Guía

Para la gestión y notificación de vulneraciones a la seguridad de los datos personales

Anexo Único del Acuerdo INE-CT-ACG-PDP-002-2020

Noviembre 2020

Instituto Nacional Electoral

CONTENIDO

OBJETIVO

Esta guía tiene como finalidad que las áreas responsables de las bases de datos, y quienes intervengan en su tratamiento, como custodios, usuarios y encargados, conozcan las acciones a seguir para gestionar las vulneraciones y, en caso de ser necesario, integrar y/o complementar las actividades necesarias en el proceso relacionado con su atención.

APLICABILIDAD

El presente documento es aplicable a los Órganos Ejecutivos, Técnicos de vigilancia, en materia de transparencia y de control, a nivel central y desconcentrado que, por sus funciones, traten datos personales.

REFERENCIAS NORMATIVAS

1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
2. Lineamientos Generales de Protección de Datos Personales para el Sector Público (emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales).
3. Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

ACRÓNIMOS

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

FEDE: Fiscalía Especializada en Delitos Electorales.

LGPDPPSO o Ley: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

UTTyPDP o Unidad de Transparencia: Unidad Técnica de Transparencia y Protección de Datos Personales.

TÉRMINOS Y DEFINICIONES

Para los efectos de esta guía, se tomarán las definiciones establecidas en el artículo 3° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Además, sin perjuicio de lo previsto en la normativa aplicable a la materia, se entenderá por:

Activo	En términos generales, es un bien tangible o intangible que una organización posee y que es requerido para su funcionamiento y el logro de objetivos; es decir, tiene valor para la organización.
Activo primario	En materia de datos personales, es la información que contiene datos personales.
Activo secundario	Todos los elementos físicos (como archivos e instalaciones) y/o tecnológicos (como servidores y sistemas) a través de los cuales se da tratamiento al activo primario.
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.
Agente de amenaza	Método dirigido a la explotación intencional de una vulnerabilidad o que puede provocar accidentalmente una vulnerabilidad.[1]
Amenaza	Circunstancia o evento con el potencial de impactar adversamente las operaciones de la organización (incluida la misión, funciones, imagen o reputación), sus activos o las personas que la integran.[2]
Cadena de custodia	Sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo; desde su localización, descubrimiento o aportación, en el lugar de los hechos o hallazgo, hasta que la autoridad competente ordene su conclusión. Con el fin de corroborar los elementos materiales probatorios y la evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: condiciones de recolección, preservación, empaque y traslado.[3]
Confidencialidad	Principio de seguridad que garantiza que la información no se divulgue a personas no autorizadas.

[1] Definición obtenida de https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
[2] Definición obtenida de https://csrc.nist.gov/glossary/term/
[3] Definición obtenida de http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_220120.pdf

Control	Acciones de protección de datos personales resultado de las obligaciones de la normativa en la materia. Es una medida que modifica el riesgo del dato personal.[4]
Criptografía de llave pública o Criptografía asimétrica	Técnica de codificación que utiliza un par de claves diferentes para el cifrado y descifrado de información y garantiza el no repudio, la confidencialidad y la integridad.[5]
Custodio	Área que implementa las medidas de seguridad de la información y asesora a los propietarios sobre los mecanismos de seguridad existentes.
Disponibilidad	Propiedad de la seguridad con relación a los datos y recursos para que éstos sean accedidos de manera oportuna por las personas autorizadas.
Evento de seguridad	Suceso anómalo que tiene la posibilidad de comprometer un proceso, sistema o la información que el sistema procesa, almacena o transmite, del que no se tiene la certeza de implicaciones negativas.[6]
Evidencia (digital)	Conjunto de datos en formato binario que incluye archivos, contenido o referencia a estos (metadatos) que se encuentran en el hardware o el software del sistema vulnerado. [7]
Incidente de seguridad	Es un riesgo materializado que afecta de forma negativa la confidencialidad, integridad o disponibilidad de un sistema o la información que procesa, almacena o transmite debido a la explotación de una vulnerabilidad por un agente de amenaza, o que constituye una violación de las políticas y procedimientos de seguridad o políticas de uso aceptable[8]
Integridad	Principio de seguridad que garantiza que la información y los métodos de procesamiento no se modifiquen por usuarios o procesos no autorizados, de forma maliciosa o accidental.
Medio de almacenamiento físico	Es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales. *(Por ejemplo, los expedientes del personal almacenados en un archivero. En este sentido hay que considerar cuartos especiales, bóvedas, muebles, cajones y cualquier espacio donde se guarden soportes físicos, o bien equipo de cómputo u otros medios de almacenamiento de datos personales).*

[4] ISO/IEC 27000:2018, Information Technology – Security Techniques- Information security system – Overview and vocabulary.
[5] Definición obtenida de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
[6] Definición obtenida de https://www.pmg-ssi.com/2016/09/iso-27001-diferencia-entre-evento-e-incidente/
[7] Definición obtenida de http://recibe.cucei.udg.mx/revista/es/vol4-no3/computacion01.html
[8] Definición obtenida de https://csrc.nist.gov/glossary/term/security_incident

Medio de almacenamiento digital	Es todo recurso al que se puede acceder mediante el uso de equipo que procese su contenido para examinar, modificar o almacenar los datos personales. (*Por ejemplo, discos duros (tanto los propios del equipo de cómputo como los portátiles), memorias extraíbles como USB o SD, CDs, Blu-rays, discos duros extraíbles, entre otros. También podemos contemplar como medio de almacenamiento digital, el uso de servicios de almacenamiento en línea.)*
Plan de respuesta a incidentes de seguridad de la información o Plan de respuesta a incidentes	Procedimiento que permite actuar rápido y eficaz ante cualquier incidente en materia de seguridad de la información. Incluye medidas para comunicar de forma correcta los incidentes a quien corresponda (tanto dentro como fuera de la organización), los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.[9]
Proceso	Conjunto de fases sucesivas de un fenómeno natural o de una operación artificial. [10] Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto.[11]
Proceso de negocio	Procesos que prescriben la forma en la que se utilizan los recursos -datos, capital, personas- de una organización para lograr sus objetivos de negocio.[12]
Propietaria	El área dueña de las bases de datos personales, que toma decisiones respecto a su tratamiento y es la responsable final de la protección y el uso de los datos.
Riesgo	Probabilidad de que ocurra un evento (en función de que una amenaza explote una vulnerabilidad) con sus consecuencias negativas (impactos adversos). [13]
Riesgo inherente	Riesgo intrínseco al dato personal derivado del impacto negativo a la privacidad que puede causar en la persona.
Sistema de tratamiento o sistema de datos personales	Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos. [14] El sistema puede ser automatizado o manual.

[9] Definición obtenida de https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/respuesta-incidentes.pdf
[10] Diccionario de la Lengua española en línea, URL: https://dle.rae.es/proceso
[11] Gestión de Calidad. Universidad Santiago de Cali, URL: https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones
[12] F. Leymann and W. Altenhuber, "Managing business processes as an information resource," in IBM Systems Journal, vol. 33, no. 2, pp. 326-348, 1994.
[13] Definición obtenida de https://csrc.nist.gov/glossary/term/risk
[14] Recomendaciones para el manejo incidentes de seguridad de datos personales. INAI"

Sitios de almacenamiento	Instalaciones donde se resguarden los medios de almacenamiento, en cualquier soporte documental.
Transmisión	Envío electrónico de información desde una ubicación a otra u otras.[15]
Usuaria	El área autorizada para acceder a los datos. Son quienes utilizan la información.
Vulnerabilidad	Debilidad o fallo en un sistema de información, procedimientos de seguridad del sistema, controles internos o de la implementación de un control que podría ser explotada o activada de manera intencional o no por una amenaza.
Vulneración	Incidente de seguridad que involucra datos personales.

[15] Definición obtenida de https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7298r1.pdf

1 INTRODUCCIÓN

La **LGPDPPSO** ha incorporado nuevas obligaciones a los responsables del tratamiento de los datos personales. De acuerdo con lo señalado en el artículo 40, el responsable deberá informar a la persona titular y al INAI *-y según corresponda-* aquellas vulneraciones que afecten de forma significativa los derechos patrimoniales o morales en cuanto se confirme su ocurrencia.

NOTA. Si bien existen diversos marcos normativos respecto a la atención de incidentes de seguridad, este documento se limita únicamente a los relacionados con los que afecten datos personales.

LA GUÍA RESPONDE A LAS PREGUNTAS:			
¿Qué es (y qué no es) una vulneración?	¿Qué tipos existen?	¿Por qué gestionar las vulneraciones?	¿Quiénes intervienen en su atención y cuáles son sus funciones?
¿Cuáles son las causas de sanción?	¿Cómo me preparo para una posible vulneración?	¿Qué acciones debo tomar para responder ante una vulneración?	
Y se divide en dos apartados			
Apartado I. Generalidades		**Apartado II. Atención a las vulneraciones**	

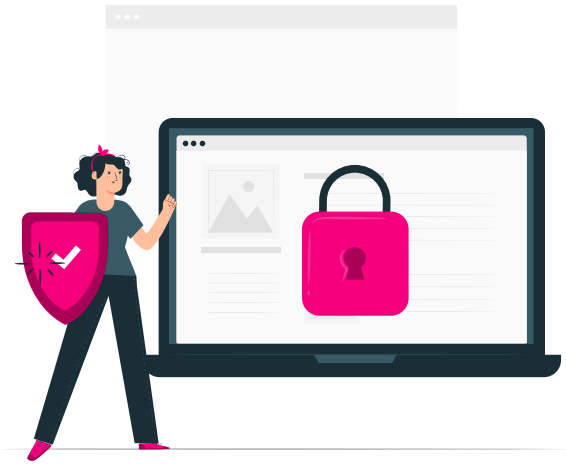
Además, en materia electoral se integra un apartado específico, señalando sus características especiales relacionadas con datos personales.

2 APARTADO I. GENERALIDADES

2.1 ¿QUÉ ES UNA VULNERACIÓN?

Una vulneración es un incidente de seguridad de la información que afecta los datos personales -en cualquier fase de su tratamiento-.

Figura 1. Fases que conducen a una vulneración y los elementos que intervienen



Todas las vulneraciones son incidentes de seguridad de la información, pero no todos los incidentes de seguridad se consideran vulneraciones.

2.2 ¿QUÉ TIPO DE VULNERACIONES EXISTEN?

Los tipos de vulneraciones enmarcados en la Ley y en la normativa internacional en la materia son:

a) Pérdida o destrucción no autorizada.

Pérdida: cuando lo datos existen, pero el área propietaria pierde el control o el acceso a ellos.

Destrucción: cuando los datos ya no existen, o existen en una forma que ya no es posible utilizarlos, sin que haya mediado una autorización de por medio.

Ejemplos:

- El inmueble donde se encuentran resguardados los soportes físicos que contienen datos personales se inunda y afecta los expedientes, ocasionando que no se pueda visualizar la información. A pesar de que se poseen los documentos, no es posible consultarlos.
- La organización tiene almacenados expedientes digitalizados los cuales se encuentran cifrados y la clave únicamente la tiene el director, quien la olvida y es imposible descifrar los archivos; en este supuesto nos encontramos ante una posible pérdida, ya que el área propietaria perdió el acceso a los datos personales.

b) Robo, extravío o copia no autorizada.

Robo: cuando un persona, organización o grupo organizado se apodera de los datos personales, sin derecho y sin consentimiento del área propietaria.

Extravío: cuando el área propietaria, custodia o usuaria por un descuido, desconoce u olvida dónde se encuentra el activo secundario que contiene la información, provocando la pérdida de los datos personales.

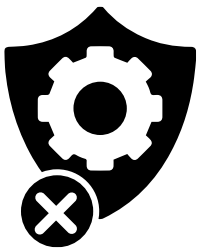
Copia no autorizada: cuando el área propietaria no dio consentimiento para la generación de una copia de la información que contiene datos personales, ya sea que se encuentre en la base de datos, en los repositorios o en cualquier otro soporte documental.

Ejemplos:

- Personal del área de recursos humanos de una organización realiza una copia sin autorización del área propietaria del documento en Excel en el cual se encuentra información laboral, de salud y contacto de los trabajadores.
- Los datos personales son recabados en formularios impresos (físicos), el área propietaria almacena los documentos y posteriormente le son requeridos para actividades del proceso de negocio; sin embargo, el área propietaria olvida la ubicación de los formularios mencionados; produciendo un extravío de datos personales.

c) Uso, acceso o tratamiento no autorizado.

Aunque el tratamiento incluye el uso y acceso a los datos personales, se considera que existe tratamiento no autorizado cuando son utilizados para finalidades distintas para las que fueron recabados o cuando son accedidos sin autorización previa del área propietaria.



Ejemplo:

El área propietaria recaba los datos personales para un concurso; sin embargo, el custodio los utiliza para pruebas en el desarrollo de sistemas

sin haber informado a las personas titulares que sus datos personales serían utilizados para finalidades secundarias[16].

d) Daño, alteración o modificación no autorizada.

Existe cuando los datos personales sufren una transformación -perdiendo su calidad e integridad- derivado de acciones realizadas por una persona, organización o grupo organizado, sin la autorización de la persona propietaria y de manera intencional o no intencional.

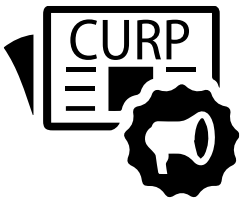
Ejemplo:

El área técnica actualiza una base de datos y coloca de manera errónea los números telefónicos, por lo que no corresponden con el dato de contacto de las personas titulares y no se podrá establecer comunicación con ellos, perdiendo su calidad.

e) Divulgación o revelación no autorizada:

Existe cuando la información que contiene datos personales es divulgada o revelada por personas internas o externas a la organización sin previa autorización o fuera de los tiempos establecidos en el procedimiento.

Ejemplo:



En un programa de reclutamiento, el área responsable de su ejecución debe publicar en la página de la institución -con forme a su procedimiento- el nombre completo y CURP de las personas que fueron seleccionadas, sin embargo, personal del área comete un error y publica no solo a los seleccionados, sino también a todos los candidatos que participaron, incluyendo las calificaciones.

[16] **Finalidad primaria:** Motivo principal y necesario por el cual existe una relación entre el titular de los datos y el responsable.
Finalidad secundaria: Motivos extras por los que se recaban los datos personales y que no son esenciales.
En ambas finalidades es necesario solicitar el consentimiento del titular de los datos a excepción de los supuestos señalados en la LGPDPPSO.

Los siguientes son algunos ejemplos de actividades que NO se consideran vulneraciones para el Instituto:

- ✗ Cuando personal del Instituto se percata que otro sujeto obligado no salvaguarda la información que le fue compartida -derivado de una transferencia en cumplimiento de sus obligaciones- o la utiliza para fines distintos.
- ✗ Cuando el sistema informático mediante el cual se tratan los datos personales no se encuentra disponible debido a una actualización de éste.
- ✗ Divulgación de información en cumplimiento de una obligación o por una orden judicial.
- ✗ Cuando se elimina información debido a que se terminó el tiempo de retención establecido.

2.3 ¿POR QUÉ ATENDER LAS VULNERACIONES?

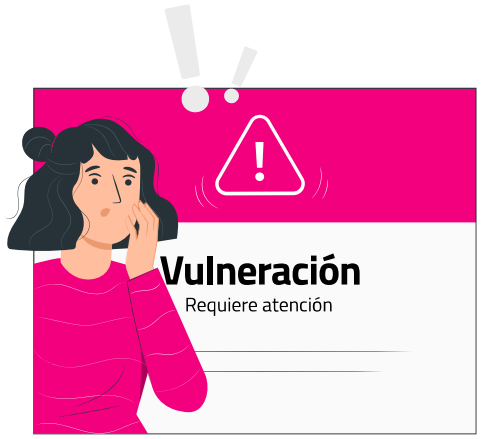
Porque una vulneración puede afectar los derechos patrimoniales o morales de las personas; además, porque es indispensable evitar que se presenten nuevas vulneraciones y porque las personas titulares deben conocer las acciones a seguir.

La **LGPDPPSO** especifica tres obligaciones que las áreas propietarias deben cumplir respecto de las vulneraciones:

a) Analizar las causas por las cuales se presentó la vulneración e incluir en su plan de trabajo -del Documento de Seguridad- las acciones preventivas y correctivas (artículo 37).

b) Llevar una bitácora de vulneraciones (artículo 39).

c) Informar al titular y al INAI las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales de la persona titular (artículo 40).



Recuerda que la atención de las vulneraciones tiene como objetivo:

Para las áreas propietarias: realizar acciones específicas para proteger los datos personales -con base en la normativa aplicable- para evitar que presenten nuevamente la vulneración;

Para las personas titulares: que el sujeto obligado les notifique de manera oportuna la vulneración de la que fueron objeto –*cuando afecte de forma significativa los*

derechos patrimoniales o morales de las personas titulares- y de esta manera conozcan las acciones a seguir con la finalidad de que sus derechos no se vean afectados.

2.4 ¿QUIÉNES INTERVIENEN EN SU ATENCIÓN Y CUÁLES SON SUS FUNCIONES?

Las áreas que intervienen en la atención de las vulneraciones son:

- Área propietaria;
- Unidad de Transparencia.

Y en su caso,

- Encargados;
- Área de Tecnologías de la Información (TI);
- Área de Seguridad informática;
- Área usuaria;

La tabla 1 especifica el rol al que está asociada cada área y las funciones que tiene respecto de la atención de una vulneración.

Tabla 1.
Áreas, roles y funciones sugeridas para la atención de vulneraciones

Área /rol	Función sugerida	Ejemplos
Área propietaria **(rol Propietario)**	• Atender las vulneraciones. • Autorizar la implementación de medidas de seguridad para la mitigación de la vulneración, así como las medidas correctivas aplicadas de forma definitiva y las preventivas -a largo plazo- para la atención de la vulneración. • Determinar con apoyo de la Unidad de Transparencia, si se tiene que notificar la vulneración al INAI y a las personas titulares. • Notificar a las personas titulares -en caso de haberse determinado-. • Llevar una bitácora de las vulneraciones.	Órganos ejecutivos, técnicos de vigilancia, en materia de transparencia y de control, a nivel central y desconcentrado.

Tabla 1.
Áreas, roles y funciones sugeridas para la atención de vulneraciones

Área /rol	Función sugerida	Ejemplos
Unidad de Transparencia	✔ Colaborar con el área propietaria en el análisis para determinar si se notificará la vulneración al INAI y a las personas titulares. ✔ Notificar al INAI. ✔ Proveer el formato para las bitácoras de vulneraciones a las áreas propietarias.	
Encargados	✔ Notificar a las áreas propietarias sobre cualquier incidente que pueda afectar la seguridad de los datos personales. ✔ Atender las actividades que el área propietaria le indique.	
Áreas de TI y de Seguridad informática **(rol Custodio)**	**Áreas de seguridad informática,** solo en caso de que la vulneración involucre activos informáticos ✔ Atender la vulneración, junto con el área propietaria, ✔ En caso de contar con un *Plan de respuesta a incidentes de seguridad de la información o de vulneraciones* llevar a cabo las actividades que en él se establezcan. ✔ Determinar y diseñar las acciones de mitigación, correctivas definitivas y preventivas de largo plazo, junto con el área propietaria. ✔ Proveer al área propietaria la información acerca de la detección, contención, erradicación de la vulneración y, en su caso, recuperación de los activos secundarios afectados para la toma de decisiones. ✔ Proponer al área propietaria las medidas de seguridad para mitigar la vulneración. ✔ Implementar las medidas correctivas aplicadas de forma definitiva y las medidas preventivas (a largo plazo). ✔ Disponer de las herramientas y algoritmos para el debido cuidado de la evidencia, en caso de que aplique. **Áreas de Tecnologías de Información** ✔ Proveer un ambiente aislado y controlado para atender la vulneración, en caso de que aplique.	**Unidad Técnica de Servicios de Informática (UTSI).** **Direcciones o subdirecciones de seguridad informática.** **Coordinaciones o Direcciones de Tecnologías de la Información.**

Tabla 1. **Áreas, roles y funciones sugeridas para la atención de vulneraciones**		
Área /rol	**Función sugerida**	**Ejemplos**
	✔ En caso de contar con un *Plan de respuesta a incidentes de seguridad de la información*, ejecutar las actividades que se consideren necesarias conforme a este.	
Áreas usuarias **(rol usuarios)**	✔ Reportar cualquier irregularidad, funcionamiento anormal o evento de seguridad identificado en cualquier fase del tratamiento de los datos personales.	Todas las áreas que utilicen la información que contenga datos personales.

2.5 ¿CUÁLES SON LAS CAUSAS DE SANCIÓN?

Las causas de sanción[17] en caso de vulneraciones son:

- **Presentar vulneraciones a la seguridad de los datos personales por falta de implementación de medidas de seguridad.** El área propietaria tiene la obligación de implementar medidas de seguridad para proteger los datos personales en su posesión. Si por dicha omisión se presenta una vulneración será objeto de sanción.

- **Obstruir en la verificación de la autoridad**. Se presenta en caso de que el INAI decida realizar un proceso de verificación y el personal no facilite la información que se solicite, ni apoye a lo que se necesite realizar.

Además, el artículo 165 de la LGPDPPSO establece que las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de una violación a lo antes señalado, son independientes de las sanciones de orden civil, penal o de cualquier otro tipo que puedan derivar de los mismos hechos.

La reincidencia en el incumplimiento de las obligaciones será considerada como grave para efecto de sanciones administrativas.

[17] artículo 163 de La LGPDPPSO.

2.6 PARTICULARIDADES DE LAS VULNERACIONES RELACIONADAS CON PROCESOS ELECTORALES

El INE tiene entre sus fines integrar el Registro Federal de Electores, asegurar a la ciudadanía el ejercicio de sus derechos políticos y velar por la autenticidad y efectividad del sufragio.[18]

La Ley General en Materia de Delitos Electorales, establece como un delito electoral la **alteración en cualquier forma, sustitución, destrucción, comercialización o uso ilícito** de documentos relativos al Registro Federal de Electores, Padrón Electoral o Lista de Electores[19].

De igual forma se contempla como un delito electoral:		
La participación en la alteración del Registro Federal de Electores, Padrón Electoral o Listado de Electores;	La participación en la expedición ilícita de una o más credenciales para votar con fotografía;	La alteración, falsificación, destrucción, posesión, uso, adquisición, comercialización, suministro o transmisión de manera ilegal de archivos o datos de cualquier naturaleza, relativos al Registro Federal de Electores, Padrón Electoral o Listado de Electores.

[18] De conformidad con lo establecido en el artículo 30, párrafo 1, incisos c) d) y f) de la Ley General de Instituciones y Procedimientos Electorales.

[19] Artículo 8, fracción I Ley General en Materia de Delitos Electorales.

Atendiendo a la relevancia de los documentos relacionados con el Registro Federal de Electores es necesario agregar particularidades al proceso de atención de vulneraciones, por lo que el área propietaria además de atender a lo establecido en el *Apartado II. Gestión y notificación de vulneraciones* del presente documento, **se sugiere considerar lo siguiente en la determinación de responsabilidades**:

- Concentrar los documentos relacionados con la atención del incidente que vulneró la seguridad de los datos personales, así como las evidencias que se hayan tomado para su atención.
- Generar dos juegos de copias certificadas para remitirlos a la Dirección Jurídica del INE, con la finalidad de presentar una denuncia ante la FEDE y a la Unidad Técnica de lo Contencioso Electoral para que, en caso de considerar procedente, inicie un Procedimiento Ordinario Sancionador[20], a través de su área legal.
- Atender a lo establecido en los Lineamientos del Instituto Nacional Electoral para la atención de requerimientos de información y documentación, formulados en términos de lo dispuesto en el artículo 126, párrafo 3 de la Ley General de Instituciones y Procedimientos Electorales.

[20] Responsable de tramitar el Procedimiento Sancionador, de conformidad con el artículo 71 inciso a) del Reglamento Interior del INE

3 Apartado II. Gestión y notificación de vulneraciones

Este apartado se divide en dos fases:

1. **Preparación**. Incluye información que es recomendable que el área propietaria disponga para gestionar de manera óptima un escenario de vulneración.
2. **Respuesta**: Integra todas las actividades que el área propietaria debe llevar a cabo para atender la vulneración.

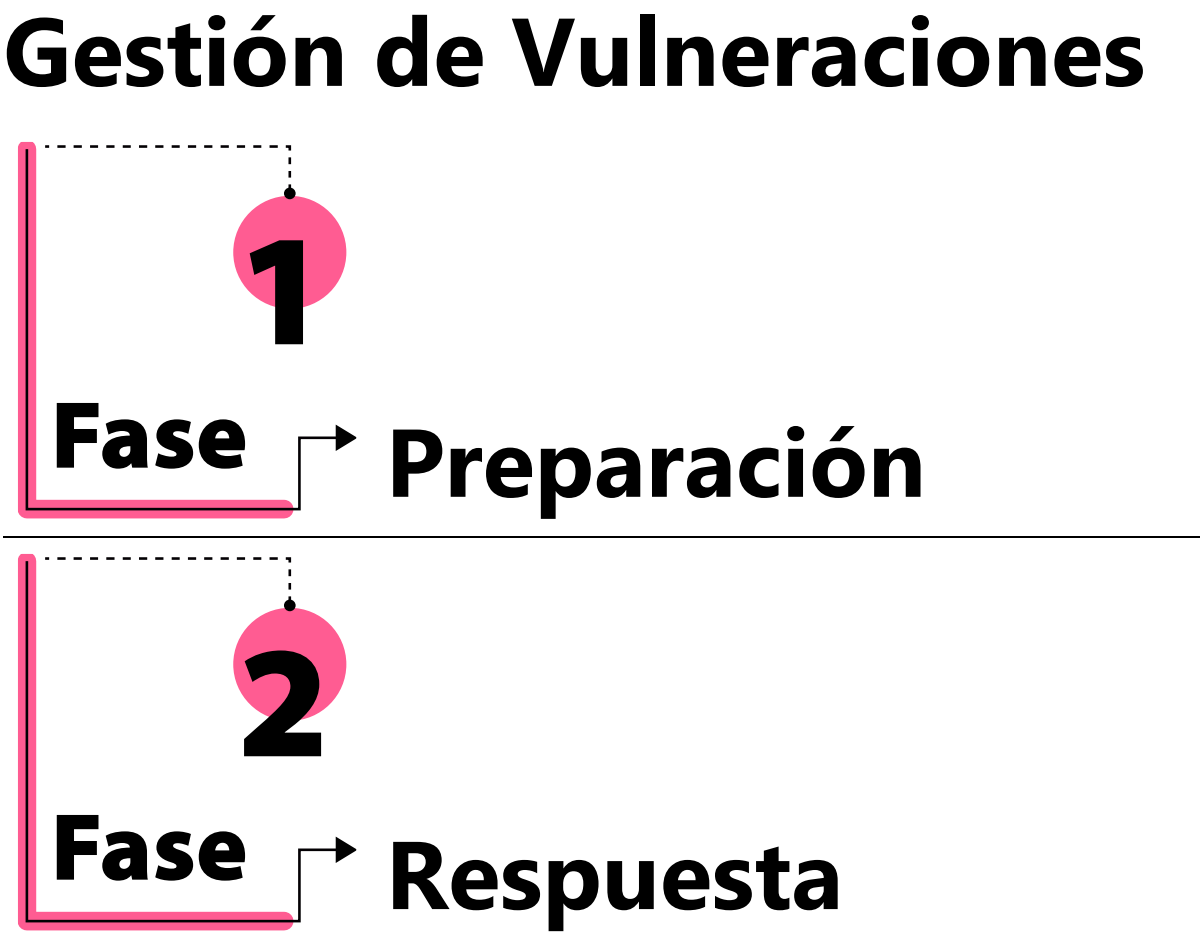
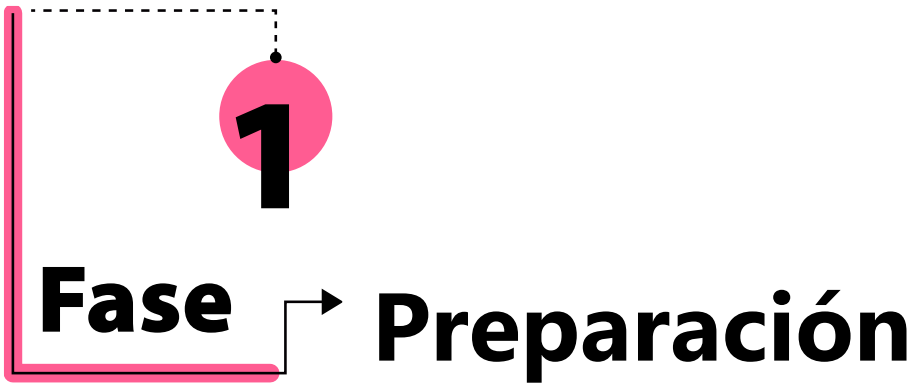


Figura 2. Fases para la atención de vulneraciones

a. Fase 1. Preparación

Esta fase atiende a la pregunta: **¿Cómo me preparo antes de que ocurra una vulneración?**



En la medida en que las personas estén preparadas para afrontar una vulneración podrán responder de forma rápida, ordenada y eficaz (**capacidad de respuesta**) ante dicha situación, minimizando las consecuencias tanto para los titulares como para el Instituto, por lo que se sugiere que las áreas propietarias:

a) Dispongan de un Plan de respuesta a incidentes.

Es recomendable y, en algunos casos obligatorio -dependiendo del tipo, cantidad de datos personales tratados, número de titulares y riesgos de privacidad identificados- que las áreas propietarias cuenten con procedimientos o planes de actuación denominados *Planes de respuesta a incidentes*[21]. Estos planes incluyen, entre otros puntos, la forma de detectar las alertas de seguridad para determinar si se trata de un incidente, así como las especificaciones sobre las herramientas y equipo a utilizar para su atención.

Lo anterior también aplica a los Encargados, para permitir un tratamiento adecuado de los datos personales y una comunicación apropiada con los responsables.

[21] Si desea conocer más acerca de este tema, pude consultar la norma internacional *ISO/IEC 27035 Gestión de Incidentes de Seguridad*, que es una guía para la localización, análisis y evaluación de vulnerabilidades e incidentes, así como las recomendaciones del Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) en su documento "*Computer Security Incident Handling Guide*" – SP 800-61 Rev.2

b) Identifiquen a los contactos.

Para gestionar las vulneraciones es necesario que el área propietaria identifique claramente a las personas que estarán involucradas, mediante las siguientes actividades:

- Designar un enlace. Especificar una persona que funja como enlace para que mantenga comunicación con la Unidad de Transparencia. Puede ser personal de la propia área o bien, el enlace de protección de datos personales;
- Elaborar un directorio. Elaborar y mantener en constante actualización el directorio con los datos de contacto del personal asignado para atender las vulneraciones -esto incluye áreas técnicas, usuarias o las que se considere necesario- y compartirlo con quienes estén involucrados en la atención de incidentes.

c) Firmen acuerdos de confidencialidad.

Es recomendable que las personas designadas para la atención de vulneraciones firmen acuerdos de confidencialidad, con la finalidad de que la información no se divulgue a personas no autorizadas.

Los acuerdos deben contener, al menos:

- Nombre, puesto, área de adscripción y número de empleado/a.
- La función que el personal desempeñará en la atención de vulneraciones.
- El compromiso que tiene el personal de guardar la secrecía y discreción sobre la información en cualquier formato -verbal, impreso, digital, entre otros formatos- a la que tendrá acceso y/o conocimiento, durante su relación laboral y una vez que esta haya finalizado.

- El impedimento que tiene el personal de utilizar la información para fines distintos a la atención de las vulneraciones, limitándose a cumplir con las actividades bajo su responsabilidad. Por lo que no podrá utilizarla, difundirla, reproducirla, publicarla, cederla, venderla y/o usarla para fines personales, lucrativos, comerciales o en beneficio de terceros.
- Que la información podrá ser clasificada como reservada o confidencial, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública.
- Las sanciones a las que podría ser acreedor en caso de divulgar y/o revelar la información.

En el Anexo I de este documento, se dispone de un formato de Acuerdo de confidencialidad.

d) Determinen los medios para comunicar las vulneraciones.

Este paso es importante para establecer una eficiente comunicación entre el personal que designado para su atención. Por lo que es necesario establecer un procedimiento de comunicación y escalación de vulneraciones, que contenga, al menos:

a. La definición de los canales apropiados para garantizar una comunicación ágil del incidente, entre ellos correo electrónico institucional, llamadas telefónicas, mensajería instantánea (WhatsApp, telegram, signal, por mencionar algunos).

b. El nombre del contacto oficial a quien se debe informar una posible vulneración.

c. Dar a conocer a las y los usuarios cómo reportar brechas o debilidades que identifiquen puedan poner en riesgo la seguridad de los datos personales y a través de qué medios pueden reportar.

Respecto a la forma de enviar la información, el procedimiento debe contemplar su confidencialidad, integrando en algún apartado lo siguiente:

i. Para el envío de información digital.

i. Especificar el uso de correo institucional, evitando conectarse a redes públicas; de no ser posible, hacer uso de una red privada virtual (VPN, por sus siglas en inglés), provista por el Instituto.

ii. De requerirse, utilizar la Firma Electrónica Avanzada Institucional.

iii. Uso de criptografía[22]:

   1. Cifrar toda la información mediante criptografía de llave pública -previo a su transmisión o almacenamiento en medios electrónicos (disco compacto, memoria *flash*, USB o cualquier otro soporte documental digital).

ii. Para el envío de la información impresa.

iv. Enviar la documentación a través de mensajería institucional o en su caso, servicios de mensajería previamente contratados por el Instituto.

v. De considerarse necesario, monitorear la ruta que se sigue en el traslado de la información a través de:

   1. En caso de mensajería institucional, a través de comunicación directa con el mensajero desde la salida de la información y hasta su entrega o uso de un Sistema de Posicionamiento Global (GPS, por sus siglas en inglés);

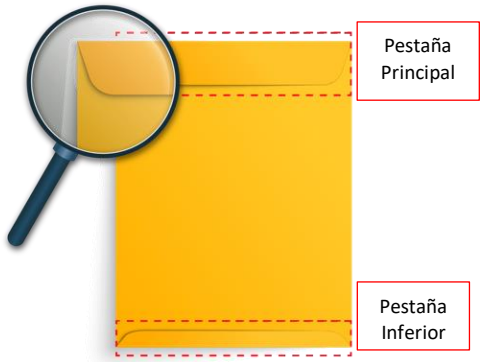
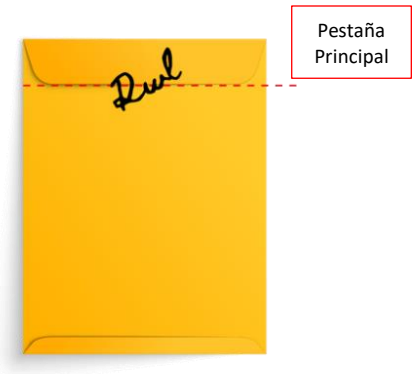
   2. En caso de mensajería externa, a través de números guía de identificación del paquete que el servicio de mensajería proporcione.

vi. Entregar la información impresa referente a la vulneración de manera personal a la o el destinatario con acuse de recibo, sello y firma, indicando la hora y fecha de recepción.

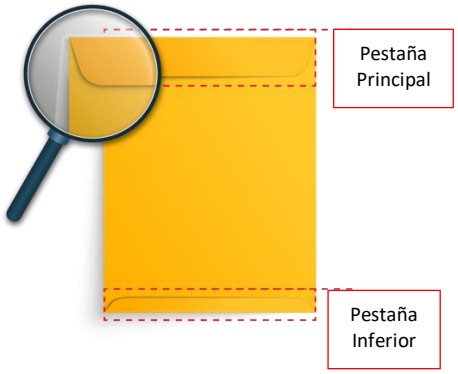
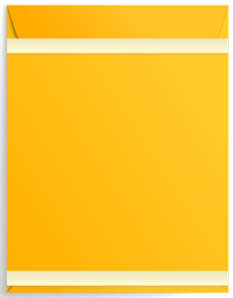
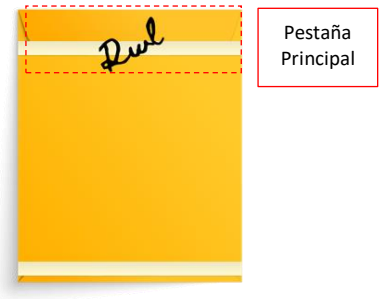
vii. Concentrar los documentos en un sobre cerrado, tomando en cuenta las siguientes consideraciones:

[22] Para más información respecto de este tema y del software a utilizar, se sugiere consultar a las áreas de TI o de seguridad de la información del Instituto.

1. Si dispone de cinta adhesiva de seguridad

1. Identificar todas las uniones de apertura del sobre. 	2. La persona responsable o propietaria debe colocar su firma autógrafa o rúbrica entre la pestaña de apertura principal del sobre y el cuerpo de este. 
3. Colocar la cinta adhesiva de seguridad sobre las uniones de apertura del sobre. 	4. Adherir una etiqueta en la parte frontal del sobre que contenga los siguientes datos: • Nombre del destinatario. • Dirección de destino, y • La leyenda ***"Esta información contiene datos personales y puede ser sujeta a clasificación".*** 

2. Si dispone de una cinta de enmascarar o *masking tape.*

1. Identificar todas las uniones de apertura del sobre. 	2. Colocar cinta de enmascarar *(masking tape*) sobre las uniones de apertura. 
3. La persona responsable o propietaria debe colocar su firma autógrafa o rúbrica sobre la cinta de enmascarar asegurándose que el trazo alcance la pestaña de apertura principal y el cuerpo del sobre. 	4. Adherir una etiqueta en la parte frontal del sobre que contenga los siguientes datos: • Nombre de la persona destinataria; • Dirección de destino, y • La leyenda ***"Esta información contiene datos personales y puede ser sujeta a clasificación".*** 

e) Establecer simulacros.

El área propietaria debe establecer escenarios en los cuales se simule un incidente que vulnere la seguridad de los datos personales, para generar una práctica en su manejo y responder de mejor forma en caso de que suceda. Se sugiere realizar estos ejercicios al menos una vez al año.

Los simulacros deben:

- Involucrar a todas las áreas que intervienen en el tratamiento de los datos personales durante todo su ciclo de vida.
- Involucrar los activos secundarios que involucran tratamiento de datos personales.
- Tomar en cuenta los escenarios de riesgos identificados en sus análisis de riesgos de privacidad y datos personales.
- En caso de requerirse, involucrar a las áreas de TI o de seguridad informática del Instituto.

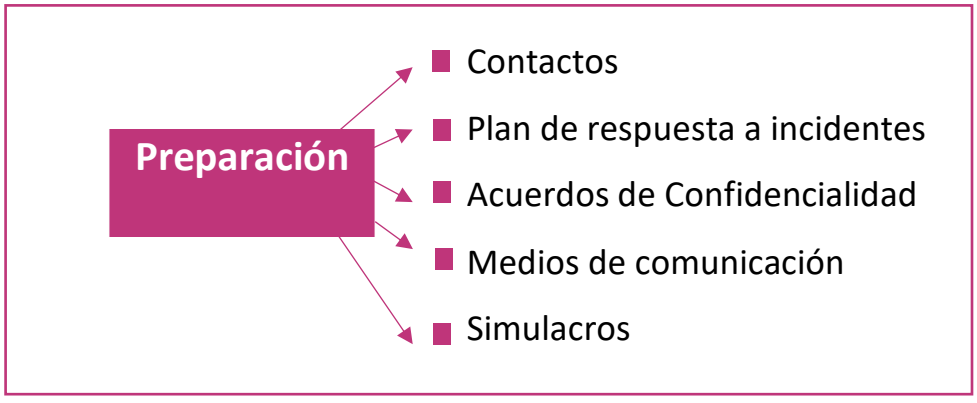
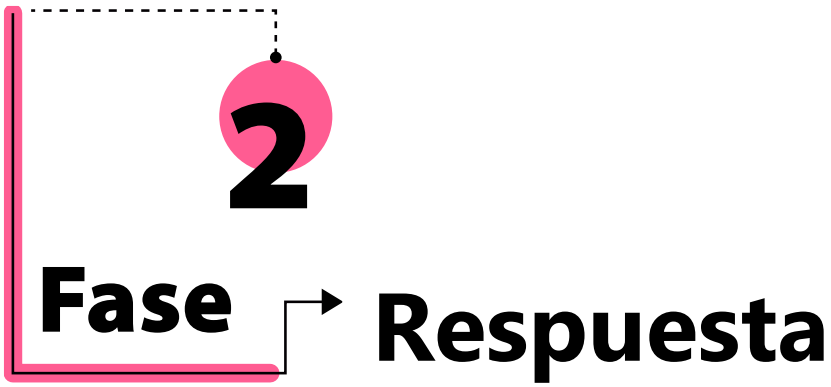


Figura 3. Elementos mínimos para prepararse ante una vulneración.

B. Fase 2. Respuesta

Esta fase atiende a la pegunta: **¿Qué acciones debo tomar para responder ante una vulneración?**



Para atender una vulneración, el área propietaria debe ejecutar las siguientes acciones:

Acción 1.
Confirma si un incidente vulneró la seguridad de los datos personales.

Acción 2.
Implementa acciones de mitigación (acciones correctivas de manera inmediata).

Acción 3.
Informa a la Unidad de Transparencia.

Acción 4.
Determina si se notifica la vulneración al titular y al INAI.

Acción 5.
Define acciones correctivas definitivas.

Acción 6.
Define acciones preventivas para evitar vulneraciones posteriores.

Acción 7.
Registra la vulneración en la bitácora.

Acción 1. Confirma si un incidente vulneró la seguridad de los datos personales

Para confirmar la vulneración, realizar lo siguiente:

Si, el área propietaria:	Entonces, debe:
a) Detecta una ejecución inadecuada de los procedimientos establecidos o sistemas informáticos que tratan datos personales provocando interrupción o desvío que pudiera afectar su seguridad. b) Recibe una notificación de un incidente de seguridad de la información que afecta sus procesos de negocio.	i. Identificar la cantidad de datos personales y número de titulares afectados. ii. Categorizar los datos personales afectados, (consultar el Anexo II de este documento). iii. Identificar si hubo activos secundarios afectados, mediante la detección de los sitios y medios de almacenamiento y el tipo de soporte documental donde están contenidos los datos personales. iv. Identificar el tipo de vulneración ocurrida, conforme a lo señalado en el *"Apartado I. Generalidades, inciso 2.2 ¿Qué tipo de vulneraciones existen?"* de este documento.

Si la vulneración incluye a un externo que funja como ENCARGADO, éste debe realizar las siguientes acciones:

a) Confirmar el incidente de seguridad.

b) Confirmar que el incidente comprometió datos personales.

c) Informar al área propietaria en un plazo **máximo de 36 horas**, a partir de la confirmación de la vulneración, a través de los medios establecidos en el contrato o instrumento legal.

d) Remitir, a través de los medios establecidos en el contrato o instrumento legal, la siguiente información:

- La naturaleza del incidente.
- Los datos personales que se vieron comprometidos.
- El nombre de la persona que reportó el incidente.
- Determinar junto con el área propietaria, las acciones correctivas que debe implementar el encargado para contener la vulneración.

Para lo anterior, el encargado debe:

1. Llenar el *Formato de Aviso de Vulneraciones para encargados* al área propietaria (disponible en el Anexo III de este documento).
2. Cifrarlo[23] con la llave pública del área propietaria.
3. Enviar el formato por correo electrónico a quien designe o haya designado el área propietaria en el contrato o instrumentos legales.

Para realizar esta actividad, en caso de considerarse necesario, puede solicitar apoyo del área custodia.

Acción 2. Implementa acciones de mitigación (acciones correctivas de manera inmediata)

Para implementar acciones de mitigación, el área propietaria debe realizar las siguientes actividades:

a) Disponer o definir un área de trabajo asignada para el análisis de las vulneraciones.

b) Recolectar la evidencia que permita investigar las causas.[24]

c) Analizar las evidencias obtenidas.

d) Generar el informe de resultados del análisis de la evidencia.

e) Determinar la causa de la vulneración y proponer las medidas temporales para contenerla.

f) En el caso de que aplique, disponer de ambientes de pruebas para verificar el correcto funcionamiento y compatibilidad de las acciones de mitigación que se pretenden implementar.

g) Implementar/ejecutar las medidas temporales de mitigación.

Para realizar esta actividad, en caso de considerarse necesario, puede solicitar apoyo del área custodia.

[23] Consultar con el área de TI o de Seguridad de la información del Instituto sobre el software a utilizar para el cifrado de la información.

[24] De considerarlo necesario puede tomar en consideración las Pautas para la recopilación y archivo de pruebas (RFC 3227 - *Guidelines for Evidence Collection and Archiving*, disponible en: https://www.ietf.org/rfc/rfc3227.txt) y el Procedimiento de cadena de custodia de la Procuraduría General de la República (ACUERDO A/009/2015, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015)

Acción 3. Informa a la Unidad de Transparencia

Notificar a la Unidad de Transparencia inmediatamente al momento de confirmar la vulneración y previa a la notificación de las y los titulares y al INAI para que, junto con el área propietaria, determinen si procede la notificación.[25]

Para lo anterior, el área propietaria -a través de quien designó para establecer la comunicación- debe:

4. Llenar el *Formato de Aviso de Vulneraciones* a la Unidad de Transparencia (disponible en el Anexo IV de este documento).
5. Cifrarlo[26] con la llave pública de la Unidad de Transparencia.
   Descargue la llave pública **AQUÍ**.
6. Enviar el formato al correo electrónico notificavul.uttypdp@ine.mx.

Acción 4. Determina la notificación de vulneración al titular y al INAI

La Unidad de Transparencia y el área propietaria, analizarán la vulneración para determinar si es necesario notificar lo sucedido a las personas titulares afectadas y al INAI.

La condición para que el área propietaria notifique la vulneración es que afecte derechos patrimoniales o morales de la persona titular.

Para determinar la afectación, el área propietaria y la Unidad de Transparencia, identificarán si la vulneración afectó uno o varios de los siguientes aspectos:[27]

[25] Si bien el artículo 35 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales establece que los órganos del Instituto deben avisar a la Unidad de Transparencia de la vulneración al mismo tiempo que notifiquen a las personas titulares, se sugiere que esta acción se realice de forma previa.

[26] Consultar con el área de TI o de Seguridad de la información del Instituto sobre el software a utilizar para el cifrado de la información.

[27] Artículo 66 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Derechos patrimoniales

- Bienes muebles e inmuebles;
- Información fiscal;
- Historial crediticio;
- Ingresos y egresos;
- Cuentas bancarias;
- Seguros;
- Afores;
- Fianzas;
- Servicios contratados, o
- Cantidades o porcentajes relacionados con la situación económica de la persona titular.

Derechos morales

- Sentimientos;
- Afectos;
- Creencias;
- Decoro;
- Honor;
- Reputación;
- Vida privada;
- Configuración y aspecto físico;
- Consideración que de sí mismo tienen los demás, o
- Cuando menoscabe ilegítimamente la libertad o integridad física o psíquica de la persona titular.

¿Hubo afectación de los derechos patrimoniales o morales de las personas titulares?	**Entonces** el área propietaria debe:
Sí	a) Notificar a la persona titular[28]. b) Notificar al INAI[29] con apoyo de la UTTyPDP.
No	**Iniciar con la implementación de las acciones correctivas definitivas** (contenidas en el apartado Acción 5. de este documento).

El área propietaria contará con un **plazo máximo de 72 horas** para notificar al **INAI** y a la persona titular a partir del momento de la confirmación de la vulneración.

a) Notificar a la persona titular

El área propietaria debe elaborar la notificación de forma clara y sencilla, tomando en consideración que va dirigida a las personas titulares de los datos personales y únicamente debe incluir información sobre la vulneración.

La información que debe contener es la siguiente:[30] [31]

- La naturaleza del incidente o vulneración ocurrida.
- Los datos personales comprometidos.
- Las recomendaciones dirigidas a la persona titular sobre las medidas que podría adoptar para proteger sus intereses, mediante un listado de acciones a realizar para minimizar los efectos adversos propiciados por la vulneración.
- Las acciones correctivas realizadas de forma inmediata por parte del responsable.
- Los medios puestos a disposición de la persona titular para que pueda obtener más información al respecto.
- La descripción de las circunstancias generales en torno a la vulneración, que ayude a la persona titular a entender el impacto del incidente.

[28] Artículo 34 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.
[29] Artículo 35 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.
[30] Artículo 68 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
[31] Artículo 41de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- Cualquier información o documentación que considere conveniente para apoyar a las y los titulares.

La notificación a la persona titular puede realizarse de dos formas:

1. **Directa.** A través de correo electrónico, teléfono, correo postal o en persona, y puede utilizarse más de un medio de comunicación.
2. **Indirecta.** Mediante la publicación en sitios web oficiales y medios de comunicación masivos. Se realiza en caso de que la notificación directa se encuentre en uno de los siguientes supuestos:

- Pueda causar más afectaciones a la persona titular.
- Sea muy costosa.
- No cuente con la información de contacto.

El área propietaria tiene la obligación de notificar la vulneración a la persona titular a través de los mismos medios de comunicación con los que el Instituto mantiene contacto con ella, asegurándose que cuenten con las siguientes características:

- Ser gratuitos.
- De fácil acceso.
- Con amplia cobertura.
- Que estén debidamente habilitados y disponibles en todo momento para la o el titular[32].

El medio seleccionado para notificar a las personas titulares dependerá del número de afectados.

Ejemplo:

Una Universidad tiene un programa de becas para personas de escasos recursos. Todos los estudiantes tienen la oportunidad de participar, pero únicamente 100 personas obtienen la beca.

[32] Artículo 68 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Después del proceso de selección, el área propietaria envía a su área de TI los nombres de las personas seleccionadas y solicita que el listado se publique en la página de la Universidad.

Sin embargo, en vez de publicar la información de las personas que obtuvieron la beca, se cargó en la página el concentrado de los exámenes psicométricos de las y los estudiantes, que incluye el nombre completo, correo electrónico y sus resultados, derivando en una divulgación no autorizada.

Por lo anterior, el responsable debe notificar a los alumnos la vulneración.

A continuación, se presenta la notificación enviada por la universidad a cada de los titulares involucrados mediante correo electrónico, donde se observan los elementos que debe contener atendiendo a la normativa.

Para: estudiante@universidad.edu
Asunto: Notificación sobre vulneración de Datos Personales

Estimada Alumna:

La naturaleza del incidente o vulneración ocurrida.

Hago de su conocimiento que, por un error involuntario, personal de esta Universidad publicó los resultados de los exámenes psicométricos de los estudiantes de nuevo ingreso, entre ellos los relacionados con usted. Los datos publicados son:

Los datos personales comprometidos.

- Nombre completo.
- Correo electrónico.
- Resultados obtenidos en el examen psicométrico (puntaje).

Las acciones correctivas realizadas de forma inmediata por parte del responsable.

En este sentido, la universidad eliminó de la página institucional dicha información, con la finalidad de que la misma no causara daños a las personas titulares.

La descripción de las circunstancias generales en torno a la vulneración, que ayude a la persona titular a entender el impacto del incidente.

Cabe destacar que la publicación del resultado de su examen psicométrico (puntaje), es un dato personal que puede dar origen a discriminación y afecta sus derechos morales, dañando la imagen que usted y los demás tienen de su persona.

Las recomendaciones dirigidas a la persona titular sobre las medidas que podría adoptar para proteger sus intereses, mediante un listado de acciones a realizar para minimizar los efectos adversos propiciados por la vulneración.

Por lo anterior, se recomienda que acuda a la Secretaría Académica, en caso, de que enfrente situaciones discriminatorias y/o acoso escolar, con la finalidad de tomar las medidas conducentes.

Los medios puestos a disposición de la persona titular para que pueda obtener más información al respecto.

Finalmente, le comento que, en caso de cualquier duda respecto al presente correo, puede comunicarse con la directora del Plantel a su correo institucional dirección@universidad.edu o, bien, acudir de manera personal a las oficinas de la Dirección.

b) Notificar al INAI

La Unidad de Transparencia es la encargada de notificar al INAI sobre la vulneración[33] en un plazo máximo de 72 horas, que comenzará a correr el mismo día natural en que el área propietaria confirme la vulneración.

La información mínima que el área propietaria debe enviar a la UTTyPDP es: [34]

- Hora y fecha de la identificación de la vulneración;
- Hora y fecha del inicio de la investigación sobre la vulneración;
- La naturaleza de la vulneración ocurrida;
- Descripción detalla de las circunstancias en torno a la vulneración ocurrida;
- Categorías y número aproximado de personas titulares afectadas;
- Sistemas de tratamiento y datos personales comprometidos;
- Acciones correctivas realizadas de forma inmediata;
- Descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
- Las recomendaciones dirigidas a la persona titular;
- El medio puesto a disposición del titular para que pueda obtener más información al respecto;
- Nombre completo de la o las personas designadas y sus datos de contacto, o
- Cualquier otro dato complementario que considere conveniente y que proporcione más información acerca de la vulneración.

[33] Artículo 35 del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales.
[34] Artículo 67 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Para tal efecto, la Unidad de Transparencia elaboró el *Formato de notificación al INAI* (disponible en el Anexo V de este documento), el cual debe ser completado y enviado.

Si el envío es digital	Si el envío es físico
1. Cifrar[35] el documento con la llave pública de la Unidad de Transparencia. Descargue la llave pública **AQUÍ**. 2. Enviar el formato cifrado al correo electrónico notificavul.uttypdp@ine.mx.	Enviar mediante oficio, siguiendo las recomendaciones de la **Fase 1. Preparación, inciso d)** de este apartado.

En ambos casos el **plazo máximo para la notificación es de 36 horas** que comenzará a correr el mismo día natural en que el área propietaria confirme la vulneración, para que la Unidad notifique al INAI dentro de las 72 horas que la Ley señala.

Una vez realizada la notificación por parte de la Unidad, el INAI determinará si inicia un procedimiento de verificación.

La Figura 4, detalla la línea del tiempo desde la detección de un evento de seguridad hasta el momento de avisar a la persona titular y al INAI, en caso de que corresponda.

[35] Consultar con el área de TI o de Seguridad de la información del Instituto sobre el software a utilizar para el cifrado de la información.

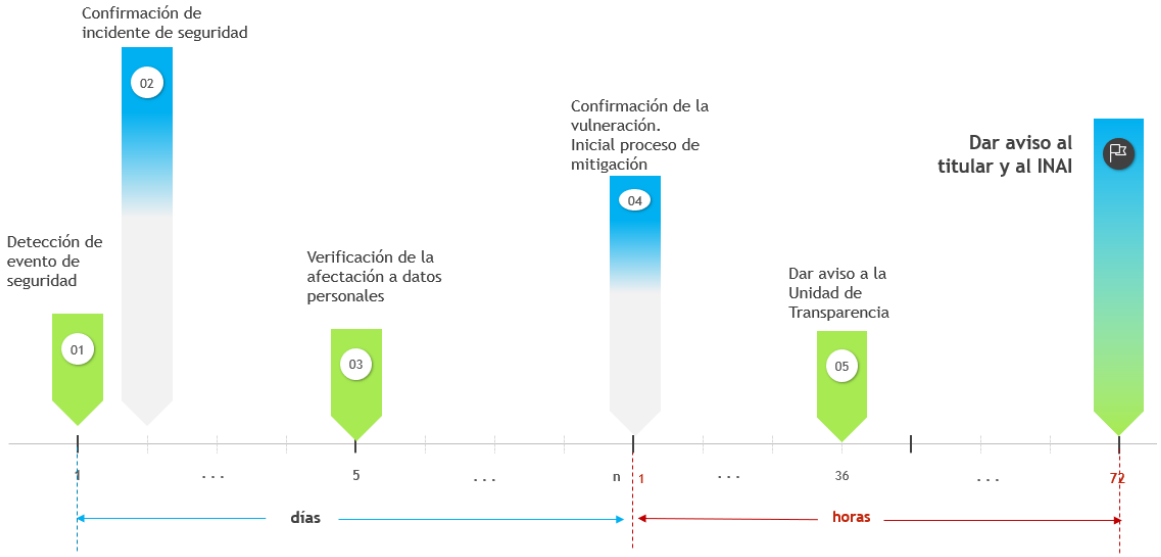


Figura 4. Línea del tiempo para notificar la vulneración al INAI y a las personas titulares.

Acción 5. Implementa acciones correctivas definitivas

El área propietaria debe implementar las acciones correctivas definitivas para resolver la vulneración.

Es necesario que estas acciones sean incluidas en el Plan de trabajo[36] de su Documento de Seguridad y estén enfocadas en implementar o mejorar las medidas de seguridad existentes necesarias para corregir las causas de la vulneración.

Para el caso del encargado, el área propietaria es quien debe autorizar las acciones correctivas que fueron previamente determinadas en conjunto, debiendo privilegiar la integridad, confidencialidad y disponibilidad de los datos personales afectados.

Para realizar esta actividad, en caso de considerarse necesario, puede solicitar apoyo del área de custodia.

Acción 6. Define acciones preventivas para evitar vulneraciones posteriores

Una vez que la vulneración fue confirmada, contenida y corregida, el área propietaria debe:

a) Definir e implementar las medidas de seguridad que prevengan que la vulneración se presente nuevamente u ocurra alguna similar.

[36] Artículo 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

b) Verificar que los activos secundarios y las medidas que los protegen operen con normalidad.

Para realizar esta actividad, en caso de considerarse necesario, puede solicitar apoyo del área custodia.

Acción 7. Registra la vulneración en la bitácora

Una vez atendida la vulneración, el área propietaria tiene la obligación de mantener un registro de todas las vulneraciones en una bitácora, con finalidad de documentar los detalles de lo sucedido y poder comunicar a todos los involucrados al interior del Instituto el estado de seguridad de los datos personales posterior al incidente.

La bitácora -en la que el área propietaria mantendrá un histórico- contendrá, al menos, la siguiente información:

Obligatorias

Artículo 39 de la LGPDPPSO y el 33 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

- La fecha en la que ocurrió la vulneración;
- Explicación breve de la vulneración;
- Descripción de la vulneración;
- Área de adscripción;
- Las acciones correctivas implementadas de forma inmediata;
- Las acciones correctivas implementadas de forma definitiva;
- Las acciones preventivas que, en su caso, puedan ser implementada para vulneraciones posteriores;
- Consecuencias y
- Motivación.

Complementarias

Se consideran como información relevante para futuras referencias con base en las buenas prácticas

- Nombre completo de la persona que da aviso;
- Puesto;
- Correo institucional;
- Extensión;
- Área de adscripción;
- Dirección de área;
- Hora en la que inició la vulneración;
- Fecha en la que se elaboró el reporte;
- Hora en la que se elaboró el reporte;
- Fecha en la que concluyó la vulneración;
- Categoría de la vulneración;
- Acciones realizadas;
- Tipo de agente malicioso;
- Descripción del agente malicioso;
- Referencia y localización del agente malicioso;

- Información/Datos comprometidos;
- Hardware;
- Software;
- Comunicaciones;
- Documentación soporte;
- Proceso;
- Brecha de confidencialidad;
- Brecha de integridad;
- Brecha de disponibilidad;
- Destrucción;
- Lineamiento, política o directriz no atendida, y
- Estatus de la vulneración.

La Unidad de Transparencia elaboró el formato *Bitácora de Vulneraciones de Seguridad de los Datos Personales* para que las áreas propietarias lleven su registro y seguimiento.

Su uso es de observancia obligatoria[37] y puede descargarse AQUÍ.

[37] De conformidad con el artículo 36 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

4. ANEXOS

A continuación, se incluyen en el documento -y para su descarga- los siguientes formatos y documentos de apoyo para la gestión de las vulneraciones:

Número	Formatos
I.	**Formato de acuerdo de confidencialidad** *(con hipervínculo para descarga).*
II.	**Categorización de datos personales.**
III.	**Formato de Aviso de Vulneraciones para Encargados** *(con hipervínculo para descarga).*
IV.	**Formato de Aviso de Vulneraciones a la UTTyPDP** *(con hipervínculo para descarga).*
V.	**Formato de Aviso de Vulneraciones para notificar al INAI** *(con hipervínculo para descarga).*

Para el uso de los formatos, considerar lo siguiente:

- El texto en color **negro** se encuentra predeterminado.
- El texto en *azul y cursiva* es utilizado para explicar y/o ejemplificar, por lo que debe ser eliminado o modificado, según corresponda.
- En caso de requerir la firma de documentos:
    - Firma autógrafa, se deberá rubricar la primera página y firmar en la segunda, en el recuadro asignado.
    - Firma Electrónica Avanzada Institucional (FEA), únicamente se asentará en el recuadro asignado el nombre de la personal incorporando la leyenda "*Firmado electrónicamente*"; posteriormente, firmar el documento mediante la FEA.

Acuerdo de Confidencialidad

El/La que suscribe *nombre completo*, en mi calidad de *puesto que desempeña* de la *Dirección de área*, identificándome con el número *señalar número de empleado*, como *empleado/empleada* del Instituto Nacional Electoral, en relación con la gestión de vulneraciones que pudieran presentarse en el *sistema/proceso de negocio/servicio*, donde desempeño la función de *señalar la función que desempeñará*.

Atendiendo a mis obligaciones y responsabilidades reconozco que tendré acceso a información susceptible de ser clasificada como confidencial o temporalmente reservada.

Además, entiendo que el acceso a tal información, sin importar su fuente, sea verbal, escrita, impresa, virtual o cualquier otra, tendrá el único propósito de cumplir con actividades requeridas en la gestión de vulneraciones, por lo que me comprometo a:

1. Desempeñar las actividades que me correspondan, bajo los principios de legalidad, profesionalismo, honradez, lealtad, integridad y eficiencia.
2. Facilitar las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes que correspondan.
3. Guardar cabal y absoluta secrecía y discreción durante y aún concluida mi relación laboral con el Instituto.

Por lo anterior, no podré utilizarla, difundirla, divulgarla, reproducirla, publicarla, cederla, transferirla, alterarla, falsificarla, destruirla, enajenarla de manera personal o por conducto de terceros, por cualquier medio a persona alguna y/o usarla con fines personales, lucrativos, comerciales u otro, en beneficio propio o de terceros y, en general, realizar cualquier acción no autorizada por escrito o contraria a los intereses del INE, que pueda poner en riesgo la ejecución de las funciones y atribuciones del Instituto.

En el marco de todo lo observado acepto:

a) La posibilidad de ser sujeto de responsabilidades administrativas, civiles y penales en caso de incurrir en alguna de las acciones, omisiones o violaciones estipuladas en el presente acuerdo,
b) Abstenerme de participar en cualquier acto u omisión en el que exista la posibilidad de tener un conflicto de interés,
c) Estar obligado a notificar de forma inmediata a mi superior jerárquico y al área administrativa pertinente, en caso de tener conocimiento de algún hecho hipotético similar a los señalados en los incisos anteriores.

Lo anterior con base en los siguientes preceptos normativos:

- Artículos 3, 110 fracción VI, 113, 174 y 186, fracción IV de la Ley Federal de Transparencia y Acceso a la Información Pública.
- Artículos 4, 113, fracción VI, 116, 201 y 206 fracción IV de la Ley General de Transparencia y Acceso a la Información Pública.
- Artículos 6, 7, 153, 163 y 165 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Artículo 75 de la Ley General de Responsabilidades Administrativas.
- Artículos 126, párrafo 3 y 480 de la Ley General de Instituciones y Procedimientos Electorales.
- Artículos 5, 8 fracciones I y XI y 13 fracción II Ley General en Materia de Delitos Electorales.
- Artículos 14 y 15 del Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública.
- Artículo 7 del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales.
- Artículo 71, fracción XVIII del Estatuto del Servicio Profesional Electoral Nacional.
- Artículos 140, 210, 211, 211 Bis, 214 fracción IV, 220 fracción II del Código Penal Federal.

Leído el presente acuerdo de confidencialidad y con conocimiento de los derechos y obligaciones que de ella emanan, manifiesto mi conformidad con sus términos y asumo sin restricción alguna, las condiciones y responsabilidades que me correspondan, así como las consecuencias que deriven del incumplimiento de los compromisos establecidos por el INE, en las leyes mexicanas y en las normas institucionales.

Ciudad de México o entidad federativa a la que pertenezca a *día* de *mes* de *año.*

Nombre y firma del empleado

Categorización de datos personales de acuerdo con su tipo		
Categoría	**Tipo de datos personales** *(con ejemplos)*	**Riesgo inherente**
Estándar	**Identificación y contacto, laborales y académicos**. Como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, domicilio, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.	**BAJO**
Sensible	**De Ubicación física de la persona**, la relativa al tránsito de las personas dentro y fuera del país (geolocalización) y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más (dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.).	**MEDIO**
	De patrimonio. Todos aquellos que permitan inferir el patrimonio de una persona, incluye entre otros, saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados, número de tarjeta bancaria de crédito y/o débito.	**MEDIO**
	De autenticación. Información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.	**MEDIO**
	Jurídicos, como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.	**MEDIO**

Categorización de datos personales de acuerdo con su tipo		
Categoría	**Tipo de datos personales** *(con ejemplos)*	**Riesgo inherente**
Sensible	Todos aquellos que afecten la esfera más íntima de su titular, es decir, los que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular, como revelar aspectos del origen racial o étnico, estado de salud, pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales, entre otros, según el caso en concreto.	**ALTO**
Especial	Son todos los datos que pueden causar daño directo a los titulares, debido a su naturaleza o bien, debido a un cambio excepcional en el contexto de las operaciones usuales, como: • información adicional de la tarjeta bancaria -número de tarjeta de crédito o débito más cualquier otro dato relacionado o contenido en la misma (fecha de vencimiento, código de seguridad, datos de la banda magnética, número de identificación personal PIN • Conjunto de varios tipos de datos personales en una base de datos.	**REFORZADO**

Formato de Aviso de Vulneraciones para Encargados

- Fecha de la identificación de la vulneración | dd/mm/aaaa

Descripción de la Vulneración

Descripción general de la vulneración.	*Justificación*
Acciones correctivas implementadas de forma inmediata	*Justificación*
El nombre de la persona que reportó el incidente.	*Justificación*

Datos Personales comprometidos

Categoría	Listado de datos personales
Justificación	*Justificación*

Información complementaria

Puesto *(de la persona que da aviso)*	*Justificación*
Correo institucional *(de la persona que da aviso)*	*Justificación*

Hora en la que inició la vulneración	*Indicar en un formato de 24:00 horas*
Fecha en la que se elaboró el reporte	*dd/mm/aaaa*
Hora en la que se elaboró el reporte	*Indicar en un formato de 24:00 horas*
Fecha en la que concluyó la vulneración	*dd/mm/aaaa*
Categoría de la vulneración	*Justificación*
Acciones realizadas	*Justificación*
Tipo de agente malicioso	*Justificación*
Descripción del agente malicioso	*Justificación*
Referencia y localización del agente malicioso	*Justificación*
Estatus de la vulneración	*Justificación*

Componentes/Activos afectados	
Información/Datos comprometidos	*Justificación*

Hardware	*Justificación*
Software	*Justificación*
Comunicaciones	*Justificación*
Documentación soporte	*Justificación*
Proceso	*Justificación*

Brecha de seguridad	
Brecha de confidencialidad	*Justificación*
Brecha de integridad	*Justificación*
Brecha de disponibilidad	*Justificación*
Destrucción	*Justificación*
Lineamiento, política o directriz no atendida	*Justificación*

Formato de Aviso de Vulneraciones a la UTTyPDP

Fecha de la identificación de la vulneración | dd/mm/aaaa

Descripción de la Vulneración	
Naturaleza de la vulneración	*Justificación*
Descripción de las circunstancias en torno a la vulneración ocurrida	*Justificación*
Acciones correctivas implementadas de forma inmediata	*Justificación*
Acciones implementadas para corregir los daños ocasionados	*Justificación*
Descripción de las posibles consecuencias de la vulneración ocurrida	*Justificación*

Información de activos secundarios comprometida	
Bases de datos	*Justificación*
Sistemas de tratamiento	*Justificación*

Datos Personales comprometidos	
Categoría	**Listado de datos personales**
Justificación	*Justificación*
Categoría	**Número aproximado de titulares afectados**
Justificación	*Justificación*

Formato de Aviso de Vulneraciones para notificar al INAI

Datos de la vulneración	
Fecha de la identificación de la vulneración	*dd/mm/aaaa*
Hora de la identificación de la vulneración	*Indicar en un formato de 24:00 horas*
Fecha de inicio de la investigación sobre la vulneración	*dd/mm/aaaa*
Hora de inicio de la investigación sobre la vulneración	*Indicar en un formato de 24:00 horas*

Descripción de la Vulneración	
Naturaleza	*Justificación*
Descripción de las circunstancias en torno a la vulneración ocurrida	*Justificación*
Acciones correctivas realizadas de forma inmediata (acciones realizadas para corregir los daños ocasionados)	*Justificación*

Información comprometida	
Bases de datos	*Justificación*
Sistemas de tratamiento	*Justificación*

Datos Personales comprometidos	
Categoría	**Listado de datos personales**
Justificación	*Justificación*
Categoría	**Número aproximado de personas titulares afectadas**
Justificación	*Justificación*

Adicional	
Las recomendaciones dirigidas a la persona titular	*Justificación*
El medio puesto a disposición de la persona titular para que pueda obtener más información al respecto	*Justificación*
Nombre completo de las personas designadas y datos de contacto	*Justificación*
Comentario adicional sobre la vulneración	*Justificación*

VI. REFERENCIAS

AEPD. (s.f.). *Guía para la gestión y notificación de brechas de seguridad*. Recuperado el 25 de agosto de 2020, de https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

Bolaños-Burgos, F., & Gómez-Giacoman, C. (Noviembre 2015 de Año 4 No. 3 No). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. *Revista electrónica de computación, informática, biomédica y electrónica*. Obtenido de http://recibe.cucei.udg.mx/revista/es/vol4-no3/computacion01.html

Estandarés de Protección de Datos Personales para los Estados Iberoamericanos. (20 de junio de 2017). Obtenido de Institito de Transparencia Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios: https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (3 de octubre de 2017). *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679*. Obtenido de Agencia Española de Protección de Datos Personales: https://www.aepd.es/media/criterios/wp250rev01-es.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (junio de 2018). *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*. Obtenido de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

ISO/IEC. (2011). Information technology - Security techniques - Privacy framework. *ISO/IEC 29100:2011*.

McCallister, E., Grance, T., & Scarfone, K. (April de 2010). Guide to protecting the confidentiality of personal identifiable information (PII). *Special Publication 800-122*. Gaithersburg.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo . (27 de abril de 2016). Obtenido de Agencia Estatal Boletín Oficial del Estado : https://www.boe.es/doue/2016/119/L00001-00088.pdf

Technology, N. I. (08 de 2012). *Computer Security Incident Handling Guide*. Obtenido de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf