



ECIJA  
GPA

Ecuador

NOTA INFORMATIVA

**Análisis y  
Recomendaciones  
sobre el Formulario en  
línea para la  
Notificación de  
Vulneración de la  
Seguridad de los Datos  
Personales**

Área de Derecho de Tecnologías, Medios,  
Telecomunicaciones, Ciberseguridad y  
Protección de Datos Personales



# Análisis y Recomendaciones sobre el Formulario en línea para la Notificación de Vulneración de la Seguridad de los Datos Personales

**DICIEMBRE 2024**

---

## Antecedentes

La Superintendencia de Protección de Datos Personales (SPDP) ha habilitado un Formulario en línea para la Notificación de Vulneración de la Seguridad de los Datos Personales, accesible a través del portal <https://spdp.gob.ec/vulneraciondatos/>

Este mecanismo tiene como objetivo facilitar a los responsables del tratamiento de datos el cumplimiento de la obligación de reportar incidentes de seguridad, tal como lo establece la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General.

En este informe, se realiza un análisis de las secciones del formulario, destacando su estructura, los requisitos específicos y los elementos críticos que los responsables deben considerar al momento de completarlo. Asimismo, se proporcionan recomendaciones mínimas para garantizar la transparencia, la diligencia y la efectividad del proceso de notificación, en línea con los principios

de protección de datos y la prevención de riesgos para los titulares afectados.

Este análisis busca orientar a las organizaciones sobre la importancia de cumplir con los requerimientos normativos y contribuir al fortalecimiento de la confianza en el manejo de los datos personales.

## Análisis de la Sección de Identificación en el Formulario de Notificación de Vulneraciones de Seguridad

La primera pantalla del formulario de notificación de vulneraciones de seguridad de datos personales es clave para iniciar correctamente el proceso de notificación ante la Superintendencia de Protección de Datos Personales. Este análisis tiene como objetivo orientar a los responsables del tratamiento sobre cómo cumplimentar correctamente esta sección.

## Elementos del Formulario y Cómo Cumplimentarlos

### Selección del tipo de vulneración

- **Confidencialidad:** Seleccione esta opción si los datos han sido accedidos o divulgados sin autorización. Ejemplo: un ciberataque que expone información personal de clientes.
- **Disponibilidad:** Marque esta opción si los datos no están accesibles o han sido destruidos. Ejemplo: un fallo técnico que elimina registros importantes o un ataque de ransomware.

- **Integridad:** Utilice esta opción si los datos han sido alterados o corrompidos sin autorización. Ejemplo: modificaciones no autorizadas en una base de datos.

*Consejo práctico:* Si tiene dudas sobre cuál categoría elegir, piense en el impacto principal del incidente:

- ¿Se expusieron datos? (Confidencialidad)
- ¿No puede acceder a los datos? (Disponibilidad)
- ¿Los datos están alterados o incompletos? (Integridad)

### Explicación de la naturaleza de la vulneración

**Descripción breve del incidente:** Indique qué ocurrió. Ejemplo: "Un acceso no autorizado a nuestra base de datos de clientes permitió la exposición de información de contacto."

**Contexto del incidente:** Explique cómo ocurrió el evento. Ejemplo: "Un ataque cibernético dirigido a nuestras credenciales de administrador comprometió el servidor principal."

**Tipo de datos afectados:** Mencione los datos comprometidos. Ejemplo: nombres, correos electrónicos, información financiera.

*Consejo práctico:* Sea claro y directo. Evite términos técnicos innecesarios y céntrese en lo esencial: qué pasó, qué datos están comprometidos y en qué contexto ocurrió.

*Elementos implícitos que deben ser considerados:* Aunque esta pantalla no solicita explícitamente detalles

sobre algunos aspectos requeridos por el Reglamento, es importante que los responsables del tratamiento los incluyan indirectamente en la explicación:

- ¿Hubo pérdida de control o acceso? Si el incidente implica que ya no tiene acceso o control sobre los datos (por ejemplo, debido a un ransomware), asegúrese de mencionarlo en la descripción.
- ¿Datos sensibles o de alto riesgo? Si la información afectada incluye datos sensibles (e.g., salud, financieros), esto debe destacarse.

**Impacto potencial en los titulares:** Reflexione si la vulneración podría afectar significativamente los derechos y libertades de las personas, y si es así, inclúyalo en la descripción.

Ejemplo: "La exposición de datos financieros podría derivar en un riesgo de fraude para los titulares."

**Temporalidad del incidente:** Por qué es relevante: Aunque esta pantalla no lo pide, el Reglamento exige que las notificaciones se realicen dentro de las 72 horas desde la detección del incidente. Por ello, en su descripción, incluya:

- Cuándo ocurrió el incidente.
- Cuándo se detectó.
- Si ya se han tomado medidas correctivas iniciales.

Ejemplo de inclusión en la descripción: "El incidente ocurrió el 1 de diciembre y fue detectado el 2 de diciembre. Inmediatamente se desactivaron las credenciales comprometidas y se contactó a los equipos de seguridad."

## Consideraciones Clave para Cumplimentar esta Sección

*No omita detalles relevantes:* Aunque la pantalla parece sencilla, la claridad y la precisión en la descripción son esenciales para que la Superintendencia pueda evaluar adecuadamente el riesgo asociado al incidente.

*Adapte la clasificación al impacto:* Si no está seguro de qué categoría seleccionar, evalúe el principal efecto del incidente (exposición, inaccessibilidad o alteración de los datos).

*Incluya elementos que no se solicitan explícitamente pero son importantes:* La pérdida de control, la naturaleza sensible de los datos y el impacto en los titulares deben estar presentes en la descripción, aunque no sean requeridos directamente.

## Conclusión

La correcta cumplimentación de esta primera pantalla es crucial para iniciar un proceso de notificación conforme a la normativa ecuatoriana. Al seguir estas recomendaciones, los responsables del tratamiento podrán garantizar que su notificación cumple con lo establecido en el Reglamento, minimizando riesgos regulatorios y facilitando la evaluación del incidente por parte de la autoridad.

## Preguntas clave para completar la primera pantalla del formulario de notificación de vulneración de seguridad

### 1. Identificación de la vulneración

- ¿Qué tipo de vulneración hemos

detectado?

- Confidencialidad: ¿Se han expuesto datos personales sin autorización?
- Disponibilidad: ¿No es posible acceder a los datos por un incidente?
- Integridad: ¿Han sido modificados los datos sin autorización, comprometiendo su integridad?
- ¿Cuál es la naturaleza del incidente?
  - ¿Cómo ocurrió la vulneración (acceso no autorizado, ataque externo, error humano, etc.)?
  - ¿Cuándo y cómo se detectó el incidente?
- ¿Qué datos personales se han visto afectados?
  - ¿Qué tipo de información fue vulnerada? (ej.: nombre, direcciones, información financiera, datos sensibles).
  - ¿Cuántos registros o individuos están comprometidos?
- ¿Cuál es el contexto de la vulneración?
  - ¿En qué sistema, plataforma o proceso ocurrió el incidente?
  - ¿Existían medidas de seguridad implementadas?

### 2. Evaluación del impacto

- ¿Quiénes son los afectados por el incidente?
  - ¿Se trata de empleados, clientes, usuarios, proveedores u otras partes?
  - ¿Existen personas vulnerables dentro del grupo afectado (menores, adultos mayores, etc.)?



- ¿Cuáles son las posibles consecuencias de la vulneración?
  - ¿La vulneración puede llevar a un robo de identidad, fraudes financieros o perjuicio reputacional?
  - ¿Qué nivel de riesgo representa para los derechos y libertades de los titulares de los datos?

### 3. Acciones tomadas

- ¿Se ha documentado internamente el incidente?
  - ¿Se cuenta con un registro del incidente que incluya hora, fecha y detalles relevantes?
  - ¿Qué responsables o equipos han participado en la identificación y gestión del incidente?
- ¿Se ha implementado alguna medida de contención o mitigación?
  - ¿Qué acciones inmediatas se han tomado para minimizar el impacto?
  - ¿Se ha limitado el acceso a los datos comprometidos o corregido las vulnerabilidades?
- ¿Se ha informado a las partes afectadas o a otros organismos relacionados?
- ¿Existen planes para comunicar a los titulares de los datos sobre el incidente?

### 4. Cumplimiento normativo

- ¿La vulneración debe ser notificada a la Superintendencia?
  - ¿Cumple con los criterios de gravedad y riesgo establecidos por la normativa vigente?
  - ¿Se han verificado los plazos para realizar la notificación?

## Análisis de la Segunda Sección del Formulario de Notificación de Vulneración de Datos Personales

La segunda pantalla del formulario de notificación de vulneración de datos personales, emitido por la Superintendencia de Protección de Datos Personales (SPDP), se enmarca en las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General, que regulan la obligación de los responsables del tratamiento de datos de reportar incidentes de seguridad que afecten los derechos de los titulares.

### Elementos Analizados en la Segunda Pantalla

#### 1. Identificación de los Titulares o Interesados Afectados por la Vulneración

Se debe detallar quiénes fueron las personas, empresas u organizaciones afectadas por el incidente, sin exceder los 300 caracteres.

El responsable debe identificar los titulares afectados con el fin de implementar las acciones correctivas necesarias y cumplir con la obligación de transparencia.

#### 2. Descripción de los Sistemas o Componentes Tecnológicos Vulnerados

Se debe detallar los servidores, bases de datos, aplicaciones o redes afectadas, con un límite de 500 caracteres.

El análisis de los sistemas vulnerados es fundamental para establecer medidas correctivas y prevenir futuras brechas.





### 3. Causa Presunta de la Vulneración

Descripción del Requisito: Se debe explicar brevemente la causa técnica, humana o externa que originó el incidente, en un máximo de 400 caracteres.

El objetivo es facilitar la evaluación del riesgo asociado a la vulneración y establecer responsabilidades.

### 4. Identificación de los Tipos de Datos Comprometidos:

La sección "Tipos de Datos comprometidos" permite categorizar el alcance de la vulneración y cumplir con los principios de transparencia y proporcionalidad. A continuación, se describe cada categoría:

- Información Personal (nombres, direcciones, etc.)
  - Ejemplo: nombres completos, direcciones, documentos de identidad.
  - Implicación: Facilita robo de identidad, fraudes o ataques de ingeniería social.
- Credenciales de Acceso (usuarios, contraseñas):
  - Ejemplo: contraseñas, tokens de autenticación.
  - Implicación: Permite accesos no autorizados y robo de información.
- Información Financiera (tarjetas de crédito):
  - Ejemplo: números de tarjeta, códigos de seguridad.
  - Implicación: Riesgo de fraudes financieros y transacciones no autorizadas.
- Datos de Salud:
  - Ejemplo: historial médico, diagnósticos.

- Implicación: Vulneración de privacidad y posibles daños reputacionales.
- Información Confidencial de la Empresa (Datos Personales de Clientes):
  - Ejemplo: nombres, roles, direcciones de correo electrónico de clientes.
  - Implicación: Riesgo de contacto no autorizado, suplantación de identidad o uso indebido.
- Registros de Clientes:
  - Ejemplo: bases de datos con nombres, contactos e historiales de compra.
  - Implicación: Exposición a fraudes y afectación a la confianza del cliente.
- Historial de Transacciones:
  - Ejemplo: registros de pagos y facturación.
  - Implicación: Riesgo de análisis indebido o fraudes financieros.

Seleccionar las categorías correctas permite evaluar con precisión el impacto de la vulneración y cumplir con los requisitos de notificación.

### 5. Volumen de Datos Comprometidos:

El formulario clasifica el volumen de datos en rangos específicos.

En esta sección del formulario, se solicita al responsable del tratamiento proporcionar una cuantificación del alcance del incidente, en función del número de registros de datos personales comprometidos. La cuantificación es clave para dimensionar el impacto de la vulneración y permitir a la autoridad evaluar la gravedad del incidente y las acciones correctivas necesarias.



### *Categorías de cuantificación utilizadas:*

- Menos de 100 registros: Esta opción corresponde a incidentes de bajo impacto, generalmente asociados a vulneraciones localizadas o limitadas en alcance. Es una cifra típica cuando los datos pertenecen a un número reducido de titulares, como empleados o clientes específicos.
- Entre 100,000 y 5,000,000 registros: Esta categoría abarca incidentes de mediano a alto impacto, donde la cantidad de datos comprometidos implica una afectación significativa. Es común en casos donde se comprometen bases de datos de organizaciones grandes o plataformas con un volumen considerable de usuarios.
- Entre 5,000,000 y 1,000,000,000 registros: Esta última categoría representa una vulneración de gran escala, con efectos masivos, generalmente vinculados a organizaciones con operaciones globales, infraestructuras críticas, o sistemas que manejan volúmenes masivos de datos personales (por ejemplo, servicios financieros, salud, o plataformas tecnológicas).

### *Importancia de la cuantificación:*

- Evaluación de impacto: El número de registros afectados permite dimensionar el riesgo y la gravedad de la vulneración en términos de afectación a los titulares.
- Medidas proporcionales: Una cuantificación precisa guía la aplicación de medidas correctivas y preventivas proporcionales a la magnitud del incidente.
- Transparencia: Facilita a la autoridad determinar la responsabilidad del responsable

del tratamiento y verificar la eficacia de sus acciones.

- Comunicación: Es un indicador crítico para informar a los afectados y garantizar la transparencia, especialmente en incidentes de mayor escala.

### *Buenas prácticas para la cuantificación:*

- Identificación rápida de registros afectados a través de herramientas de auditoría y monitoreo de sistemas.
- Clasificación previa de datos personales, lo que facilita una estimación más eficiente en caso de vulneración.
- Registro documental: Documentar claramente cómo se llegó a la cifra indicada, para demostrar diligencia en el proceso.

### 6. Medidas Adoptadas y Previstas:

Esta sección tiene como objetivo conocer las acciones realizadas o planificadas por la organización para mitigar los efectos de la vulneración de datos y prevenir futuros incidentes similares.

Es fundamental proporcionar información clara y precisa que demuestre un manejo adecuado y responsable del incidente. Se deben incluir detalles sobre:

- *Acciones inmediatas implementadas:* Describir las medidas adoptadas en cuanto se identificó la vulneración, como la contención del incidente, aislamiento de sistemas afectados, suspensión de accesos no autorizados, o cualquier otra acción destinada a frenar el impacto inicial.

- *Medidas técnicas y organizativas adicionales:* Incluir las acciones correctivas y preventivas implementadas o planificadas, como actualizaciones de sistemas, refuerzo de firewalls, auditorías de seguridad, capacitación del personal en protección de datos, o revisión de políticas de seguridad existentes.
- *Planes a corto, mediano y largo plazo:* Proporcionar información sobre estrategias y proyectos para fortalecer la seguridad de los sistemas, como la adopción de nuevas tecnologías de protección, implementación de procedimientos de monitoreo continuo, y creación de protocolos más robustos para la gestión de incidentes.

Es crucial que la información presentada sea transparente, específica y detallada, ya que esto refleja la responsabilidad y diligencia con la que la organización está gestionando la vulneración. Una descripción precisa no solo facilita la evaluación por parte de la autoridad, sino que también demuestra el compromiso de la organización con la protección de los derechos de los titulares de datos personales.

### 7. Evaluación del Riesgo:

La organización debe contar con una metodología formal para evaluar el riesgo derivado de la vulneración, que permita clasificarlo de manera objetiva (bajo, medio o alto). Esta clasificación debe considerar factores como la naturaleza de los datos comprometidos, el volumen afectado y la posible afectación a los derechos de los titulares.

Como ejemplo, se puede utilizar el siguiente enfoque:

### *Clasificación del Riesgo:*

- **Bajo:** Datos de contacto general con impacto limitado (por ejemplo, nombres y direcciones sin información sensible).
- **Medio:** Datos personales más detallados, como credenciales de acceso o información financiera parcial.
- **Alto:** Datos sensibles o críticos, como información de salud, credenciales completas o registros financieros.

### **Importancia de la Segunda Pantalla en el Proceso de Notificación**

La información recopilada en esta sección es fundamental para que la SPDP pueda:

- Determinar la magnitud y gravedad del incidente de seguridad.
- Identificar con precisión a los titulares afectados y los sistemas o infraestructura comprometida.
- Evaluar las medidas correctivas y preventivas adoptadas o planificadas por el responsable del tratamiento.
- Garantizar la protección efectiva de los derechos de los titulares de datos personales.

### **Conclusión**

La segunda pantalla del formulario proporciona una estructura clara y completa para que el responsable del tratamiento reporte información clave en relación con la vulneración de datos personales.

Facilita la identificación de los titulares afectados, los sistemas comprometidos, la causa preliminar de la vulneración, así como el tipo y





Facilita la identificación de los titulares afectados, los sistemas comprometidos, la causa preliminar de la vulneración, así como el tipo y volumen de datos comprometidos. Además, exige detallar las medidas adoptadas y previstas para mitigar el incidente y realizar una evaluación del riesgo asociado.

Cumplir con estos requerimientos no solo garantiza la transparencia en el reporte, sino que también permite a la autoridad ejercer su función de vigilancia y control, asegurando la protección efectiva de los derechos de los titulares conforme a la LOPDP y su Reglamento General.

## **Preguntas clave para completar la segunda pantalla del formulario de notificación de vulneración de seguridad**

### **1. Identificación de los Titulares o Interesados Afectados**

- ¿Cuántas personas o entidades fueron afectadas por la vulneración?
- ¿Cuál es el nivel de compromiso de los datos personales involucrados (ej., datos generales, sensibles, financieros)?
- ¿Se cuenta con registros precisos y actualizados para identificar a los afectados?
- ¿Existen mecanismos para contactar a los titulares afectados?

### **2. Descripción de los Sistemas o Componentes Tecnológicos Vulnerados**

- ¿Qué sistemas, servidores, bases de datos o aplicaciones se vieron comprometidos?
- ¿Qué tipo de datos personales se almacenaban en los sistemas afectados?

- ¿Se ha identificado la vulnerabilidad técnica que permitió el incidente?
- ¿Qué medidas tecnológicas y de seguridad se habían implementado en los sistemas afectados?

### **3. Causa Presunta de la Vulneración**

- ¿La vulneración fue causada por un error humano, fallo tecnológico o ataque externo?
- ¿Se ha identificado la raíz del problema (p. ej., accesos no autorizados, brechas de seguridad, malware)?
- ¿Existían controles o medidas de prevención que fallaron?
- ¿Qué acciones inmediatas se tomaron para contener la vulneración y mitigar el impacto?

### **4. Tipos de Datos Comprometidos**

- ¿Qué categoría de datos personales se vio comprometida (datos básicos, financieros, de salud, biométricos, etc.)?
- ¿Incluyen los datos comprometidos información sensible que requiera especial atención?
- ¿Se identificaron datos críticos que puedan afectar directamente la seguridad o privacidad de los titulares?

### **5. Volumen de Datos Comprometidos**

- ¿Cuántos registros de datos personales fueron comprometidos?
- ¿Se cuenta con una cifra exacta o solo una estimación preliminar del número de afectados?
- ¿Se identificaron patrones o segmentos específicos de los datos afectados?
- ¿El volumen de datos compromete a un grupo pequeño o a un número significativo de titulares?



## 7. Evaluación del Riesgo

- ¿Qué nivel de riesgo supone la vulneración para los derechos y libertades de los titulares (bajo, medio o alto)?
- ¿Cuáles son las posibles consecuencias para los titulares de los datos (fraude, robo de identidad, pérdida de privacidad, etc.)?
- ¿Existen factores que incrementen el riesgo, como la sensibilidad de los datos o la posibilidad de uso indebido?
- ¿Qué acciones de mitigación se están considerando para minimizar el impacto del riesgo identificado?
- ¿El riesgo afecta a los titulares individualmente o también a la organización responsable del tratamiento?

### Descripción de la última sección del formulario

La última pantalla del Formulario de Notificación de Vulneración de la Seguridad de Datos Personales está enfocada en la identificación del remitente y en la finalización del proceso de notificación. Incluye los siguientes campos obligatorios:

#### 1. Nombres y Apellidos

El responsable del tratamiento debe ingresar su nombre completo, asegurando una identificación clara y precisa de quién está notificando el incidente.

Este campo permite a la Superintendencia de Protección de Datos Personales (SPDP) registrar la identidad del declarante para futuros seguimientos o aclaraciones.

## 2. Correo Electrónico

Se solicita un correo electrónico válido, el cual servirá como canal de comunicación oficial entre la SPDP y el responsable del tratamiento.

La dirección de correo debe ser utilizada para confirmar la recepción del informe y notificar cualquier requerimiento adicional o respuesta oficial.

Esta sección tiene como objetivo validar y formalizar la identidad del responsable del tratamiento que realiza la notificación, asegurando la transparencia y trazabilidad del proceso. Además, facilita a la autoridad competente la posibilidad de establecer contacto directo con la persona responsable en caso de requerir información adicional o seguimiento de las acciones correctivas tomadas.

---

### Área de Derecho de Tecnologías, Medios, Telecomunicaciones, Ciberseguridad y Protección de Datos Personales

#### **Disclaimer:**

Este análisis se basa en nuestra experiencia y conocimiento en materia de protección de datos personales, aplicando mejores prácticas internacionales y el marco normativo vigente en Ecuador al momento de su elaboración. Sin embargo, la protección de datos es un terreno dinámico y en constante evolución. La Superintendencia de Protección de Datos Personales (SPDP), como autoridad competente, podrá emitir nuevas regulaciones o directrices que podrían cambiar algunos criterios aquí expuestos.

Nos mantenemos siempre atentos a cualquier actualización normativa y estamos preparados para ajustar nuestros enfoques y recomendaciones, asegurando que nuestros clientes y aliados cuenten con soluciones actualizadas, precisas y alineadas con las exigencias regulatorias. ¡El cumplimiento es un camino constante y nosotros los acompañamos en cada paso!



## Ecuador:

### Quito

Av. 12 de octubre, N26-97 y Lincoln  
Edificio Torre 1492, 170516,  
Piso 10, oficina 1005  
Telf.: +(593-2) 2986528/29/30/31  
Info.ecuador@ecija.com

### Guayaquil

Av. Numa Pompilio Llona s/n  
Puerto Santa Ana  
Edificio The Point, Piso 8, oficina 806  
Telf.: +59343883007  
Info.ecuador@ecija.com

### Cuenca

Av. Roberto Crespo y Alfonso Uriguen  
Telf.: +(593-7) 2817664  
Info.ecuador@ecija.com

### Manta

Calle M3 y Avenida 24  
Edificio Fortaleza, piso 8  
Telf.: +(593-5) 5003008  
Info.ecuador@ecija.com