GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

EN EL TRATAMIENTO DE DATOS PERSONALES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

2020

Industria y Comercio
SUPERINTENDENCIA

El futuro es de todos
Gobierno de Colombia

Industria y Comercio
SUPERINTENDENCIA

GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

EN EL TRATAMIENTO DE DATOS PERSONALES

El futuro es de todos
Gobierno de Colombia

Industria y Comercio
SUPERINTENDENCIA

ANDRÉS BARRETO GONZÁLEZ
Superintendente de Industria y Comercio

NELSON REMOLINA ANGARITA
Superintendente Delegado para la Protección de Datos Personales

ANGÉLICA MARÍA ACUÑA PORRAS
Secretaria General

ANGÉLICA ASPRILLA
Jefe Oficina de Servicios al Consumidor y Apoyo empresarial OSCAE

LUIS ALBERTO MONTEZUMA
CATERINE GÓMEZ CARDONA
CARLOS ENRIQUE SALAZAR
AÍDA LUCÍA HURTADO BEJARANO
Autores primera edición

DIANA MARIÑO LÓPEZ
Edición

YENNY PAOLA CASTIBLANCO GARCÍA
Diagramación

BOGOTÁ - COLOMBIA 2020

CONTENIDO

1. INTRODUCCIÓN

Sin seguridad no hay debido Tratamiento de Datos Personales. Por eso, la Ley 1581 de 2012 establece lo siguiente:

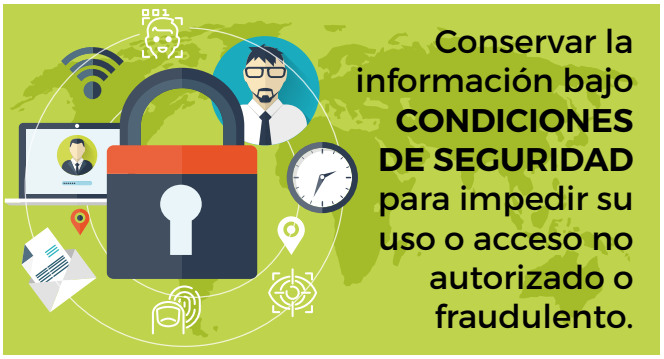
"La información sujeta a tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;(...)"[1]

En desarrollo de lo anterior, la Ley impone a los Responsables y Encargados del Tratamiento los siguientes deberes:

"Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; (...)"[2]

"Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares"[3]

DEBERES DE LOS **Responsables y Encargados** DEL TRATAMIENTO DE DATOS



INFORMAR A LA AUTORIDAD ENCARGADA cuando se presenten violaciones o existan riesgos en la administración de la información de los titulares.

1 Cfr. Literal g) del artículo 4 de la Ley 1581 de 2012
2 Cfr. Literales d) y b) de los artículos 17 y 18 de la Ley 1581 de 2012
3 Cfr. Literales n) y k) de los artículos 17 y 18 de la Ley 1581 de 2012 . El Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio describe la violación a los códigos de seguridad y la existencia de riesgos en la administración de la información de los Titulares como cualquier "violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base [sic] de datos [sic]física o automatizada administrada por el Responsable del Tratamiento o por su Encargado".

El principio y el deber de seguridad tienen un criterio eminentemente preventivo, lo cual obliga a los Responsables o Encargados del Tratamiento a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos. Pero si las medidas de seguridad fallan, las organizaciones deben estar preparadas para mitigar los riesgos y daños que se pueden causar a los derechos y libertades fundamentales de los Titulares y a las organizaciones.

El principio y el deber de seguridad tienen un CRITERIO EMINENTEMENTE PREVENTIVO.

Estos riesgos y daños pueden ser de gravedad y probabilidad variables, materiales o inmateriales, en particular, si esos incidentes generan situaciones de discriminación; divulgación de información o aspectos íntimos de los Titulares o daños a su dignidad, buen nombre o reputación; y afectación de datos de carácter sensible de niños, niñas y adolescentes o de personas con algún grado de discapacidad, grupos de personas en situación de especial vulnerabilidad, o en riesgo de exclusión social, o de seguridad, o cualquier otro perjuicio económico o social.

Si las medidas de seguridad fallan, las organizaciones deben estar preparadas para mitigar los riesgos y daños que se pueden causar a los derechos y las libertades fundamentales de los Titulares y a las organizaciones.

La Ley Estatutaria 1581 de 2012 no solo define como "tratamiento" cualquier actividad que se realice con Datos Personales, sino que en el artículo 19 dice lo siguiente: *"La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley."*

Adicionalmente, dicha norma ordena a esta entidad *"Velar por el cumplimiento de la legislación en materia de protección de Datos Personales"*. En línea con lo anterior se expide la siguiente guía cuyos objetivo y precisiones señalamos a continuación.

2. OBJETIVOS Y PRECISIONES

Esta guía tiene como propósito presentar algunas sugerencias a los Responsables y los Encargados del Tratamiento de Datos Personales, con miras a orientarlos para que cuenten con un plan dirigido a afrontar los incidentes de seguridad que afecten los Datos Personales bajo su custodia o posesión. Cualquier acción en este sentido debe centrarse en mitigar su impacto sobre los Titulares de la información y sus datos.

Adicionalmente, si las organizaciones no toman a tiempo las medidas técnicas y organizativas, aquellos eventos que afecten los Datos Personales pueden entrañar daños y perjuicios materiales o inmateriales para sus Titulares. De ahí que la importancia de la gestión de los incidentes de seguridad deba ser desde: i) el diseño de las actividades del Tratamiento; ii) el complemento de las políticas de seguridad de la información y protección de Datos; y iii) la ética corporativa de las empresas.

Las orientaciones contenidas en este texto solo comprenden algunos de los temas más relevantes. Esta guía no define las medidas concretas que deben implementarse al interior de las organizaciones para administrar los incidentes de seguridad, porque ellas dependen de las particularidades de cada caso, sino que aborda con pragmatismo la forma de actuar en caso de ocurrencia.

Este documento no es un concepto legal ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas sobre todos los temas que involucra la gestión de incidentes de seguridad en el Tratamiento de Datos Personales.

Así pues, las organizaciones, independientemente de su tamaño o naturaleza jurídica, son las llamadas a definir cómo proceder ante un incidente de seguridad. Por consiguiente, es importante resaltar que este documento no incluye todos los deberes legales sobre la materia, tampoco resuelve situaciones particulares ni las exime de cumplir los requerimientos de ley.

LA GESTIÓN DE LOS INCIDENTES
de seguridad debe ser desde:

i.

El diseño de las **ACTIVIDADES** del Tratamiento.

10100101
10101

ii.

El complemento de **LAS POLÍTICAS** de seguridad de la información y protección de Datos.

iii.

LA ÉTICA corporativa de las empresas.

3. MARCO NORMATIVO
PARA EL REPORTE DE INCIDENTES DE SEGURIDAD

La Ley 1581 de 2012 ordena lo siguiente:

"ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (…)

"n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares. (…)"

"ARTÍCULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (…)

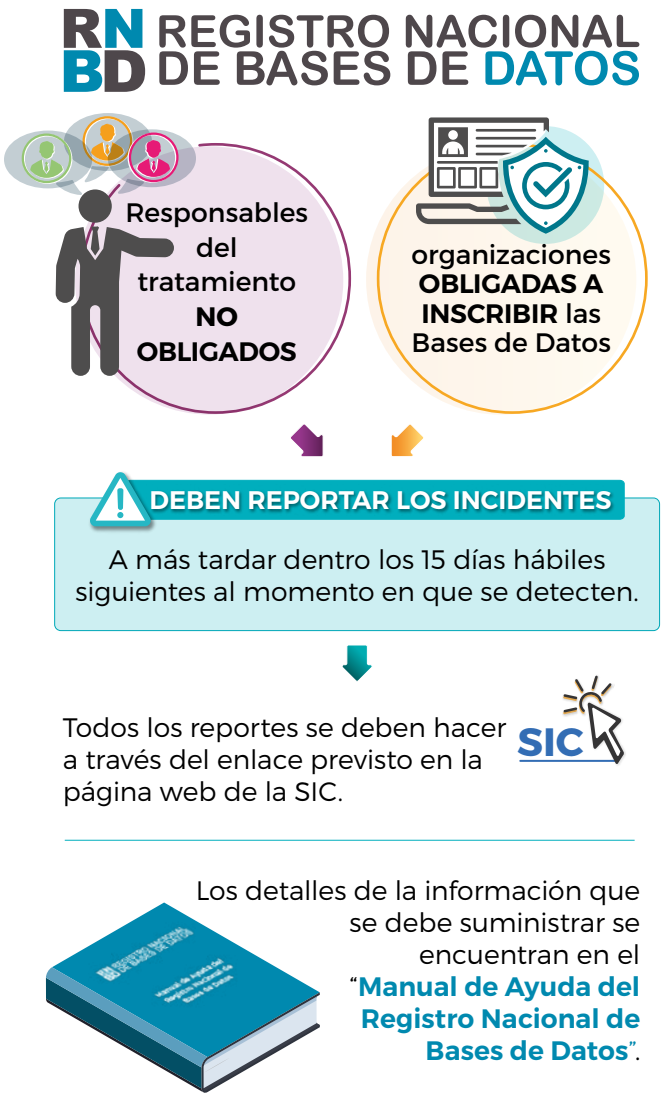
"k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares; (…)"

El Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio establece que las organizaciones que están obligadas a inscribir las Bases de Datos Personales ante el Registro Nacional de Bases de Datos (en adelante "RNBD"), deberán reportar el incidente de seguridad dentro los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o el área encargada de atenderlos.

Los Responsables del Tratamiento, que no se encuentren obligados a registrar sus Bases de Datos en el RNBD, y los Encargados del Tratamiento deberán hacer el reporte de los incidentes de seguridad en los mismos términos señalados en el párrafo anterior.

Independientemente del tamaño y complejidad del incidente de seguridad, todos los reportes deberán efectuarse a través del enlace previsto en la página web de la SIC.

Con respecto a la información que se deberá suministrar en el aplicativo, los detalles se recogen en el "Manual de Ayuda del Registro Nacional de Bases de Datos".



4. REPORTE DE INCIDENTES DE SEGURIDAD CUANDO SE ACUDE A ENCARGADOS DEL TRATAMIENTO

Si su organización -Responsable del Tratamiento- contrata a otra empresa o a un tercero -Encargado del Tratamiento- para realizar cualquier actividad que involucre Tratamiento de Datos Personales (por ejemplo prestación de servicios de cloud computing) exíjale el cumplimiento de su Política de Tratamiento de Datos Personales y los deberes legales que esto conlleva. Recuerde que esos terceros obran por cuenta de su organización y ésta responde frente a los Titulares de los datos y las autoridades por los errores o negligencia de ellos.

Es recomendable que las organizaciones incorporen en sus contratos de transmisión cláusulas dirigidas a que los Encargados del Tratamiento les comuniquen sin dilación indebida los incidentes de seguridad que involucren los Datos Personales transmitidos. Lo anterior, permitirá conocer rápidamente el incidente y, de este modo, poner en marcha las medidas oportunas.

El contrato de transmisión debe prever, entre otras, lo siguiente:

- Protocolo de respuesta en el manejo de incidentes de seguridad.
- Roles y responsabilidades.
- Puntos o personas de contacto.
- Procedimiento para el trámite de las consultas e inquietudes que puedan presentar los Titulares de la información.
- Reporte de los incidentes de seguridad por parte de otros Encargados del Tratamiento, en caso de que se hayan hecho subencargos sobre cualquier operación del Tratamiento.
- Cumplir las políticas de Tratamiento de información (PTI) de su entidad.

Debe quedar claro que el hecho de incluir la anterior información en los contratos de transmisión **no libera a los Encargados de la obligación de efectuar la notificación del incidente de seguridad ante la SIC**, de conformidad con el literal k) del artículo 18 de la Ley 1581 de 2012.

5. CONSERVACIÓN DE REGISTROS INTERNOS

Un elemento clave en cualquier sistema de administración de riesgos asociados al Tratamiento de Datos Personales es la documentación de todos los aspectos de cada incidente de seguridad en los registros internos de las organizaciones. Estos soportes no solo permitirán demostrar el cumplimiento del régimen de protección de Datos Personales en caso de una investigación, sino que serán útiles para evitar que esos incidentes ocurran nuevamente en su organización.

Dichos registros documentales deberán incluir lo siguiente:

Una descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos -sensibles, privados, etc.- comprometidos).

Las categorías de Titulares de la información afectados.

La fecha y hora del incidente de seguridad y del descubrimiento del mismo.

Las indagaciones preliminares e investigaciones realizadas por la organización.

Las medidas correctivas.

Los Responsables del manejo del incidente de seguridad.

La prueba del reporte efectuado ante la SIC, así como la comunicación realizada a los Titulares de la información, si fue necesario.

La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares y los factores tenidos en cuenta.

La inclusión de detalles personales, cuando deban establecerse.

Las organizaciones deben ser conscientes de que la información almacenada en los registros tiene que:

- Contener suficientes detalles para que la autoridad evalúe si se actuó diligentemente en el manejo del incidente de seguridad.
- Conservarse con las medidas de seguridad y confidencialidad necesarias para protegerla de cualquier amenaza.
- Estar sujeta a los plazos de conservación establecidos por cada organización, en concordancia con los principios de finalidad, necesidad y proporcionalidad.
- Garantizar la originalidad e integridad de la prueba técnica en los términos de la Ley 527 de 1999.

6. PROTOCOLO DE RESPUESTA EN EL MANEJO DE INCIDENTES DE SEGURIDAD

La *"Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)"*[4] establece que el Programa Integral de Gestión de Datos Personales debe involucrar un componente de gestión de riesgos que le permita a las organizaciones identificar sus vulnerabilidades a tiempo y enfocar sus recursos en la adopción de las medidas de mitigación de riesgos, tanto para ellas como para los Titulares de la Información.

Es por esto que, contar con un protocolo de respuesta facilitará a las organizaciones actuar de forma rápida, ordenada y eficaz ante cualquier incidente que afecte la confidencialidad, disponibilidad e integridad de los datos personales bajo su protección.

DETECCIÓN, IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS INCIDENTES DE SEGURIDAD

Como se mencionó, las medidas de seguridad tienen un carácter preventivo para evitar la pérdida de la información, su adulteración, así como la consulta, uso, circulación o acceso no autorizado o fraudulento.

Las medidas de seguridad deben ser apropiadas considerando varios factores como: (i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares, y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; (iv) el número de Titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles, (vii) el estado de la técnica, y (viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad deben ser objeto de revisión, evaluación y mejora permanente.

Ahora bien, si la seguridad falla es fundamental que las organizaciones cuenten con mecanismos de monitoreo y control que les permita detectar de inmediato o prontamente el incidente de seguridad. Esto ayudará a reducir la magnitud del daño para la organización y para los Titulares de los Datos Personales. Por ende, es crucial que se cuente con herramientas de "alertas" para actuar tan pronto ocurra el incidente.

Las organizaciones deben aplicar todas las medidas técnicas, administrativas y organizativas para determinar de inmediato si se ha producido un incidente de seguridad que afecte los Datos Personales y, de ser así, deben implementar las acciones necesarias para abordar dicho evento u ocurrencia. Así mismo, en cumplimiento de lo que establece la Ley 1581 de 2012, reportarlo a la SIC y, dependiendo del caso, comunicarlo a los Titulares de la información.

¿CUÁLES SON LOS TIPOS DE INCIDENTES DE SEGURIDAD?

Los incidentes de seguridad pueden clasificarse dependiendo del grado de pérdida de las siguientes características de la información:

- Confidencialidad
- Integridad
- Disponibilidad

4 El texto de la guía puede consultarlo en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

¿CUÁLES SON LAS CAUSAS QUE GENERAN UN INCIDENTE DE SEGURIDAD?

Los incidentes de seguridad pueden generarse por diferentes razones como, entre otras, las siguientes:

- Inexistencia de políticas preventivas de seguridad
- Errores o negligencia humana.
- Casos fortuitos.
- Actos maliciosos o criminales.
- Fallas en los sistemas de la organización.
- Procedimientos defectuosos.
- Deficiencias o defectos en las operaciones.
- Alteración; destrucción; robo o pérdida de archivos físicos.

Todos los incidentes de seguridad deben ser tomados seriamente y evaluados por parte de las organizaciones. Los que inicialmente parezcan irrelevantes podrían ser significativos o graves respecto de los derechos y las libertades de los Titulares de la información.

¿CUÁLES SON LAS MEDIDAS PREVENTIVAS DENTRO DE UNA ORGANIZACIÓN PARA HACER FRENTE A UN INCIDENTE DE SEGURIDAD?

- Entrenar periódicamente al equipo humano de la organización para actuar frente al incidente de seguridad. Se recomienda efectuar simulacros preventivos como se hacen, por ejemplo, para casos de incendios o temblores. Frente a un incidente de seguridad, la gente debe estar preparada para actuar de inmediato, profesionalmente e inteligentemente.
- Precisar exactamente cuándo se está ante un incidente de seguridad que afecte Datos Personales. No todas las fallas de seguridad necesariamente involucran la confidencialidad, integridad y disponibilidad de información de carácter personal.
- Definir las medidas y el procedimiento interno para el manejo de los incidentes de seguridad.
- Diseñar la metodología para la evaluación del impacto de los incidentes de seguridad en los Titulares de la información.
- Evaluar posibles consecuencias adversas para una persona, en caso de que se desencadene un incidente de seguridad, por ejemplo, el cometimiento de delitos; la afectación de derechos; etc.
- Conocer los procesos de respuesta a incidentes de seguridad, sistemas de corrección y de recuperación, incluidos aquellos establecidos por los Encargados del Tratamiento.
- Cumplir con lo establecido en la Ley 1581 de 2012, así como con las órdenes y/o instrucciones que imparta la SIC.
- Reportar el incidente de seguridad tanto a la SIC como a otras autoridades públicas, según sea el caso.
- Preparar al equipo de comunicaciones frente a las posibles preguntas e inquietudes de Titulares de la información, accionistas, clientes, proveedores, empleados y medios de comunicación, respecto del incidente de seguridad.

¿QUÉ ES UN PROTOCOLO DE RESPUESTA EN EL MANEJO DE INCIDENTES DE SEGURIDAD?

Es un marco general que incorpora roles, responsabilidades y acciones que deben ser desplegadas al interior de las organizaciones para gestionar un incidente de seguridad. Dicho instrumento debe ser:

- Documentado
- Implementado
- Comunicado al equipo humano de la organización
- Monitoreado.

Como señala la *"Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)"*, el monitoreo consiste en realizar un seguimiento constante para velar porque las medidas que se hayan establecido al interior de las organizaciones se apliquen y funcionen en la práctica, en particular, cuando desarrollen nuevos

productos o servicios; empleen nuevas tecnologías; realicen ajustes en sus políticas, procedimientos y procesos; existan incidentes de seguridad; etc.

No sobra recordar que el protocolo debe estar disponible al interior de las organizaciones con el fin de garantizar que el personal entienda claramente cómo debe actuar en caso de que se presente un incidente de seguridad y cuál sería la respuesta más efectiva.

¿QUÉ DEBERÍA INCLUIR EL PROTOCOLO?

Los detalles del protocolo dependen de las necesidades específicas de cada organización.

De forma esquemática, este puede incluir los siguientes elementos:

Una explicación clara de lo que constituye un incidente de seguridad.

Esto ayudará al personal de las organizaciones a identificar aquellos eventos que afecten la confidencialidad, la integridad y la disponibilidad de la información de carácter personal.

Una estrategia para identificar, contener y mitigar los incidentes de seguridad.

En este punto se pueden incluir las acciones que el personal de la organización, el Oficial de Protección de Datos Personales o el Área de Protección de Datos Personales y el equipo de respuesta adoptarán, en caso de que exista un incidente que afecte o involucre Datos Personales.

Se deberá tener en cuenta:

- Las medidas para contener y revertir el impacto que puede tener un incidente de seguridad.
- La gestión de los incidentes como una cuestión prioritaria.
- La capacidad del personal para evaluar adecuadamente los incidentes de seguridad y su impacto en los Titulares de la información.
- Requisitos legales o contractuales.
- Una estrategia de comunicación clara y precisa a los Titulares de la Información (si fuese necesario); el reporte del incidente tanto a la SIC como a otras entidades[5] (por ejemplo: Fiscalía General de la Nación, Policía Nacional, agencias de seguridad y ciberseguridad, operadores de información, Superintendencia Financiera de Colombia; etc.)
- Una metodología para determinar el nivel de riesgo para los Titulares de la Información.

Los roles y responsabilidades del personal.

Describir las responsabilidades del personal cuando se presente un incidente de seguridad, incluyendo las que están en cabeza de la Alta Gerencia.

Línea de tiempo de ejecución.

El protocolo debe establecer los tiempos de atención a los incidentes de seguridad.

Reporte de progreso.

El protocolo de respuesta debe ser monitoreado. Asimismo, es necesario evaluar su progreso en periodos preestablecidos (bien sea por horas; días; semanas o meses), e identificar los posibles puntos conflictivos que se puedan generar en el manejo del incidente de seguridad.

Evaluación de respuesta y modificaciones.

Una vez se haya gestionado el incidente de seguridad, el equipo de respuesta deberá revisar el protocolo, y hacer los ajustes pertinentes.

Acciones.

Establecer (o referirse a) las acciones que se espera adopte el equipo de respuesta cuando se presente un incidente de seguridad.

Documentación.

Documentar en un registro interno la información relacionada con el incidente de seguridad.

5 Notificación a otras entidades oficiales como, la Fiscalía General de la Nación; la Procuraduría General de la Nación; Gaula; Policía Nacional; Superintendencia Financiera de Colombia.;Centro Cibernético Policial; colCERT; CSIRT Policial; CSIRT Asobancaria, CSIRT Sectorial, entre otras.

Revisión.

La evaluación de cómo ocurrió el incidente de seguridad y el éxito de su gestión, puede ayudar a la organización a evaluar la efectividad del protocolo y a documentar las lecciones aprendidas para tenerlas presentes en futuras ocasiones.

¿Por qué es necesario contar con un equipo de respuesta ante incidentes de seguridad?

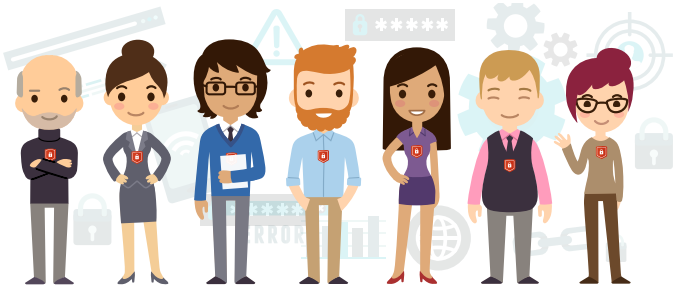
El tamaño potencial y el alcance de las consecuencias relacionadas con un incidente de seguridad no se puede entender sin la inclusión y la experiencia de las áreas (o departamentos) claves dentro de la organización.

El equipo de respuesta es el responsable de definir e implementar las acciones necesarias para reducir el impacto de un incidente de seguridad en los Titulares de la información. En todo caso, el primer objetivo dentro de ese conjunto de acciones es siempre prevenir, minimizar o remediar cualquier daño para los Titulares de los Datos.

Es fundamental que el personal que conforma el equipo, así como sus roles y responsabilidades, estén plenamente definidos y documentados en el protocolo antes de que ocurra un incidente de seguridad. De lo contrario, la respuesta al mismo se puede retrasar innecesariamente.

¿Quiénes conforman el equipo de respuesta ante incidentes de seguridad?

El equipo de respuesta ante un incidente de seguridad en el Tratamiento de Datos Personales dependerá de las particularidades de cada organización. Las entidades pueden considerar la creación de un equipo central y la adición de otros miembros según sea necesario, pues se pueden necesitar diferentes habilidades y conocimientos para responder a un incidente de seguridad.



Ejemplos de áreas y/o personas que pueden conformar ese comité son:

- El Presidente de la organización.
- El Oficial de Protección de Datos Personales o el Área de Protección de Datos Personales.
- Legal.
- Cumplimiento.
- Seguridad de la Información.
- Archivo.
- Recursos Humanos.
- Tecnología
- Telecomunicaciones.
- Marketing/Publicidad.
- Comunicaciones y Relaciones Públicas.
- Riesgos.
- Finanzas.
- Atención al Cliente.
- Asesores externos.

Resulta indispensable que el equipo de respuesta tenga la autoridad para desarrollar los pasos descritos en el protocolo sin necesidad de solicitar permiso a otras instancias dentro de la organización, ya que esto permitirá una reacción más rápida ante el incidente de seguridad.

Se reitera que es crucial entrenar periódicamente al equipo humano de la organización para actuar frente a incidentes de seguridad en el tratamiento de datos personales, por lo que se recalca la importancia de efectuar simulacros preventivos como se hacen, por ejemplo, para casos de incendios o temblores. Frente a un incidente, la gente debe estar preparada para actuar de inmediato, profesionalmente e inteligentemente.

7. PASOS PARA RESPONDER A UN INCIDENTE DE SEGURIDAD

01 Contener el incidente de seguridad y hacer una evaluación preliminar

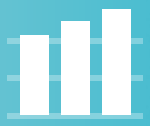
Una vez que las organizaciones tengan conocimiento de la ocurrencia de un incidente de seguridad deberán adoptar las medidas inmediatas para limitar esa falla y evitar cualquier compromiso adicional a la información de carácter personal bajo su cuidado.

En esta primera etapa, las organizaciones también deberán comenzar una investigación inicial sobre el evento u ocurrencia. La indagación preliminar les ayudará a responder las siguientes preguntas respecto del incidente de seguridad:

- ¿Cómo se produjo?
- ¿Cuándo y dónde tuvo lugar?
- ¿Cuál fue la naturaleza y quién lo detectó?
- ¿Se continúa compartiendo o divulgando información personal sin Autorización?
- ¿Quién tiene acceso a la información personal?
- ¿Qué se puede hacer para asegurar la información o detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados?
- ¿Es un incidente de seguridad relacionado con Datos Personales que requiere la notificación a las personas tan pronto como sea posible?

Durante esta etapa preliminar, las organizaciones deben tener cuidado de no destruir la evidencia que pueda ser valiosa para:

- Establecer la causa del incidente de seguridad.
- Identificar todos los riesgos generados a los Titulares de la información.
- Responder los requerimientos de la SIC u otras autoridades.



02 Evaluar los riesgos e impactos asociados con el incidente de seguridad

La adecuada gestión de riesgos requiere un profundo y juicioso proceso de identificación y evaluación del nivel de severidad del incidente de seguridad; la probabilidad de daño para los Titulares de la Información; el nivel de riesgo para sus derechos y libertades; y el Tratamiento que se dará a esos riesgos.

Un incidente de seguridad puede tener una variedad de efectos adversos sobre las personas que puede dar lugar a problemas de discriminación, suplantación de identidad o fraude, pérdidas financieras, daño reputacional, pérdida del carácter confidencial de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo.

.**El nivel de riesgo del incidente de seguridad frente a los Titulares de la información puede ser cuantificado y/o calificado.**

Dependiendo de la metodología definida por cada organización, el riesgo puede ser calificado en:

BAJO RIESGO: es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo.

RIESGO MEDIO: el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial

RIESGO ALTO: el incidente de seguridad puede tener un impacto considerable en las personas afectadas.

RIESGO GRAVE: el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas.

Se debe tener en cuenta que el nivel del riesgo no debe basarse únicamente en la clasificación de los Datos Personales (público, semiprivado, privado y sensible), en razón a que el impacto de un incidente de seguridad en los Datos Personales involucra un carácter contextual. Por ejemplo, el hurto de una base de datos que contiene los nombres de las personas junto con los números de identificación personal, la descripción de la finalidad o las fechas de nacimiento pueden representar un alto nivel de riesgo, mientras que, el hurto de una base de datos que contiene solo los nombres de las personas puede representar un riesgo menor.

Corresponderá a cada organización, de acuerdo con el Principio de Responsabilidad Demostrada, definir su propio modelo interno de evaluación donde el foco de atención no se centrará en los riesgos que se ciernen sobre ella, sino por el contrario, en el riesgo para los Titulares de la información.

Son factores que pueden ser tenidos en cuenta para determinar el nivel de riesgo:

En los Titulares de la información

- ¿Qué cantidad de personas fueron afectadas?
- ¿Qué categoría de personas fueron afectadas?
- ¿Cuáles son las características especiales de las personas afectadas? Por ejemplo: niños, niñas y/o adolescentes; personas en estado de vulnerabilidad; personal del sindicato, etc.

En los datos personales

- ¿Cuál fue el volumen de los datos afectados?
- ¿Cuál fue el periodo durante el cual los datos fueron afectados o estuvieron comprometidos?
- ¿Qué tipo de información personal fue afectada? Por ejemplo, identificación personal, datos biométricos, historia clínica, datos genéticos, pruebas académicas, registros de localización, direcciones IP, mensajes de texto, información financiera y crediticia, datos genéticos, perfiles de comportamiento, puntajes de crédito, etc.
- ¿Qué tan sensible es la información comprometida? Por ejemplo: datos de niños, niñas y/o adolescentes; datos biométricos, genéticos o de salud; perfiles de comportamiento; resultados de decisiones automatizadas; orientación sexual; datos políticos; etc.
- ¿Cuál es el contexto de la información personal comprometida?
- ¿Estaba la información personal adecuadamente cifrada, anonimizada? ¿Era inaccesible?
- ¿Cómo se puede utilizar la información personal afectada?
- ¿Existe un riesgo a una mayor exposición de la información personal?
- ¿Está la información personal disponible públicamente en internet?
- ¿Se puede utilizar la información personal para fines fraudulentos o puede causar cualquier tipo de daño material y/o inmaterial al Titular?
- ¿Se ha recuperado la información personal?

En la organización

- ¿Qué causó el incidente de seguridad?
- ¿Cuándo y con qué frecuencia ocurrió el incidente de seguridad?
- ¿Es este un problema sistémico o aislado?
- ¿Cuál fue el alcance del incidente de seguridad?
- ¿Qué medidas se han tomado para mitigar el daño?
- ¿Cuáles son las actividades y operaciones que desarrolla la organización? Por ejemplo: entidades financieras, entidades públicas, proveedores de aplicaciones móviles, colegios, farmacias, hospitales, almacenes de ropa, operadores de información, proveedores de redes sociales, etc.
- ¿Los datos comprometidos afectarán las transacciones que debe realizar la organización con terceros externos?

03 Identificar los daños para las personas, organizaciones y público en general

¿Qué daños para las personas podrían resultar de un incidente de seguridad? Los ejemplos incluyen:

- Riesgo en su seguridad física o psicológica
- Extorsión económica o sexual
- Hurto de identidad
- Suplantación de identidad
- Pérdida financiera
- Negación de un crédito o seguro
- Perfilamiento con fines ilícitos
- Pérdida de negocios u oportunidades de empleo
- Discriminación
- Humillación significativa o pérdida de dignidad y daño a la reputación.

¿Qué daño para la organización podría resultar de un incidente? Los ejemplos incluyen:

- Pérdida reputacional
- Pérdida de clientes o usuarios
- Pérdida de confianza en la organización
- Honorarios de consultores e ingenieros forenses
- Pérdida de activos
- Sanciones, órdenes e instrucciones administrativas
- Exposición financiera
- Órdenes judiciales
- Demandas judiciales

¿Qué daño para el público podría resultar de un incidente de seguridad? Los ejemplos incluyen:

- Riesgo para la salud pública
- Riesgo para la seguridad pública
- Pánico económico
- Alteración de los pilares constitucionales de un país

04 Notificar a la Superintendencia de Industria y Comercio

www.sic.gov.co

Las organizaciones deben reportar la ocurrencia del incidente de seguridad ante la SIC sin dilación indebida y a más tardar dentro los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

La notificación de un incidente de seguridad en Datos Personales debe contener, como mínimo, la información que establece el Registro Nacional de Bases de Datos (RNBD).

05 Comunicar a los Titulares de la información

La comunicación a los Titulares de la Información brinda la oportunidad para que ellos mismos puedan adoptar las medidas necesarias para protegerse de las consecuencias de un incidente de seguridad. Por ejemplo, cambiar su nombre de usuario y contraseña; monitorear su historial crediticio; cancelar su tarjeta de crédito; etc.

Debe tenerse en cuenta que la *"Guía para la Implementación del Principio de Responsabilidad Demostrada"* señala que es importante que las organizaciones implementen mecanismos que les permitan comunicarse de manera eficiente con los Titulares de la información para: (i) informarles sobre el incidente de seguridad relacionado con sus Datos personales y las posibles consecuencias; y, (ii) proporcionar herramientas a los Titulares para minimizar el daño potencial o causado.

Dicho esquema de comunicación debe estar incluido en el protocolo de respuesta.

Por ello, las organizaciones deberán abordar los siguientes cuatro interrogantes si decide comunicar el incidente a los Titulares de la información:

1. ¿Cuándo comunicar?
2. ¿Cómo comunicar?
3. ¿Quién debe comunicar?
4. ¿Qué debe incluirse en la comunicación?

Las comunicaciones deben ser suficientes claras y precisas para permitir que los Titulares de la información comprendan la importancia del incidente y que tomen las medidas, si es posible, para reducir los riesgos que podría resultar de su ocurrencia. Es primordial no incluir información personal innecesaria en el aviso para evitar una posible divulgación no autorizada.

06 Prevenir futuros incidentes de seguridad en Datos Personales

Una vez que se hayan tomado las medidas necesarias para mitigar los riesgos asociados con el incidente, las organizaciones deberán ejecutar un plan de prevención para evitar futuros eventos que puedan afectar los datos personales que han tratado.

Esto genera retos al interior de las organizaciones:

- Revisar las condiciones del Tratamiento.
- Realizar auditorías internas, externas o mixtas.
- Robustecer las políticas, procesos y procedimientos.
- Ajustar las evaluaciones de impacto en datos personales
- Establecer esquemas de trabajo a corto, mediano y largo plazo. Así como los roles y responsabilidades.
- Generar apoyo y compromiso de la Alta Gerencia para desplegar los cambios que se requieran al interior de las organizaciones.

Ejemplos de medidas a implementar con posterioridad a la ocurrencia de un incidente:

- Reforzar los programas de capacitación y educación del personal.
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.
- Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus de la organización.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.
- Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.
- Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas.

8. INCREMENTE Y MANTENGA LA CONFIANZA DE LOS TITULARES DE DATOS PERSONALES.

Desde hace algunas décadas se ha afirmado que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que involucre el Tratamiento de Datos Personales. Por eso, se ha sostenido que "las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización" [6].

La confianza se entiende como la expectativa de que "se puede contar con la palabra del otro" y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que una entidad es fiable, cumple su palabra, es sincera, íntegra y lleva a cabo las acciones prometidas[7].

La seguridad genera confianza. Si falla, es clave estar muy bien preparados y entrenados para actuar frente a los incidentes de seguridad de manera inmediata, profesional e inteligente.

6 Cfr. Edelman Trust Barometrer de 2019.https://www.edelman.com/trust-barometer

7 Cfr. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

9. REFERENCIAS

Agencia Española de Protección de Datos, AEPD, "Guía para la gestión y notificación de brechas de seguridad", en: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

Agencia Española de Protección de Datos, AEPD, "Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD", en: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

Comisión de Protección de Datos de Irlanda (The Data Protection Commission, DPC), "Self-Assessment Checklist.", en: https://www.dataprotection.ie/

Comisión de Protección de Datos Personales de Singapur (The Personal Data Protection Commission, PDPC), "GUIDE TO MANAGING DATA BREACHES", en: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-managing-data-breaches-v1-0-(080515).pdf

Densmore, Russell R., "Privacy Program Management. Tools for Managing Privacy Within Your Oganization".

European Union Agency for Network and Information Security, ENISA, "Recommendations for a methodology of the assessment of severity of personal data breaches". Working Document, v1.0, December 2013.

Grupo de Trabajo de Protección de Datos del artículo 29 (Hoy, Comité Europeo de Protección de Datos). "Opinion 03/2014 on Personal Data Breach Notification", en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

Grupo de Trabajo de Protección de Datos del artículo 29 (Hoy, Comité Europeo de Protección de Datos). "Guidelines on Personal data breach notification under Regulation 2016/679", en: https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, "Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.", en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Oficina del Comisionado Australiano de Información (Office of the Australian Information Commissioner, OAIC), *"Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)"*, en: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

Oficina del Comisionado de Información de Gran Bretaña (The Information Commissioner's Office, ICO), *"Personal data breaches"*, en: https://ico.org.uk/

Oficina del Comisionado de Privacidad de Canadá (Office of the Privacy Commissioner of Canada*), "What you need to know about mandatory reporting of breaches of security safeguards"*, en: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Oficina del Comisionado de Privacidad para los Datos Personales de Hong Kong (The Office of the Privacy Commissioner for Personal Data, PCPD), *"Guidance on Data Breach Handling and the Giving of Breach Notifications"*, en: https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

Oficina de Administración y Presupuesto de la Casa Blanca (The Office of Management and Budget (OMB) Memorandum M-07-16, *"Safeguarding Against and Responding to the Breach of Personally Identifiable Information"*, en: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

Superintendencia de Industria y Comercio, *"Guía para la Implementación del Principio de Responsabilidad Demostrada"*, en: https://issuu.com/quioscosic/docs/guia_accountability_26_p__g

Supervisor Europeo de Protección de Datos, SEPD (The European Data Protection Supervisor, EDPS), *"Guidelines on personal data breach notification For the European Union Institutions and Bodies"*, en: https://edps.europa.eu/sites/edp/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf

Unión Europea, *"REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)"*, en: https://eur-lex.europa.eu/legal-content/En/TXT/PDF/?uri=CELEX:32016R0679&from=

Industria y Comercio
SUPERINTENDENCIA

www.sic.gov.co

@sicsuper

Superintendencia de Industria y Comercio de Colombia

Superintendencia de Industria y Comercio

Conmutador: **(571) 5 870 000** - Contact Center: **(571) 5 920 400**
Línea gratuita nacional desde teléfonos fijos: **01 8000 910 165**