POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO Y COMPROMISO

La presente política establece las directrices para garantizar la Confidencialidad, Integridad y Disponibilidad de los activos de información de Bahos & Burbano. Como firma de práctica digital, asumimos la seguridad como un componente indisociable del secreto profesional y la excelencia jurídica.

2. MARCO NORMATIVO

Esta política se fundamenta en la Constitución Política de Colombia, la Ley 1581 de 2012, el Decreto 1074 de 2015, y se alinea con los estándares internacionales ISO/IEC 27001:2022 y las directrices de ciberseguridad para servicios legales vigentes.

3. ARQUITECTURA DE SEGURIDAD: MODELO "ZERO TRUST"

La Firma adopta un modelo de Confianza Cero (Zero Trust), bajo el cual no existe la confianza implícita por ubicación de red o propiedad del dispositivo. Todo acceso a la información está sujeto a:

- **Autenticación Robusta:** Uso obligatorio de factores de autenticación multifactor (MFA) de grado bancario.
- **Privilegio Mínimo:** El acceso se concede estrictamente sobre la base de la necesidad de saber para el cumplimiento de la labor jurídica.

4. MEDIDAS TÉCNICAS DE PROTECCIÓN

Para mitigar riesgos de interceptación, alteración o pérdida, la Firma implementa:

- **Cifrado Avanzado:** Toda información en tránsito y en reposo es protegida mediante algoritmos de cifrado asimétrico de última generación (AES-256 o superior).
- **Arquitectura Desacoplada:** El ecosistema digital de la Firma opera sobre infraestructuras de computación en la nube distribuidas, eliminando puntos únicos de fallo y garantizando alta disponibilidad.

- **Integridad Verificada:** Los documentos oficiales emitidos por la Firma cuentan con firmas digitales o identificadores criptográficos que permiten verificar su autenticidad y detectar cualquier alteración posterior.

5. SEGURIDAD EN EL CICLO DE VIDA DE LOS DATOS

La gestión de la información sigue un proceso de Seguridad desde el Diseño:

- **Captura Segura:** Canales de comunicación con cifrado de extremo a extremo.
- **Almacenamiento Resiliente:** Uso de repositorios en la nube con redundancia geográfica.
- **Despliegue Controlado:** Los cambios en nuestra infraestructura digital se realizan mediante procesos automatizados que incluyen pruebas de seguridad previas a su puesta en producción.

6. GOBERNANZA DE INTELIGENCIA ARTIFICIAL Y NUEVAS TECNOLOGÍAS

En el uso de herramientas de procesamiento avanzado e IA, la Firma garantiza:

- **No Reutilización de Datos:** No se emplean datos de clientes para el entrenamiento de modelos de IA públicos.
- **Soberanía de Información:** Los datos permanecen bajo el control y jurisdicción establecidos en los acuerdos de nivel de servicio (SLA) de seguridad.

7. RESILIENCIA Y CONTINUIDAD OPERATIVA

Ante incidentes de seguridad o desastres tecnológicos, la Firma garantiza la continuidad mediante:

- **Protocolos de Respuesta Inmediata**: Capacidad de restauración de servicios en tiempos inferiores a los estándares del mercado.
- **Backups Inmutables:** Copias de seguridad protegidas contra ataques de borrado o cifrado malintencionado (Ransomware).

8. CLÁUSULA DE CONFIDENCIALIDAD SUPREMA

En concordancia con los valores de la Firma:

"TODA INFORMACIÓN SUMINISTRADA SERÁ TRATADA BAJO ESTRICTOS PROTOCOLOS DE CONFIDENCIALIDAD Y NUESTRA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN."

El incumplimiento de las directrices aquí contenidas por parte de colaboradores o terceros dará lugar a las acciones legales, civiles y penales correspondientes, así como a las sanciones ante el Consejo Superior de la Judicatura y/o la Comisión Nacional de Disciplina Judicial si a ello hubiere lugar.

9. VIGENCIA Y ACTUALIZACIÓN

Esta política es dinámica y se actualiza periódicamente para responder a la evolución del panorama de amenazas cibernéticas.

Última revisión: *19 de enero de 2026*.