2025

Capital Bridge

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS DE CAPITAL BRIDGE

En **Capital Bridge** entendemos que la confianza es la base de toda relación financiera. Sabemos que al compartir tu información personal y financiera con nosotros nos confías un activo de valor incalculable: tus datos. Por ello, nuestro compromiso con la privacidad es absoluto y no negociable.
La presente **Política de Privacidad y Protección de Datos** establece cómo recopilamos, procesamos, utilizamos, protegemos y, en casos específicos, compartimos la información personal de nuestros clientes, usuarios, socios estratégicos y visitantes de nuestras plataformas físicas y digitales.
Este documento refleja **los más altos estándares internacionales en materia de protección de datos**, incluyendo, pero no limitándose a:

- **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea.
- **Ley de Protección de Datos Personales en Colombia** (Ley 1581 de 2012 y decretos reglamentarios).
- **Ley Federal de Protección de Datos Personales en Posesión de Particulares** (México).
- Principios y directrices de la **OCDE para la Privacidad**.
- **Normas ISO/IEC 27001 y 27701** para la seguridad y gestión de datos personales.

1. ÁMBITO DE APLICACIÓN

Esta política aplica a:
- Todos los servicios de inversión, gestión de capital, consultoría y análisis de mercado que prestamos.
- Nuestras plataformas web, aplicaciones móviles, oficinas físicas y canales de comunicación.
- Los datos personales y financieros de clientes, empleados, proveedores y prospectos.

No se limita únicamente a clientes activos: también cubre a antiguos clientes, potenciales inversores y personas que interactúan con Capital Bridge de cualquier forma.

2. INFORMACIÓN QUE RECOPILAMOS

2.1 Datos de identificación personal
- Nombre completo, fecha y lugar de nacimiento, nacionalidad, género.
- Documentos oficiales de identidad: pasaporte, DNI, cédula, licencia de conducir.
- Firma y, en procesos de verificación avanzada, datos biométricos (huellas, reconocimiento facial, voz).

2.2 Datos de contacto
- Dirección física de residencia y correspondencia.
- Teléfonos fijos y móviles.
- Correos electrónicos corporativos y personales.

2.3 Datos financieros y bancarios
- Información de cuentas bancarias, custodias y billeteras digitales.
- Historial de inversiones, transacciones y operaciones de trading.
- Información de pagos y depósitos, cifrada bajo estándares **PCI DSS**.

2.4 Datos técnicos y de acceso
- Dirección IP, tipo y versión de navegador, sistema operativo, identificador único de dispositivo.
- Datos de geolocalización (cuando el usuario lo permite).
- Registro de actividad en nuestras plataformas, incluyendo fecha, hora y acciones realizadas.

2.5 Datos derivados de cumplimiento regulatorio
- Información recabada en procedimientos **KYC (Know Your Customer)** y **AML/CFT (Anti-Money Laundering / Combating the Financing of Terrorism)**.
- Declaraciones de beneficiarios finales.
- Certificaciones fiscales y documentación para prevención de evasión tributaria.

2.6 Datos de comunicaciones
- Llamadas telefónicas grabadas para control de calidad y evidencia contractual.
- Registros de chats en vivo, correos electrónicos y tickets de soporte.

3. FINALIDADES DEL TRATAMIENTO

En Capital Bridge procesamos tu información para:
1. **Prestación de servicios financieros**: apertura y administración de cuentas, ejecución de órdenes de inversión, seguimiento de portafolios, elaboración de reportes y análisis de mercado.
2. **Cumplimiento normativo**: reportes a autoridades regulatorias, implementación de políticas de prevención de blanqueo de capitales y financiamiento del terrorismo.
3. **Gestión de riesgos**: detección de operaciones inusuales, análisis de patrones transaccionales y bloqueo preventivo de actividades sospechosas.
4. **Optimización de experiencia**: personalización de interfaces, recomendaciones basadas en perfil de riesgo, acceso a herramientas de análisis avanzado.
5. **Comunicaciones**: envío de notificaciones sobre operaciones, estados de cuenta, alertas regulatorias, boletines financieros y oportunidades de inversión.
6. **Investigación y desarrollo**: análisis de comportamiento de clientes, estudios de mercado y pruebas de nuevos productos.

4. BASES LEGALES PARA EL TRATAMIENTO

El tratamiento de datos personales por parte de Capital Bridge se sustenta en:
- El **consentimiento expreso** del titular de los datos.
- El **cumplimiento de obligaciones legales y regulatorias**.
- La **ejecución de un contrato** o relación precontractual con el titular.
- El **interés legítimo** de Capital Bridge para prevenir fraudes y optimizar servicios.

5. COMPARTICIÓN Y TRANSFERENCIA DE DATOS

5.1 Principios
- No vendemos, alquilamos ni comerciamos con tus datos personales.
- Toda transferencia se realiza bajo estrictos acuerdos de confidencialidad y seguridad.

5.2 Destinatarios posibles
- Proveedores de servicios tecnológicos y financieros.
- Entidades bancarias y custodios de valores.
- Firmas auditoras y consultoras regulatorias.
- Autoridades competentes, nacionales o extranjeras, en cumplimiento de la ley.

5.3 Transferencias internacionales
Si tus datos se transfieren a países fuera de tu jurisdicción, garantizamos el cumplimiento de **mecanismos de protección equivalentes**, como las **Cláusulas Contractuales Tipo** de la UE o marcos de privacidad aprobados.

6. SEGURIDAD DE LA INFORMACIÓN

Capital Bridge aplica un **Sistema Integral de Seguridad de la Información** con:
- Cifrado AES-256 para datos en reposo y TLS 1.3 para datos en tránsito.
- Firewalls de nueva generación, filtrado de tráfico y sistemas IDS/IPS.
- Autenticación multifactor (MFA) para clientes y personal.
- Accesos basados en el principio de "mínimo privilegio".
- Monitoreo 24/7 por un **Centro de Operaciones de Seguridad (SOC)**.
- Centros de datos con certificaciones **ISO 27001, SOC 1 y SOC 2**.

7. PREVENCIÓN DE FRAUDES Y CUMPLIMIENTO

- Procedimientos KYC reforzados para todos los clientes.
- Monitoreo continuo de operaciones para identificar movimientos inusuales.
- Reportes de operaciones sospechosas a autoridades competentes.
- Auditorías internas y externas periódicas en materia de seguridad y cumplimiento.

8. RETENCIÓN Y ELIMINACIÓN DE DATOS

Conservaremos la información durante el tiempo necesario para cumplir con las finalidades de tratamiento, con plazos mínimos de **5 a 10 años** para datos financieros según la normativa.
Los datos se eliminan mediante **borrado seguro certificado** y destrucción física de soportes, impidiendo cualquier recuperación.

9. DERECHOS DEL TITULAR

Puedes ejercer los derechos de:
- **Acceso** a tus datos.
- **Rectificación** de información inexacta.
- **Cancelación** o eliminación de datos.
- **Oposición** al tratamiento.
- **Limitación** del uso.
- **Portabilidad** de datos a otro proveedor.

Para ejercer estos derechos, deberás presentar una solicitud por escrito y verificar tu identidad.

10. COOKIES Y TECNOLOGÍAS SIMILARES

Capital Bridge utiliza cookies para:
- Mejorar la navegación.
- Personalizar la experiencia.
- Analizar el rendimiento de la plataforma.
- Ofrecer publicidad segmentada.

Puedes desactivar o limitar las cookies desde tu navegador, aunque algunas funciones podrían verse afectadas.

11. ENLACES A SITIOS EXTERNOS

Nuestras plataformas pueden contener enlaces a sitios de terceros. Capital Bridge no se responsabiliza por las prácticas de privacidad de dichos sitios y recomienda revisar sus políticas antes de interactuar.

12. MENORES DE EDAD

No recopilamos intencionadamente datos de menores de 18 años sin consentimiento verificable de padres o tutores.

13. MODIFICACIONES DE LA POLÍTICA

Podremos modificar esta política para adaptarla a cambios regulatorios, tecnológicos o de negocio. Las actualizaciones se publicarán en nuestros canales oficiales con la fecha de entrada en vigor.ANEXO I – Artículos del GDPR Aplicables

La presente política se ajusta especialmente a los siguientes artículos del **Reglamento (UE) 2016/679 (GDPR)**:

1. **Art. 5 – Principios relativos al tratamiento**
   - Licitud, lealtad y transparencia.
   - Limitación de la finalidad.
   - Minimización de datos.
   - Exactitud.
   - Limitación del plazo de conservación.
   - Integridad y confidencialidad.
2. **Art. 6 – Licitud del tratamiento**
   - Consentimiento.
   - Ejecución contractual.
   - Cumplimiento de obligaciones legales.
   - Intereses legítimos.
3. **Art. 7 – Condiciones del consentimiento**
   - Consentimiento libre, informado y verificable.
4. **Art. 12 a 14 – Transparencia y comunicación**
   - Información clara sobre el uso de datos.
   - Plazos para la entrega de información.
5. **Art. 15 a 22 – Derechos del interesado**
   - Derecho de acceso, rectificación, supresión, limitación, portabilidad y oposición.
6. **Art. 24 a 32 – Responsabilidad proactiva y seguridad**
   - Medidas técnicas y organizativas apropiadas.
   - Gestión de riesgos.
   - Cifrado y seudonimización.
7. **Art. 33 y 34 – Notificación de violaciones de datos**
   - Comunicación a la autoridad competente en un máximo de 72 horas.
   - Notificación al interesado cuando sea necesario.
8. **Art. 44 a 50 – Transferencias internacionales**
   - Salvaguardas adecuadas para el envío de datos fuera del EEE.

ANEXO II – Procedimientos Internos y Protocolos de Respuesta ante Incidentes de Datos

1. Clasificación de la Información

- **Nivel 1:** Información pública (material de marketing, información corporativa no confidencial).
- **Nivel 2:** Información interna (procedimientos operativos, manuales internos).
- **Nivel 3:** Información confidencial (datos personales de clientes e inversores).
- **Nivel 4:** Información crítica (datos financieros sensibles, credenciales de acceso, registros AML/KYC).

2. Controles Preventivos

- **Autenticación reforzada:** doble factor para todo acceso a sistemas internos.
- **Cifrado de extremo a extremo:** AES-256 para almacenamiento, TLS 1.3 para transmisión.
- **Monitorización 24/7:** detección automática de intrusiones y actividad anómala.
- **Segmentación de redes:** separación de entornos críticos y públicos.

3. Protocolo de Respuesta ante Incidentes

Fase 1 – Detección:
- Monitorización continua por sistemas SIEM (Security Information and Event Management).
- Alertas automáticas ante actividad no autorizada.

Fase 2 – Contención:
- Bloqueo inmediato de accesos sospechosos.
- Aislamiento de sistemas afectados.

Fase 3 – Evaluación:
- Análisis forense digital para determinar alcance y origen.
- Identificación de datos comprometidos.

Fase 4 – Notificación:
- Aviso a la Autoridad de Protección de Datos en **máximo 72 horas** (Art. 33 GDPR).
- Comunicación a los interesados si existe riesgo para sus derechos y libertades (Art. 34 GDPR).

Fase 5 – Recuperación:
- Restauración de sistemas a partir de copias de seguridad verificadas.
- Implementación de mejoras preventivas.

Fase 6 – Documentación y Auditoría:
- Registro detallado del incidente, medidas aplicadas y tiempos de respuesta.
- Revisión anual de protocolos para mejoras continuas.

4. Auditorías y Formación

- Auditorías internas semestrales de cumplimiento de seguridad y privacidad.
- Formación obligatoria anual a todo el personal en materia de **protección de datos y ciberseguridad**.
- Simulacros de incidentes para medir tiempos de respuesta.

2025

Capital Bridge

PRIVACY POLICY AND DATA PROTECTION

PRIVACY POLICY AND DATA PROTECTION OF CAPITAL BRIDGE

At Capital Bridge, we understand that trust is the foundation of any financial relationship. We know that by sharing your personal and financial information with us, you are entrusting us with an invaluable asset: your data. For this reason, our commitment to privacy is absolute and non-negotiable.
This Privacy and Data Protection Policy sets out how we collect, process, use, protect, and, in specific cases, share the personal information of our clients, users, strategic partners, and visitors to our physical and digital platforms.
This document reflects the highest international standards in data protection, including but not limited to:

- **General Data Protection Regulation (GDPR)** of the European Union.
- **OECD Principles and Guidelines** on Privacy.
- **ISO/IEC 27001 and 27701 Standards** for information security and personal data management.

1. SCOPE OF APPLICATION

This policy applies to:
- All investment, capital management, consulting, and market analysis services we provide.
- Our websites, mobile applications, physical offices, and communication channels.
- The personal and financial data of clients, employees, suppliers, and prospects.

It is not limited only to active clients: it also covers former clients, potential investors, and individuals who interact with Capital Bridge in any way.

2. INFORMATION WE COLLECT

2.1 Personal Identification Data
- Full name, date and place of birth, nationality, gender.
- Official identity documents: passport, national ID, driver's license.
- Signature and, in advanced verification processes, biometric data (fingerprints, facial recognition, voice).

2.2 Contact Data
- Physical residential and mailing address.
- Landline and mobile phone numbers.
- Corporate and personal email addresses.

2.3 Financial and Banking Data
- Bank account, custody, and digital wallet information.
- Investment history, transactions, and trading operations.
- Payment and deposit information, encrypted under PCI DSS standards.

2.4 Technical and Access Data
- IP address, browser type and version, operating system, unique device identifier.
- Geolocation data (when permitted by the user).
- Activity logs on our platforms, including date, time, and actions performed.

2.5 Regulatory Compliance Data
- Information collected through **KYC** (Know Your Customer) and **AML/CFT** (Anti-Money Laundering / Combating the Financing of Terrorism) procedures.
- Declarations of ultimate beneficial ownership.
- Tax certificates and documentation for anti-tax evasion measures.

2.6 Communications Data
- Recorded phone calls for quality control and contractual evidence.
- Live chat records, emails, and support tickets.

3. PURPOSES OF DATA PROCESSING

At Capital Bridge, we process your information to:
1. **Provide financial services:** account opening and management, execution of investment orders, portfolio monitoring, report generation, and market analysis.
2. **Regulatory compliance:** reporting to supervisory authorities, implementation of AML/CFT measures.
3. **Risk management:** detection of unusual transactions, analysis of transaction patterns, and preventive blocking of suspicious activity.
4. **User experience optimization:** interface customization, recommendations based on risk profile, access to advanced analysis tools.
5. **Communications:** sending notifications on transactions, account statements, regulatory alerts, financial newsletters, and investment opportunities.
6. **Research and development:** analysis of client behavior, market studies, and testing of new products.

4. LEGAL BASIS FOR DATA PROCESSING

Processing of personal data by Capital Bridge is based on:
- The data subject's explicit consent.
- Compliance with legal and regulatory obligations.
- Execution of a contract or pre-contractual relationship with the data subject.
- Capital Bridge's legitimate interest in preventing fraud and optimizing services.

5. DATA SHARING AND TRANSFERS

5.1 Principles
- We do not sell, rent, or trade your personal data.
- All transfers are carried out under strict confidentiality and security agreements.

5.2 Possible Recipients
- Technology and financial service providers.
- Banking institutions and asset custodians.
- Audit firms and regulatory consultants.
- Competent national or foreign authorities in compliance with the law.

5.3 International Transfers
If your data is transferred to countries outside your jurisdiction, we ensure compliance with equivalent protection mechanisms, such as **EU Standard Contractual Clauses** or approved privacy frameworks.

6. INFORMATION SECURITY

Capital Bridge applies a **Comprehensive Information Security System** including:

- **AES-256 encryption** for data at rest and **TLS 1.3** for data in transit.
- Next-generation firewalls, traffic filtering, and IDS/IPS systems.
- **Multi-factor authentication (MFA)** for clients and staff.
- Access control based on the **"least privilege" principle**.
- **24/7 monitoring** by a Security Operations Center (SOC).
- Data centers with **ISO 27001, SOC 1, and SOC 2** certifications.

7. FRAUD PREVENTION AND COMPLIANCE

- Enhanced KYC procedures for all clients.
- Continuous monitoring of transactions to detect unusual activity.
- Reporting of suspicious operations to competent authorities.
- Regular internal and external audits in security and compliance matters.

8. DATA RETENTION AND DELETION

We retain information for the time necessary to fulfill processing purposes, with minimum retention periods of **5 to 10 years** for financial data as per regulations.
Data is deleted through certified secure erasure and physical destruction of storage media, preventing any recovery.

9. DATA SUBJECT RIGHTS

You can exercise your rights to:

- Access your data.
- Rectify inaccurate information.
- Delete or cancel data.
- Object to processing.
- Restrict processing.
- Transfer data to another provider (portability).

To exercise these rights, you must submit a written request and verify your identity.

10. COOKIES AND SIMILAR TECHNOLOGIES

Capital Bridge uses cookies to:

- Improve navigation.
- Personalize the experience.
- Analyze platform performance.
- Offer targeted advertising.

You may disable or limit cookies in your browser, although some functions may be affected.

11. LINKS TO EXTERNAL SITES

Our platforms may contain links to third-party sites. Capital Bridge is not responsible for their privacy practices and recommends reviewing their policies before interacting.

12. MINORS

We do not knowingly collect data from individuals under 18 without verifiable parental or guardian consent.

13. POLICY CHANGES

We may modify this policy to adapt to regulatory, technological, or business changes. Updates will be published on our official channels with the effective date.

ANNEX I – Relevant GDPR Articles

This policy specifically aligns with the following provisions of **Regulation (EU) 2016/679 (GDPR):**

1. **Art. 5 – Principles of Processing**
   - Lawfulness, fairness, transparency.
   - Purpose limitation.
   - Data minimization.
   - Accuracy.
   - Storage limitation.
   - Integrity and confidentiality.
2. **Art. 6 – Lawfulness of Processing**
   - Consent.
   - Contract performance.
   - Legal obligations.
   - Legitimate interests.
3. **Art. 7 – Conditions for Consent**
   - Free, informed, and verifiable consent.
4. **Art. 12–14 – Transparency and Communication**
   - Clear information on data use.
   - Time limits for providing information.
5. **Art. 15–22 – Data Subject Rights**
   - Right of access, rectification, erasure, restriction, portability, and objection.
6. **Art. 24–32 – Accountability and Security**
   - Appropriate technical and organizational measures.
   - Risk management.
   - Encryption and pseudonymization.
7. **Art. 33–34 – Data Breach Notification**
   - Report to supervisory authority within 72 hours.
   - Notify data subjects when necessary.
8. **Art. 44–50 – International Transfers**
   - Adequate safeguards for data leaving the EEA.

ANNEX II – Internal Procedures and Data Breach Response Protocols

1. Information Classification

- **Level 1:** Public information (marketing materials, non-confidential corporate info).
- **Level 2:** Internal information (operational procedures, internal manuals).
- **Level 3:** Confidential information (personal data of clients/investors).
- **Level 4:** Critical information (sensitive financial data, access credentials, AML/KYC records).

2. Preventive Controls

- Reinforced authentication: two-factor access to all internal systems.
- End-to-end encryption: AES-256 for storage, TLS 1.3 for transmission.
- 24/7 monitoring: automatic intrusion detection and anomaly detection.
- Network segmentation: separation of critical and public environments.

3. Incident Response Protocol

Phase 1 – Detection:

- Continuous monitoring through **SIEM** (Security Information and Event Management) systems.
- Automatic alerts for unauthorized activity.

Phase 2 – Containment:

- Immediate blocking of suspicious access.
- Isolation of affected systems.

Phase 3 – Assessment:

- Digital forensics analysis to determine scope and origin.
- Identification of compromised data.

Phase 4 – Notification:

- Report to Data Protection Authority within 72 hours (**Art. 33 GDPR**).
- Notify affected data subjects if there is a risk to their rights and freedoms (**Art. 34 GDPR**).

Phase 5 – Recovery:

- Restoration of systems from verified backups.
- Implementation of preventive improvements.

Phase 6 – Documentation and Audit:

- Detailed recording of the incident, measures taken, and response times.
- Annual protocol review for continuous improvement.

4. Audits and Training

- Semi-annual internal audits on security and privacy compliance.
- Mandatory annual staff training on data protection and cybersecurity.
- Incident response drills to measure reaction times.