Edición 30

Octubre 2025

BOLETÍN INFORMATIVO

La Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales

1. INTRODUCCIÓN

En la era digital, la información personal se ha convertido en uno de los activos más valiosos para las organizaciones. Sin embargo, su tratamiento inadecuado o la falta de medidas de seguridad puede generar incidentes que vulneren los derechos de los titulares.

Por ello, la gestión de incidentes de seguridad constituye un componente esencial dentro de los Sistemas de Gestión de Seguridad de la Información (SGSI) y de los Programas de Protección de Datos Personales, garantizando la confidencialidad, integridad y disponibilidad de la información.

⚖️ 2. MARCO NORMATIVO EN COLOMBIA

La Ley 1581 de 2012, junto con el Decreto 1377 de 2013 y la Circular Externa 003 de 2018 de la Superintendencia de Industria y Comercio (SIC), establece las obligaciones de los responsables y encargados del tratamiento de datos personales. Estas normas exigen que toda organización cuente con procedimientos para la gestión y reporte de incidentes de seguridad que afecten la protección de los datos personales de los ciudadanos.

3. DEFINICIÓN DE INCIDENTE DE SEGURIDAD

"Cualquier evento que afecte o pueda afectar la seguridad de la información y que tenga como consecuencia la alteración, pérdida, acceso, uso o divulgación no autorizada de datos personales."
Estos incidentes pueden ser causados por errores humanos, fallas técnicas o ataques deliberados.
A continuación, se describen algunos ejemplos reales y sus consecuencias.

EJEMPLO 1: ACCESO NO AUTORIZADO A UNA BASE DE DATOS

Un empleado o tercero obtiene acceso a información personal sin permisos adecuados, ya sea por vulnerar contraseñas o por descuidos internos.
Consecuencia: se exponen datos sensibles como números de identificación o información financiera, generando sanciones y pérdida de confianza.

EJEMPLO 2: PÉRDIDA O ROBO DE DISPOSITIVOS CON INFORMACIÓN

Un computador o USB con bases de datos personales es sustraído o extraviado.
Consecuencia: si los datos no están cifrados, cualquier persona podría acceder a ellos, lo que constituye una grave vulneración de la confidencialidad.

EJEMPLO 3: ENVÍO ERRÓNEO DE INFORMACIÓN A DESTINATARIOS INCORRECTOS

Un funcionario remite un documento con información personal a una dirección de correo equivocada.
Consecuencia: se divulgan datos personales sin autorización, lo cual genera responsabilidad para el responsable del tratamiento.

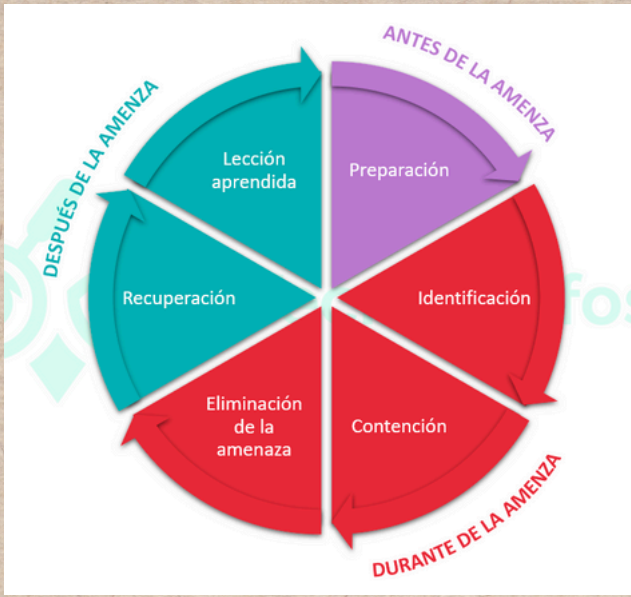
EJEMPLO 4: ATAQUE INFORMÁTICO TIPO RANSOMWARE

Ciberdelincuentes bloquean los sistemas y exigen dinero a cambio de liberar los datos.
Consecuencia: se paralizan operaciones y se ponen en riesgo datos personales, reputación y estabilidad económica.

EJEMPLO 5: ELIMINACIÓN ACCIDENTAL DE DATOS PERSONALES

Un empleado borra información relevante de clientes por error.
Consecuencia: se pierde disponibilidad de los datos, afectando la continuidad de los servicios y la gestión institucional.

⚙️ 4. FASES DEL PROCESO DE GESTIÓN DE INCIDENTES



⚙️ 1. PLANIFICACIÓN Y PREPARACIÓN

Se establecen políticas, procedimientos, herramientas y recursos para responder ante incidentes. Incluye la formación del personal, asignación de roles y creación de un Plan de Respuesta a Incidentes.

👁️ 2. DETECCIÓN Y REPORTE

Consiste en identificar eventos anómalos o sospechosos y reportarlos a tiempo a las áreas responsables. Se requiere monitoreo continuo y canales de comunicación eficientes.

⚖️ 3. EVALUACIÓN Y DECISIÓN

Se analiza la magnitud y causa del incidente, los datos afectados y el impacto potencial.
Permite determinar si se debe notificar a la Superintendencia de Industria y Comercio (SIC) o a los titulares.

🧯 4. RESPUESTA

Se ejecutan medidas técnicas y administrativas para contener el incidente y minimizar su impacto.
Ejemplos: restaurar copias de seguridad, bloquear accesos no autorizados, actualizar contraseñas y aplicar parches de seguridad.

💡 6. BUENAS PRÁCTICAS

Implementar medidas preventivas reduce significativamente la probabilidad de sufrir un incidente de seguridad y fortalece la cultura de protección de datos dentro de la organización. Algunas recomendaciones son:

🗒️ CONTAR CON UN PLAN DE RESPUESTA A INCIDENTES

Documentado, que defina responsabilidades, tiempos de reacción y canales de comunicación.

🎓 CAPACITAR DE FORMA CONTINUA AL PERSONAL

sobre seguridad de la información y protección de datos personales, fomentando la responsabilidad individual.

💾 REALIZAR COPIAS DE SEGURIDAD PERIÓDICAS

pruebas de recuperación para garantizar la disponibilidad de la información ante fallos o ataques.

🔐 USAR SISTEMAS DE CIFRADO Y CONTROL DE ACCESO

que limiten la manipulación de datos personales solo a usuarios autorizados.

⚙️ MANTENER ACTUALIZADO EL SOFTWARE Y LOS SISTEMAS DE SEGURIDAD

instalando parches y actualizaciones que corrijan vulnerabilidades.

🧠 FOMENTAR LA CONCIENCIA ORGANIZACIONAL

sobre la importancia de la privacidad y el cumplimiento normativo, integrando la seguridad como parte de la cultura instituciona

🧭 6. CONCLUSIÓN

Una adecuada gestión de incidentes permite proteger los derechos de los titulares, cumplir con la normatividad vigente y mantener la confianza institucional.
No basta con reaccionar ante un evento: la clave está en prevenir, aprender y mejorar continuamente los controles de seguridad.

🌟**"LA VERDADERA SEGURIDAD NACE DEL COMPROMISO Y LA CONCIENCIA DE CADA PERSONA; EN ESTE MUNDO DIGITAL, NUESTROS DATOS SON PARTE DE QUIENES SOMOS, Y PROTEGERLOS ES UN ACTO DE RESPETO HACIA NOSOTROS Y HACIA LOS DEMÁS."**🌟