# 1. Marco General

## 1.1. Objetivo

Establecer los procedimientos y responsabilidades para la gestión, contención, erradicación y recuperación ante cualquier **Incidente de Seguridad** o **Brecha de Datos Personales** que afecte la confidencialidad, integridad o disponibilidad de la información de los Titulares, garantizando el cumplimiento de la Ley 1581 de 2012.

## 1.2. Definiciones Operativas

- **Incidente de Seguridad:** Todo evento no deseado o inesperado que tiene una probabilidad significativa de comprometer las operaciones del negocio y la seguridad de los datos (ej. falla de *hardware*, detección de *malware*).
- **Brecha de Seguridad / Brecha de Datos Personales:** La materialización de un incidente que resulta en el **acceso, divulgación, pérdida o modificación no autorizada** de Datos Personales. **Toda brecha es un incidente, pero no todo incidente es una brecha.**
- **Equipo de Respuesta a Incidentes (ERI):** Grupo interdisciplinario responsable de ejecutar este protocolo.

## 1.3. Composición del Equipo de Respuesta a Incidentes (ERI)

| Rol | Responsabilidad Principal |
|---|---|
| **Líder / Oficial de Protección de Datos (DPO)** | Toma de decisiones, cumplimiento normativo, comunicación con la SIC y el Titular. |
| **Área de TI / Seguridad Informática** | Detección, análisis forense, contención técnica, erradicación, recuperación de sistemas. |
| **Área Legal / Jurídica** | Revisión de obligaciones legales de notificación, gestión de contratos con Encargados, preparación de respuestas legales. |
| **Área de Comunicaciones / Mercadeo** | Manejo de la comunicación externa (medios, Titulares) y mitigación del daño reputacional. |

## 2. Procedimiento Operativo: Fases de Respuesta

Este protocolo se divide en cinco fases consecutivas que deben ser ejecutadas inmediatamente tras la detección de una anomalía.

**FASE 1: Detección y Análisis (Triage)**

| Paso | Descripción del Procedimiento | Responsable | Plazo Objetivo |
|---|---|---|---|
| **1.1. Identificación** | El personal de TI o cualquier empleado identifica un evento (ej. alerta de *firewall*, pérdida de un dispositivo, reporte de un Titular). | Todo el Personal / TI | Inmediato |
| **1.2. Clasificación** | El ERI evalúa si el evento es un simple *Incidente* o una *Brecha de Datos Personales*. Se documenta qué datos fueron afectados (sensibles, financieros, de identificación) y la posible causa. | TI / DPO | 1 hora |
| **1.3. Activación** | El DPO declara formalmente la Brecha de Seguridad e inicia el protocolo completo, alertando a todos los miembros del ERI. | DPO | Inmediato tras la clasificación |

**FASE 2: Contención y Erradicación**

El objetivo es detener el incidente y evitar daños mayores.

| Paso | Descripción del Procedimiento | Responsable |
|---|---|---|
| **2.1. Contención Inmediata** | **Aislamiento:** Desconectar de la red los sistemas o *endpoints* comprometidos. **Bloqueo:** Desactivar cuentas de usuario sospechosas o credenciales filtradas. | TI |

| Paso | Descripción del Procedimiento | Responsable |
|---|---|---|
| **2.2. Análisis Forense** | Realizar una copia forense del estado actual de los sistemas para preservar la evidencia. Documentar *logs*, hora de inicio del ataque y método utilizado (vector de ataque). | TI |
| **2.3. Erradicación** | Una vez identificado el vector, eliminar la causa raíz (ej. parchear el *software*, eliminar el *malware*, cambiar configuraciones de seguridad). | TI |

**FASE 3: Recuperación y Revisión**

El objetivo es restaurar la operatividad y la integridad de los datos.

| Paso | Descripción del Procedimiento | Responsable |
|---|---|---|
| **3.1. Restauración Segura** | Restaurar los sistemas afectados utilizando las copias de seguridad (*backups*) verificadas (Fase 1 del Manual de Riesgos) que se sepa que son seguras y no están contaminadas. | TI |
| **3.2. Verificación de Integridad** | Validar que los datos restaurados son completos, veraces y que el sistema está limpio antes de reconectarlo a la red de producción. | TI |
| **3.3. Monitoreo Reforzado** | Mantener un monitoreo intensivo del sistema recuperado para detectar cualquier actividad anómala recurrente. | TI |

**FASE 4: Comunicación y Notificación (Obligaciones de Ley)**

La notificación es una obligación legal en Colombia, especialmente si existe un riesgo cierto para los Titulares.

| Paso | Descripción del Procedimiento | Responsable | Plazo Crítico |
|---|---|---|---|
| **4.1. Evaluación de Impacto** | Evaluar la severidad de la brecha y si existe un **riesgo cierto e inminente** para los derechos de los Titulares (ej. robo de datos sensibles o financieros). | DPO / Legal | 4 horas post-clasificación |
| **4.2. Notificación a la SIC** | Si el riesgo es alto, el DPO prepara y envía una comunicación oficial a la Superintendencia de Industria y Comercio (SIC) informando sobre la brecha. | DPO | **Recomendado: Máximo 72 horas** |
| **4.3. Notificación al Titular** | Si la brecha puede afectar seriamente al Titular, se le notifica la situación utilizando el canal más seguro disponible (ej. correo certificado, llamada telefónica verificada), detallando: *Naturaleza del incidente, datos comprometidos, medidas tomadas y recomendaciones al Titular.* | DPO / Comunicaciones | A la brevedad posible |

**FASE 5: Evaluación Post-Incidente**

| Paso | Descripción del Procedimiento | Responsable | Plazo Objetivo |
|---|---|---|---|
| **5.1. Documentación Final** | El ERI elabora un informe final detallando la causa raíz, las acciones de contención, los costos | DPO | 5 días hábiles |

| Paso | Descripción del Procedimiento | Responsable | Plazo Objetivo |
|---|---|---|---|
| | incurridos y el impacto final en los Titulares. | | |
| **5.2. Lecciones Aprendidas** | Realizar una reunión de análisis para identificar las fallas en los controles de seguridad y/o en el protocolo de respuesta. | ERI | 10 días hábiles |
| **5.3. Mejora Continua** | Implementar los cambios necesarios en el Manual de Riesgos y en los Controles Técnicos y de Formación para evitar la recurrencia del mismo tipo de brecha. | TI / DPO | Continua |

**LUIS HERNAN BONILLA CUERVO**

Representante Legal

ARIAPSW S.A.S.