1. Metodología y Alcance

- **Objetivo:** Identificar, analizar, evaluar y tratar los riesgos asociados al **Tratamiento de Datos Personales (DP)** y de **Hábeas Data Financiero**, para garantizar la seguridad y el cumplimiento normativo.
- **Alcance:** Aplica a todos los procesos, sistemas de información y personas que participan en la recolección, almacenamiento, uso, circulación y supresión de DP dentro de la organización.
- **Criterios de Evaluación:** Se evaluará la **Probabilidad** de ocurrencia y el **Impacto** potencial sobre los derechos de los Titulares y la organización (sanciones, reputación, demandas).

2. Matriz de Identificación de Riesgos Clave

A continuación, se presenta una tabla que detalla los riesgos más comunes asociados a los principios de la Ley 1581 de 2012 y la Ley 1266 de 2008.

Categoría de Riesgo	**Descripción del Riesgo**	**Impacto Potencial (Alto/Medio/Bajo)**	**Normativa Afectada**
I. Legalidad y Finalidad			
R1: Tratamiento sin autorización	Recolección o uso de DP sin el consentimiento previo, expreso e informado del Titular, o uso para una finalidad diferente a la autorizada.	**Alto** (Sanciones SIC)	Ley 1581/12, Art. 9
R2: Datos Sensibles	Tratamiento de Datos Sensibles sin cumplimiento de los requisitos legales o sin la autorización reforzada.	**Alto** (Vulneración Derechos Fundamentales)	Ley 1581/12, Art. 6
II. Seguridad y Calidad (Veracidad)			
R3: Filtración o Acceso no Autorizado	Vulneración de los sistemas de seguridad que permite el acceso, modificación o divulgación indebida de DP	**Alto** (Daño Reputacional y Sanciones)	Ley 1581/12, Art. 19

Categoría de Riesgo	**Descripción del Riesgo**	**Impacto Potencial (Alto/Medio/Bajo)**	**Normativa Afectada**
	(ciberataques, errores humanos).		
R4: Inexactitud de Datos	Fallas en la actualización o depuración de las bases de datos, manteniendo información errónea o incompleta.	**Medio** (Vulneración Derechos Titular)	Ley 1581/12, Art. 4
III. Derechos de los Titulares (ARCO)			
R5: Negligencia en Solicitudes	Incumplimiento de los términos legales para atender consultas, reclamos o solicitudes de supresión de datos.	**Medio** (Sanciones por Incumplimiento de Deberes)	Ley 1581/12, Art. 15
R6: Revocatoria ignorada	No aplicar la solicitud de revocatoria de la autorización, continuando con el envío de comunicaciones o el tratamiento del dato.	**Medio** (Tratamiento Ilegítimo)	Ley 1581/12, Art. 14
IV. Hábeas Data Financiero (L. 1266)			
R7: Reporte Financiero Indebido	Reportar información negativa (mora) sin la debida comunicación previa al Titular, o reportar fuera del término legal de permanencia (L. 2157/21).	**Alto** (Sanciones y Demandas)	Ley 1266/08, Art. 12

3. Controles y Tratamiento de Riesgos

Para mitigar los riesgos identificados, la organización debe implementar controles efectivos, divididos en tres áreas: Legal/Organizacional, Humano y Técnico.

3.1. Controles Legales y Organizacionales (Mitigación R1, R2, R5, R7)

Riesgo Mitigado	Control Específico	Descripción del Control
R1, R2	**Formato de Autorización Unificado**	Desarrollar un formato estándar de autorización que sea **explícito, informado** y que diferencie claramente el tratamiento de Datos Sensibles (con casilla de aceptación separada).
R5	**Procedimiento de ARCO Formalizado**	Documentar el flujo de las solicitudes de Titulares (ARCO) estableciendo responsables, plazos y el registro de la trazabilidad.
R7	**Protocolo de Reporte Financiero**	Implementar un protocolo estricto que garantice la **comunicación previa** (certificada) y la revisión del término máximo de permanencia de la información negativa antes de cualquier reporte a centrales de riesgo.
General	**Designación del Oficial de Datos**	Nombrar un responsable interno para la supervisión del cumplimiento y la gestión de riesgos.

3.2. Controles Humanos y de Formación (Mitigación R3, R4)

Riesgo Mitigado	Control Específico	Descripción del Control
R3	**Capacitación Periódica**	Realizar sesiones obligatorias de formación sobre la Política de Datos, enfocadas en la prevención de errores humanos y la concientización sobre el manejo seguro de la información.
R3	**Acuerdos de Confidencialidad (NDA)**	Incluir cláusulas de confidencialidad en los contratos laborales y de prestación de servicios, con énfasis en el deber de reserva de la información.

Riesgo Mitigado	Control Específico	Descripción del Control
R4	**Auditoría de Calidad de Datos**	Establecer un proceso trimestral de revisión y validación de las bases de datos para identificar y corregir registros duplicados, incompletos o desactualizados.

3.3. Controles Técnicos y de Seguridad (Mitigación R3)

Riesgo Mitigado	Control Específico	Descripción del Control
R3	**Gestión de Acceso por Roles (RBAC)**	Restringir el acceso a las bases de datos únicamente al personal cuya función lo requiera, implementando niveles de privilegio (solo lectura, escritura, eliminación).
R3	**Cifrado (*Encryption*)**	Aplicar mecanismos de cifrado a la información sensible y a las bases de datos almacenadas, y/o durante la transmisión de datos.
R3	**Copias de Seguridad (Backup)**	Implementar una política de *backup* periódico y verificable, almacenado de forma segura y segregada, para garantizar la disponibilidad e integridad de los datos ante un incidente.
R3	***Firewall* y Antivirus Actualizados**	Mantener soluciones de seguridad perimetral y de *endpoint* actualizadas para prevenir intrusiones y *malware*.

4. Plan de Respuesta a Incidentes de Seguridad

Este plan debe activarse inmediatamente después de detectarse un evento de seguridad que comprometa la integridad, confidencialidad o disponibilidad de los DP.

1. **Detección y Contención:** Aislar el sistema afectado para evitar la propagación del incidente.

2. **Análisis Forense:** Identificar la causa raíz, el alcance de la brecha y los datos comprometidos.
3. **Notificación a Titulares:** Si el incidente compromete gravemente los derechos de los Titulares, se debe notificar a los afectados y a la **Superintendencia de Industria y Comercio (SIC)** en un plazo no superior a 72 horas desde que se tuvo conocimiento (aunque la ley no establece un plazo fijo, es la práctica recomendada).
4. **Recuperación y Medidas Correctivas:** Restaurar los sistemas y aplicar los controles permanentes para evitar la recurrencia.

LUIS HERNAN BONILLA CUERVO

Representante Legal

ARIAPSW S.A.S.