URIBE · YÁÑEZ

Asesores Legales

GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

Cartilla Superintendencia de Industria y Comercio (2020)

URIBE · YÁÑEZ

URIBE · YÁÑEZ

TABLA DE CONTENIDOS

URIBE · YÁÑEZ

1

PRINCIPIO Y DEBER DE SEGURIDAD

DEBERES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS

De los arts. 17 y 18, de la Ley 1581 de 2012, se destacan los siguientes literales:

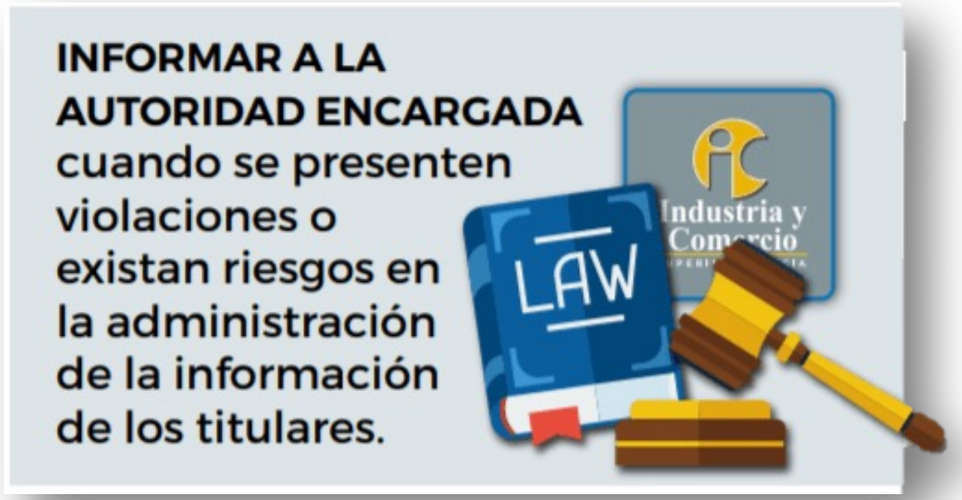


Gráfico tomado de Superintendencia de Industria y Comercio, basado en la Ley 1581, art. 17, lit. d), y art. 18, lit. b)

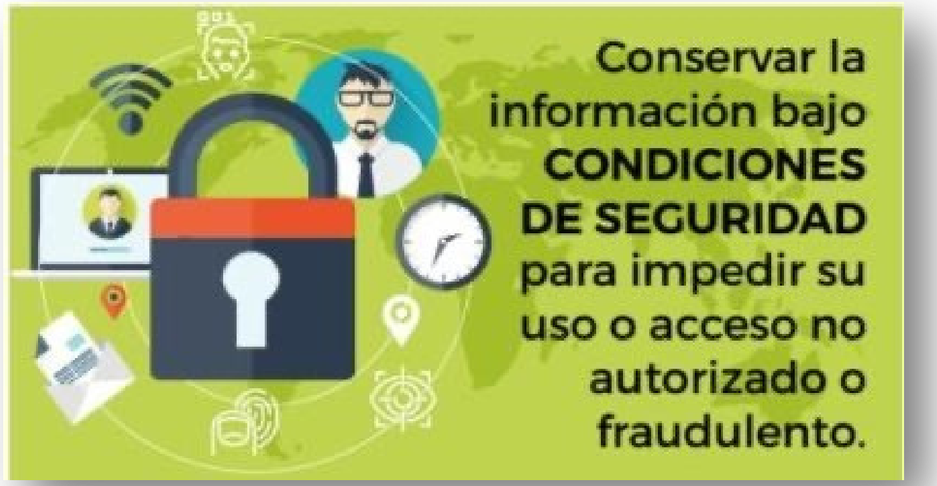


Gráfico tomado de Superintendencia de Industria y Comercio, basado en la Ley 1581, art. 17 , lit. n), y art. 18, lit. k)

PASOS PARA LA GESTIÓN DE INCIDENTES DE MANERA PREVENTIVA

Es pieza clave la prevención de las fugas de datos mediante estos tres pasos:

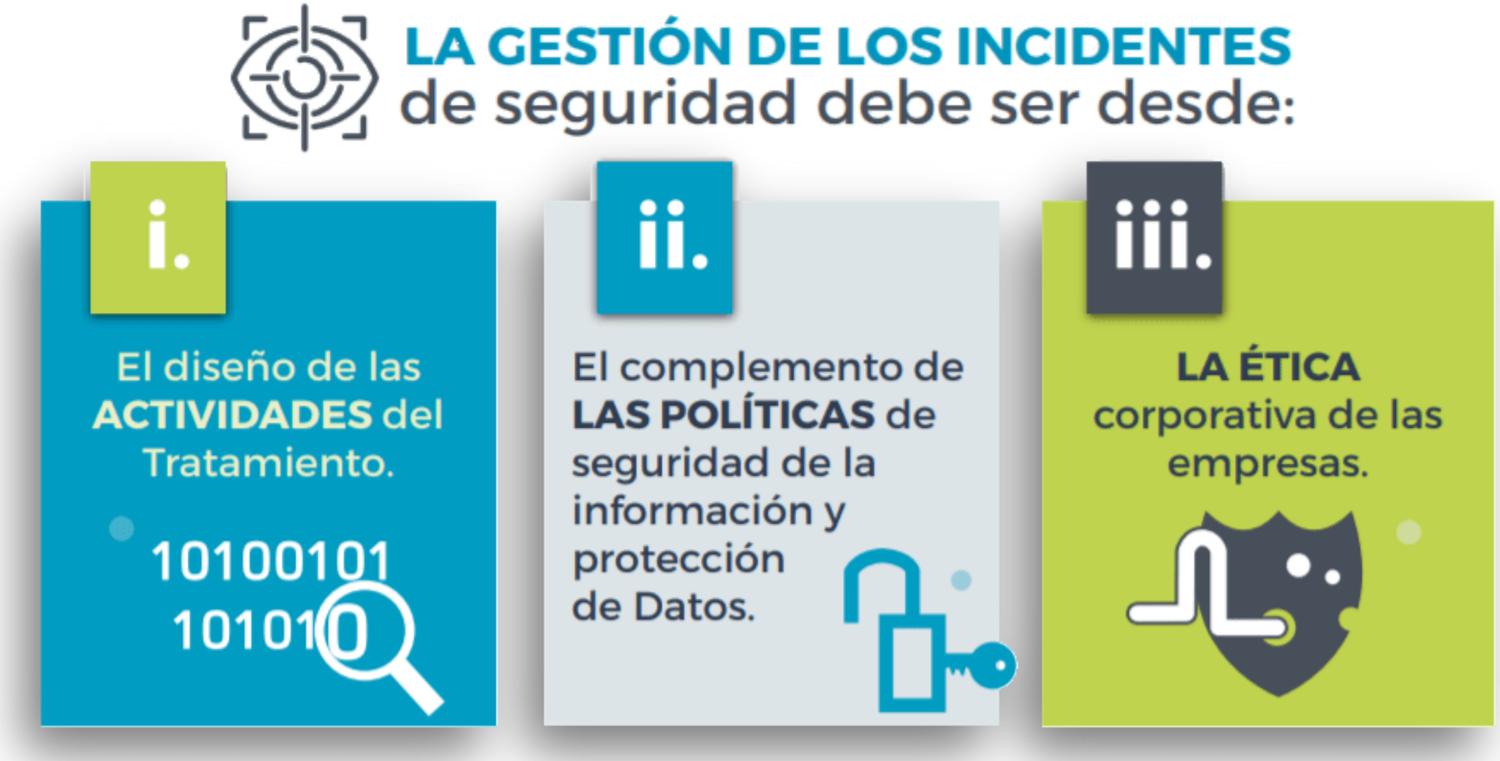


Gráfico tomado de Superintendencia de Industria y Comercio

URIBE · YÁÑEZ

2

MARCO NORMATIVO PARA EL REPORTE DE INCIDENTES DE SEGURIDAD

LEY 1581 DE 2012 Y DEBERES DE LOS RESPONSABLES Y LOS ENCARGADOS DEL TRATAMIENTO DE LOS DATOS

1. Artículo 17: "Deberes de los Responsables del Tratamiento"

"n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridady existan riesgosen la administración de la información de los Titulares." (Ley 1581-2012)

2. Artículo 18: "Deberes de los Encargados del Tratamiento"

"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; (…)" (Ley 1581-2012)

CIRCULAR ÚNICA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO: CAPÍTULO II, TÍTULO V

URIBE · YÁÑEZ

INSCRIPCIÓN DE INCIDENTES DE SEGURIDAD AL REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

¿Qué es el RNBD?

Directorio público de las bases de datos sujetas a tratamiento **que operan en el país. Es administrado por la SIC y es de libre consulta.**

¿Quiénes deben registrarse ante la RNBD

"Los Responsables del tratamiento, sociedades y entidades sinánimo de lucro que tengan activos totales superiores a 100.000 Unidades de Valor Tributario (UVT)(Art. 868, Estatuto Tributario) y personas jurídicas de naturaleza pública". (Circular Única de la SIC).

CIRCULAR ÚNICA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO: CAPÍTULO II, TÍTULO V

¿Quiénes deben reportar un incidente ante la RNBD?

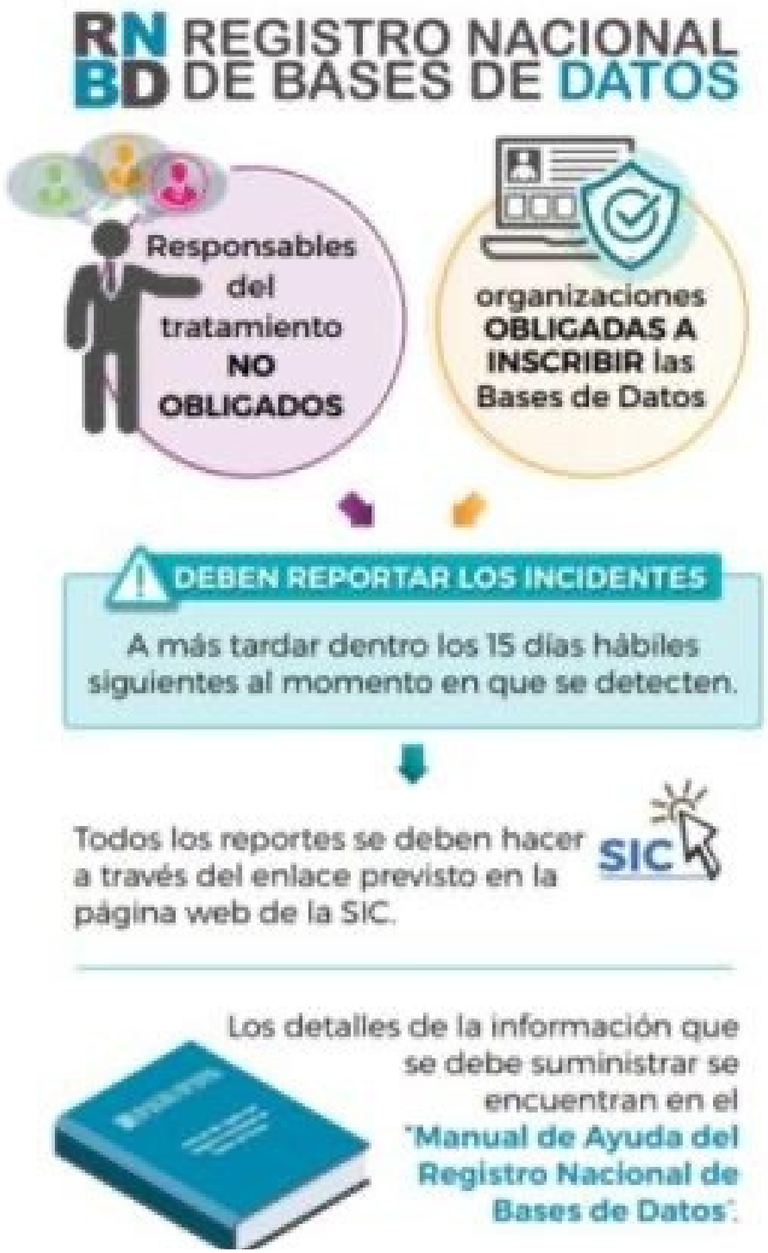


Gráfico tomado de Superintendencia de Industria y Comercio

URIBE · YÁÑEZ

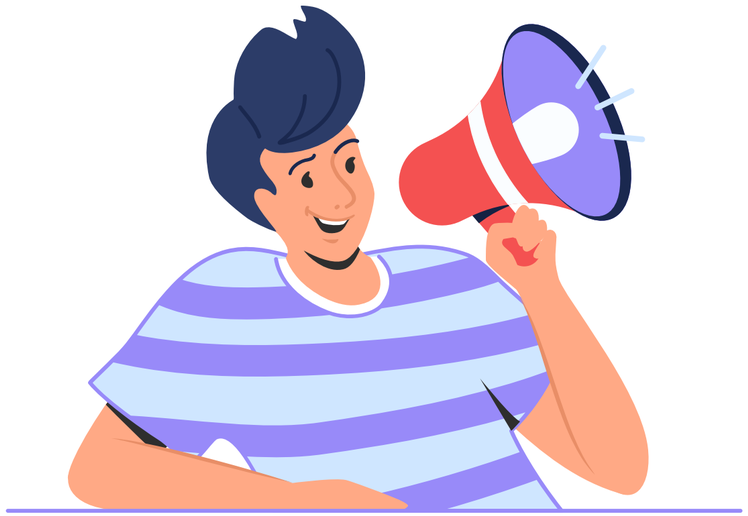
3

ENCARGADOS DEL TRATAMIENTO E INCIDENTES

CLAUSULAS EN EL CONTRATO DE TRANSMISIÓN

Recuerde que:

1. Si su organización es la Responsable del Tratamiento.
2. Se contrata a un tercero como Encargado del Tratamiento Usted debe exigir el cumplimiento de su Política de Tratamiento al tercero contratado. Si llega a haber una falta, es su empresa la que responde por negligencia ante la autoridad y el titular de los datos.



CLAUSULAS EN EL CONTRATO DE TRANSMISIÓN

Contrato de Transmisión

Para prever incidentes con el Tratamiento, se debe estipular:

Cláusulas

- "Protocolo de respuesta en el manejo de incidentes de seguridad.
- Roles y Responsabilidades.
- (SIC, 2020) Procedimiento para el trámite de consultas y dudas de los Titulares".

Cláusulas

- "Reporte de incidentes de seguridad por parte de otros Encargados del Tratamiento, en caso de "subencargos" sobre cualquier operación del Tratamiento.
- Cumplir PTI (Políticas de Tratamiento de Información) de su entidad."(SIC, 2020)

Esto no excluye a los Encargados de efectuar la notificación del incidente ante la SIC (Ley 1581-2012, Art. 18, lit. k)

URIBE · YÁÑEZ

4

CONSERVACIÓN DE REGISTROS DOCUMENTALES

SISTEMA DE ADMNISTRACIÓN DE RIESGOS

Para prever futuros incidentes de seguridad, es fundamental establecer un registro interno de cada falencia presenada, con la finalidad de:

1.“Demostrar el cumplimiento del régimen de protección de Datos Personales en caso de una investigación” (SIC, 2020).
2. Crea alertas para anticiparse a incidentes del mismo tipo.

Elementos para los Registros Documentales

Los registros deben contener:

a)Suficientes detalles para que la autoridad determine si se dio una respuesta competente.
b) Un sistema de seguridad para su protección de vulneraciones.
c) Debe tener un plazo de conservación.
d) Originalidad e integridad de la prueba técnica.*

CARACTERÍSTICAS DE LOS REGISTROS DOCUMENTALES

Tratamiento General y Medidas de Seguridad

Descripción general de las circunstancias del incidente (incluyendo la mención de la base de datos y los tipos de datos afectados)

Categorías de Titulares afectados

Fecha y hora del incidente de seguridad y de su descubrimiento

Exposición del proceder de la organización, indagaciones preliminares e investigaciones realizadas

Resumen de medidas correctivas

Responsables del manejo de incidentes del incidente

La prueba del reporte efectuado ante la SIC y la comunicación realizada a los Titulares de la información (si fue necesario)

Prueba de la evaluación de riesgo derivado del incidente de seguridad y los factores tenidos en cuenta

Inclusión de detalles personales (cuando deban establecerse

URIBE · YÁÑEZ

5

PROTOCOLO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD

URIBE · YÁÑEZ

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

1. Definición 

El protocolo es el "*marco general que incorpora roles, responsabilidades y acciones que deben ser desplegadas al interior de las organizaciones para gestionar un incidente de seguridad*" (SIC, 2020).

2. Proceso de manejo del Protocolo 

Para su incorporación en una organización,
debe ser:

a)Documentado.
b)Implementado.
C) Comunicado al equipo humano de la organización.
D) Monitoreado.

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

3. Factores para Definir los Protocolos

Cada organización debe tomar medidas de seguridad según:

1. Los niveles de riesgo del tratamiento para los derechos y libertades de los Titulares.
2. La naturaleza de los datos.
3. Las posibles afectaciones si se vulneran los datos del Titular.
4. Magnitud de titulares de los datos e información.

¿QUÉ DEBE INCLUIR EL PROTOCOLO DE TRATAMIENTO?

Depende de las necesidades de cada organización, sin embargo, aspectos generales que se deben incluir son:

1	**Explicaciónclara de qué constituye un incidente de seguridad**	Facilita al personal de la organización lo que es o no un incidente de seguridad
2	**Plan estratégico delineado y establecido para contener incidentes de seguridad**	Establece la capacidad del personal para atender incidentes y de qué manera se reportará la falla de seguridad ante la Fiscalía General de la Nación, SIC, Policía Nacional, etc.
3	**Roles y responsabilidades del personal**	Fundamental para repartir funciones en un incidente. También se debe mencionar el rol de la Alta Gerencia.
4	**Tiempos de atención y reporte de progreso en el protocolo**	Se deben establecer tiempos de atención al incidente y verificación del proceso. En este último, se debe establecer un rango de horas o días entre cada análisis del incidente para revisar el progreso de mitigación

URIBE · YÁÑEZ

¿QUÉ DEBE INCLUIR EL PROTOCOLO DE TRATAMIENTO?

Depende de las necesidades de cada organización, sin embargo, aspectos generales que se deben incluir son:

Una vez se gestione el incidente de seguridad, el equipo de respuesta debe evaluar si el protocolo necesita cambios.

Evaluación de efectividad del protocolo 5

Dividir las tareas o gestiones a cada una de las áreas encargadas de la mitigación de incidentes, buscando ser lo más eficientes.

Asignación de operaciones 6

Es fundamental tener un registro interno de los incidentes para efectos legales, permitiendo visualizar fácilmente el proceder de la corporación.

Documentación del incidente 7

La revisión de cómo ocurrió el incidente y su debido manejo deben ser analizados, para efectuar cambios en el protocolo o ahondar en los manejos que se realizaron correctamente.

Evaluación y análisis de la gestión 8

URIBE · YÁÑEZ

TIPOS DE INCIDENTES DE SEGURIDAD Y SUS CAUSAS

1.Tipos

Se clasifican dependiendo el grado de pérdida de las siguientes carácterica de información:

a) Confidencialidad
b) Integridad
c) Disponibilidad

2. Causas

- Inexistenciade políticaspreventivasde seguridad
- Negligenciahumana
- Casos fortuitos
- Actos maliciososo criminales
- Fallasenlos sistemasde la entidad
- Deficienciasenlas operaciones
- Alteración, pérdidao destrucciónde archivosfísicos

URIBE · YÁÑEZ

PASOS PARA RESPONDER A UN INCIDENTE DE SEGURIDAD

Gráfico tomado de Superintendencia de Industria y Comercio

URIBE · YÁÑEZ

Asesores Legales

Bogotá - Colombia
info@uribeyanez.com; gerencia@uribeyanez.com
Cra. 19B No. 83-02 oficina 304, Edificio Time Square

WWW.URIBEYANEZ.COM