**PROTOCOLO DE GESTIÓN DE INCIDENTES DE SEGURIDAD**

**FUSIONSOLUTIONS CIA. LTDA.**

## 1. INFORMACIÓN GENERAL Y RESPONSABLES

- **Responsable del Tratamiento:** FUSIONSOLUTIONS CIA. LTDA.
- **RUC:** 1792322804001
- **Delegado de Protección de Datos (DPO):** Luis Villarroel
- **Contacto DPO:** 0998539764 | info@abogadoslatam.com

## 2. OBJETIVO

Establecer los pasos a seguir ante cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los datos personales manejados por la empresa, especialmente en aquellos almacenados en infraestructura internacional (USA) o plataformas de terceros (Intuit).

## 3. FASES DEL PROTOCOLO

### Fase I: Identificación y Reporte

Cualquier colaborador que detecte una anomalía (ej. acceso no autorizado a sistemas bibliotecarios, pérdida de un backup, error en migración o ingreso sospechoso a Intuit) deberá:

1. Notificar de inmediato al **DPO**.
2. No manipular el sistema afectado para preservar la evidencia digital.
3. Completar el reporte inicial con la hora del hallazgo y el sistema comprometido.

### Fase II: Clasificación del Incidente

El DPO categorizará el incidente según su gravedad:

- **Nivel 1 (Bajo):** Afectación interna sin salida de datos al exterior.
- **Nivel 2 (Medio):** Pérdida temporal de disponibilidad o alteración de datos sin compromiso de datos sensibles.

- **Nivel 3 (Alto):** Fuga de información personal, acceso no autorizado a bases de datos de clientes en USA o compromiso de datos de personal. *Este nivel requiere notificación legal obligatoria.*

**Fase III: Contención y Mitigación**

Dependiendo del proceso afectado, se aplicarán las siguientes medidas:

- **Procesos Cloud/Hosting:** Bloqueo de IPs sospechosas, cambio masivo de credenciales y desconexión de servidores si es necesario.
- **Soporte Técnico:** Revocación de accesos remotos y auditoría de logs de sesión.
- **Backups:** Verificación de la integridad del último respaldo (ciclo de 3 meses) y restauración en entorno seguro.

**Fase IV: Investigación y Resolución**

Se analizará la causa raíz (ej. falta de regulación contractual con el proveedor en USA o debilidad en la contraseña del sistema contable) y se documentarán las acciones tomadas para cerrar la vulnerabilidad.

## 4. REGISTRO DE INCIDENTES (LOG)

La empresa llevará un registro detallado de cada evento con los siguientes campos:

| Fecha | Proceso Afectado | Descripción del Incidente | Impacto en Titulares | Medidas de Remediación |
|---|---|---|---|---|
| | | | | |

## 5. MEDIDAS DE PREVENCIÓN DERIVADAS

Como parte de la mejora continua, tras un incidente se deberán reforzar los siguientes puntos críticos detectados en el RAT:

- **Transferencias Internacionales:** Asegurar que los proveedores en USA cumplan con niveles de seguridad equivalentes a la LOPDP.
- **Plazos de Conservación:** Ejecutar la eliminación definitiva de datos temporales tras los 3 meses estipulados para evitar acumulación de riesgos.
- **Gestión de Personal:** Implementar doble factor de autenticación en el software contable para proteger los datos de los empleados.

## 6. NOTIFICACIÓN EXTERNA

Si el incidente implica un riesgo para los derechos de los ciudadanos, el DPO coordinará la comunicación oficial en un plazo máximo de **72 horas** desde el conocimiento del hecho, detallando el alcance de la brecha y las recomendaciones para los afectados.