General del Tratamiento	
Planteamiento	Respuesta
Instancia responsable del tratamiento.	
Fundamento normativo del tratamiento.	
Detección	
Planteamiento	Respuesta
Nombre, cargo y adscripción de la persona servidora pública que detectó la amenaza.	
Fecha, hora y lugar en que se detectó, así como una descripción detallada de cómo fue descubierta.	
Tratamiento o sistema en que ocurrió.	
Nombre, cargo y adscripción de la persona servidora pública responsable del tratamiento o sistema.	
Datos personales involucrados en la amenaza.	

Proyección de una posible vulneración	
Planteamiento	Respuesta
Elementos que permitieron el desarrollo o persistencia de la amenaza.	
Elementos que contuvieron el desarrollo o persistencia de la amenaza.	
Actuaciones que pueden evitar la reincidencia de la amenaza.	
Descripción de los efectos que hubiera causado la anomalía si hubiere persistido hasta materializar una vulneración.	
Medidas de seguridad involucradas	
Planteamiento	Respuesta
Descripción clara de los controles físicos o electrónicos involucrados en la amenaza.	
Circunstancias que, individual o conjuntamente, permitieron la existencia de la amenaza.	
Justificar si la amenaza pudo ser <u>prevenida</u> , detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.	
Ante la materialización de la amenaza, justificar si en el futuro puede <u>evitarse su reincidencia</u> , detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente puedan impedirlo.	
Si la forma de prevenir o evitar la reincidencia de la amenaza, involucran una nueva medida de seguridad, deberá ser claramente descrita.	

Anexo 8: Formato de Informe de Causas y Acciones de una Vulneración.

De conformidad con lo establecido en el Mecanismo de monitoreo, revisión, alertas, vulneraciones y auditoría, el cual obra en el Documento de Seguridad, la instancia que presente una vulneración elaborará un informe de causas y acciones, mismo que deberá remitirse a la Unidad de Transparencia para su registro y análisis. En su elaboración, se podrá tomar como referencia el formato siguiente:

Informe de causas y acciones de una Vulneración	
Fecha de elaboración:	
Información General del Vulneración	
Planteamiento	Respuesta
Nombre, cargo y adscripción de la persona servidora pública que detectó la vulneración.	
Fecha, hora y lugar en que se detectó la vulneración.	
Tratamiento o sistema que fue vulnerado.	
Nombre, cargo y adscripción de la persona servidora pública responsable del tratamiento o sistema.	
Datos personales involucrados en la vulneración.	
Descripción detallada de la forma en que se detectó la vulneración.	
Investigación	
Planteamiento	Respuesta

Fecha y hora en que se inició la investigación de la vulneración.	
Nombre y cargo de la persona servidora pública designada para la investigación de la vulneración.	
Naturaleza de la vulneración.	
Fecha y hora de la vulneración.	
Descripción detallada de la forma en que se desarrolló la vulneración.	
Descripción detallada de las afectaciones que fueron materializadas.	
Tipo y número aproximado de las personas titulares afectadas.	
Posibles consecuencias de la vulneración.	
Medidas de seguridad vulneradas e impacto causado	
Planteamiento	Respuesta
Descripción clara de cada uno de los controles físicos o electrónicos que operan en el tratamiento o sistema, incluyendo la persona servidora pública responsable de su implementación.	
Identificación de la totalidad de las personas que cuentan con acceso a cualquiera de las fases del tratamiento, incluyendo las personas servidoras públicas o las personas ajenas a la Oficina del Gobernador.	
Identificación y descripción de la vulneración materializada.	

Determinación del nivel de impacto causado por la vulneración en relación con el tratamiento o sistema (alto, medio, bajo), considerando el número de personas titulares afectadas, así como el tipo y naturaleza de los datos personales involucrados en la vulneración.

Determinación relativa a si la vulneración generó una afectación significativa a los derechos patrimoniales y/o morales de las personas titulares de los datos personales.

De conformidad con lo previsto en los párrafos tercero y cuarto, del artículo 66, de los Lineamientos Generales de Protección, para determinar la existencia de una afectación significativa patrimonial o moral, se deberán atender los criterios siguientes:

Afectación Patrimonial	Afectación moral
La vulneración se encuentra relacionada, de manera enunciativa más no limitativa, con: ▪ Los bienes muebles e inmuebles. ▪ Información fiscal. ▪ Historial crediticio. ▪ Ingresos y egresos. ▪ Cuentas bancarias. ▪ Seguros. ▪ Afores. ▪ Fianzas. ▪ Servicios contratados. ▪ Cantidades o porcentajes relacionados con la situación económica de la persona titular.	La vulneración esté relacionada, de manera enunciativa más no limitativa, con: ▪ Los bienes muebles e inmuebles. ▪ Información fiscal. ▪ Historial crediticio. ▪ Ingresos y egresos. ▪ Cuentas bancarias. ▪ Seguros. ▪ Afores. ▪ Fianzas. ▪ Servicios contratados. ▪ Cantidades o porcentajes relacionados con la situación económica de la persona titular.

Acciones para prevenir y corregir una nueva vulneración

Planteamiento	Respuesta
Justificar si la vulneración pudo ser prevenida, es decir, si hubiera sido posible eliminar las causas del riesgo que fue materializado, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.	
Si la vulneración no pudo ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con la que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo.	
Analizar las medidas que, de acuerdo con la magnitud de la vulneración ocurrida, permitan el restablecimiento del tratamiento o sistema de datos personales.	
Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración.	
Recomendaciones para la persona titular afectada.	
Medio puesto a través del cual pueda obtenerse más información respecto de la vulneración.	
Datos de contacto de las personas servidoras públicas designadas para la gestión de la vulneración.	
Cualquier información y/o documentación que se considere conveniente.	

Anexo 7: Formato de Bitácora de Vulneraciones a la Seguridad de los Datos Personales.

De conformidad con lo establecido en el Mecanismo de actuación ante alertas y vulneraciones de seguridad, el cual obra en el Documento de Seguridad, la Unidad de Transparencia integrará la Bitácora de Vulneraciones a la Seguridad de los Datos Personales.

Para su integración, se tomará como referencia el formato siguiente:

Bitácora de Vulneraciones	
Fecha de elaboración:	
Información General del Tratamiento	
Planteamiento	Respuesta
Instancia responsable del tratamiento.	
Denominación del tratamiento.	
Fundamento normativo del tratamiento.	
Información general de la vulneración	
Planteamiento	Respuesta
Nombre, cargo y adscripción de la persona servidora pública que detectó la vulneración.	
Fecha, hora y lugar en que detectó la vulneración.	
Descripción clara del tratamiento o sistema que fue vulnerado.	

Nombre, cargo y adscripción de la persona servidora pública responsable del tratamiento o sistema.	
Datos personales involucrados en la vulneración.	
Descripción detallada de la forma en que se detectó la vulneración.	
Análisis de la implementación de acciones para prevenir y corregir una nueva vulneración	
Planteamiento	Respuesta
Aproximación de la magnitud del daño ocasionado respecto del número de personas titulares afectas, así como el tipo y naturaleza de los datos personales involucrados en la vulneración.	
Justificar si la vulneración pudo ser prevenida, es decir, si hubiera sido posible eliminar las causas del riesgo que fue materializado, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.	
Si la vulneración no pudo ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con la que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo.	
Analizar las medidas que, de acuerdo con la magnitud de la vulneración ocurrida, permitan el restablecimiento del tratamiento o sistema de datos personales.	
Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración.	