1. Introducción y Ámbito de Aplicación

- **Objetivo:** Establecer las directrices técnicas, administrativas y humanas necesarias para proteger los **Datos Personales (DP)** contra la alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de conformidad con la Ley 1581 de 2012.
- **Alcance:** Estos protocolos son de obligatorio cumplimiento para todo el personal de la organización (empleados, contratistas y terceros) que, por la naturaleza de su trabajo, manipule o tenga acceso a bases de datos o sistemas que contengan DP.

2. Seguridad Organizacional y Responsabilidades

Procedimiento	Responsable	Descripción Detallada
2.1. Gestión por Roles (RBAC)	DPO y TI	El DPO, en coordinación con TI, definirá un **mapa de acceso** a las bases de datos y sistemas que contienen DP. El acceso se concederá solo a la información estrictamente necesaria para el desempeño de cada rol (*Principio de Mínimo Privilegio*).
2.2. Revisión de Contratos	Área Legal	Todos los contratos con Encargados del Tratamiento (proveedores de *hosting*, servicios en la nube, etc.) deben incluir cláusulas que los obliguen a cumplir con los mismos estándares de seguridad definidos en este Manual.
2.3. Auditorías Internas	DPO y Auditoría	Se realizarán auditorías periódicas (anuales o bianuales) para verificar el cumplimiento de estos protocolos, los controles de seguridad y la documentación completa de las bases de datos.

3. Protocolos de Seguridad Técnica (Controles de TI)

Estos procedimientos buscan proteger los sistemas de información donde residen los datos.

3.1. Control de Acceso y Autenticación

1. **Contraseñas Robustas:** El sistema exigirá a todos los usuarios contraseñas de al menos 12 caracteres, que combinen mayúsculas, minúsculas, números y símbolos. Las contraseñas se deben cambiar obligatoriamente cada 90 días.
2. **Doble Factor de Autenticación (2FA):** La autenticación de dos factores será obligatoria para el acceso a sistemas críticos, bases de datos o herramientas que permitan la extracción masiva de DP.
3. **Bloqueo Automático:** Las sesiones de usuario en computadores y sistemas se bloquearán automáticamente tras 10 minutos de inactividad, obligando a reingresar la contraseña.

3.2. Cifrado y Respaldo (Backups)

1. **Cifrado en Tránsito:** Toda transmisión de DP a través de redes públicas (internet) debe utilizar protocolos seguros (ej. TLS/SSL) y estar cifrada.
2. **Cifrado en Reposo:** Los datos sensibles deben estar almacenados en bases de datos o dispositivos que apliquen cifrado (*encryption at rest*).
3. **Política de Backups:** Se realizarán copias de seguridad completas de todas las bases de datos críticas diariamente. Estos *backups* se almacenarán en una ubicación separada de la red de producción, aplicando cifrado y pruebas periódicas de restauración para verificar su integridad.

3.3. Seguridad Perimetral y de Red

1. ***Firewall* y Detección de Intrusos (IDS):** El *firewall* principal debe filtrar el tráfico y bloquear accesos sospechosos. Se mantendrá un sistema IDS activo para alertar al personal de TI sobre posibles intrusiones o actividades anómalas.
2. ***Patch Management:*** Se implementará un protocolo de gestión de parches para aplicar inmediatamente las actualizaciones de seguridad a todos los sistemas operativos, *software* de base de datos y aplicaciones utilizadas para el Tratamiento de Datos.
3. ***Antimalware* Centralizado:** Se mantendrá un *software* antivirus y *antimalware* instalado y actualizado centralizadamente en todos los servidores y equipos de trabajo.

4. Protocolos de Seguridad Humana y Operativa

El factor humano es la principal vulnerabilidad en la seguridad de la información.

4.1. Concientización y Formación

1. **Formación Inicial y Anual:** Todo el personal nuevo debe recibir una formación obligatoria sobre la Política de Tratamiento de Datos y estos Protocolos de Seguridad. Se debe repetir un curso de concientización anualmente.
2. **Deber de Reserva:** El personal debe ser consciente de su **deber de reserva y confidencialidad** sobre los DP, obligación que subsiste incluso después de la terminación de su relación laboral o contractual con la organización.

4.2. Protocolo de Escritorio Limpio y Pantalla Despejada

1. **Escritorio Limpio:** Queda prohibido dejar documentos físicos o notas que contengan DP sin vigilancia. Estos deben guardarse bajo llave al finalizar la jornada o cuando el puesto de trabajo esté desatendido.
2. **Pantalla Despejada:** Los usuarios deben abstenerse de anotar contraseñas o información de acceso en papeles visibles o en el equipo. Las pantallas de los equipos deben estar orientadas de forma que se evite la visualización por parte de terceros no autorizados.
3. **Prohibición de Almacenamiento Local:** Se prohíbe el almacenamiento de bases de datos o archivos con DP en discos duros locales, memorias USB no autorizadas o servicios de almacenamiento en la nube personales. Todo DP debe residir únicamente en los servidores o sistemas corporativos designados.

5. Protocolos de Seguridad Física

1. **Acceso Restringido a Servidores:** El acceso al cuarto de servidores o *datacenter* donde se almacenan las bases de datos debe estar restringido a personal de TI autorizado. El acceso debe ser controlado mediante tarjetas de proximidad o biometría y llevar un registro de entrada y salida.
2. **Vigilancia:** Las áreas donde se manipule o almacene información sensible (ej. archivos físicos, oficinas de atención al cliente) deben contar con sistemas de videovigilancia y control de acceso.

LUIS HERNAN BONILLA CUERVO

Representante Legal

ARIAPSW S.A.S.