

Sustainability
**Support ESG
Information
2025**



GLOBAL
BANK

Primer la gente



Primero la gente

Content

1. Human Rights and Labor Practices Commitment
2. Workforce Trade Union and Collective Bargaining
3. Statement of non-political contributions
4. Revenue distribution
5. Investment Portfolio
6. Information Security Policy
7. SARAS – Environmental and Social Issues
8. Integral Risk Management Policy – Extract
9. Occupational Health and Safety (OHS)
10. Privacy and Data Protection Policy for the Global Bank Group

Human Rights and Labor Practices Commitment

Global Bank is committed to respecting and promoting human rights and responsible labor practices in accordance with applicable labor legislation, internationally recognized human rights standards, the Universal Declaration of Human Rights, and the Fundamental Conventions of the International Labour Organization (ILO). We uphold the principles of freedom of association, collective bargaining, non-discrimination, equal opportunity, and the elimination of forced labor and child labor.

We are committed to providing a safe, inclusive, respectful, and healthy workplace where employment decisions are based on objective criteria, competencies, performance, and merit. We comply with applicable labor laws and regulations regarding working hours, remuneration, overtime compensation, paid annual leave, vacations, maternity and paternity protections, occupational health and safety, and other employment-related rights. Through our Internal Labor Regulations, we have established limits on working hours, mandatory rest periods, weekly rest days, and mechanisms designed to safeguard employee well-being and prevent excessive working hours, in alignment with the Panamanian Labor Code. We also promote employee well-being, professional development, equal access to opportunities, and social protection through benefits and programs that contribute to the welfare of employees and their families.

We maintain zero tolerance for discrimination, harassment, racism, sexism, retaliation, and any conduct that undermines the dignity, well-being, or rights of individuals. We further seek to promote respect for human rights and responsible business conduct in our relationships with suppliers, business partners, clients, and other stakeholders across our value chain.

Reference:

- [Code of Ethics and Conduct of Grupo Financiero G.B. Group Corporation](#), pages 4-5, 15-17.
- [Política de Igualdad y equidad de Género V.1.0](#) – Sections 5.1, 5.2, 5.6 and 5.7 covering equal opportunity, non-discrimination, human rights, inclusive workplace practices, responsible value chain management, and training.
- **Reglamento Interno de Trabajo** – Articles 15-31 (working hours, overtime, rest periods, weekly rest days and paid annual leave), Articles 35-36 (paid leave and benefits), Articles 59-76 (occupational health and safety), Articles 84-86 (employer obligations and worker protections), and Articles 99-103 (anti-discrimination, anti-harassment, anti-racism and anti-sexism provisions).
- [2024-2025 Sustainability Report](#) – Pages 158-160 (training, capacity building and employee development) and pages 167-168 (compensation, gender pay equity, benefits, social protection, well-being, and parental leave).



Workforce Trade Union and Collective Bargaining

Details	2021-2022	2022-2023	2023-2024	2024-2025
Percentage of employees represented by an independent trade union or covered by collective bargaining agreements	0%	0%	0%	0%



Statement of non-political contributions

Political contributions

Global Bank does not make contributions to political parties and/or political representatives.

Global Bank employees are free to make political contributions, as long as it is in a personal capacity and is not directly or indirectly related to the organization.

Political contribution is the delivery of money, goods, services, rights or any other resource, to political parties, organizations and/or associations of a political nature, as well as to candidates to occupy any position of popular election.



Revenue distribution

		2022-2023	2023-2024	2024-2025
Investing & Stewardship				
1	Asset Management & Custody Activities	1.10%	1.82%	1.32%
Financing				
1	Commercial Banking (corporate) and Investment Banking	45.62%	46.08%	44.86%
2	Commercial Banking (consumer)	41.91%	40.49%	41.08%
3	Project finance			
Advisory				
1	Investment Banking & Brokerage	8.66%	8.85%	10.19%
Insurance Underwriting				
1	Insurance (non-life / non-health)	2.71%	2.76%	2.55%
Investing				
1	Investment Holdings/Multi-sector Holdings	0%	0%	0%
Other				
1	Stock exchanges	0%	0%	0%
2	Index licensing	0%	0%	0%
3	Financial Data & Analytics	0%	0%	0%



Investment Portfolio

Investment Portfolio* by carbon-intensive industry

Industry	% de participación
Coal	0.0%
Oil and gas	2.7%

*Investment portfolio as of Jun-2025



Cover of the
Information
Security
Policy



POLÍTICA DE SEGURIDAD DE
INFORMACIÓN

Versión 1.4

Octubre 2025

Revisiones

VERSION	FECHA	CREADO POR	APROBADO POR	COMENTARIOS
1.0	Agosto 2019	Alejandro González	Borrador	Creación
1.1	Octubre 2019	Alejandro González	Ver memorándum de aprobación	Aprobación
1.2	Octubre 2021	Alejandro González	Ver memorándum de aprobación	Revisión bianual (agregar regulaciones y agregar temas de Privacidad de Datos, cambio de Comité Operativo por Comité de Procesos en las aprobaciones)
1.3	Octubre 2023	Gestión de Información	Ver memorándum de aprobación	Revisión bianual (cambio en el proceso de actualización, actualizar regulaciones aplicables, nuevas tecnologías, apetito al Riesgo)
1.4	Octubre 2025	Gestión de Seguridad de Información	Ver aprobaciones de Comités	Revisión bianual Cambio de logo Adición de regulación de la SSPR para Protección de Datos



TABLA DE CONTENIDO

1.0 INTRODUCCIÓN 4

1.1. Propósito..... 4

1.2. Alcance 4

1.3. Cumplimiento 5

1.4. Actualización de Política de Seguridad de Información 6

1.5. Políticas y procedimientos relacionados de El Grupo..... 6

1.6. Regulaciones relacionadas 7

1.7. Estándares internacionales relacionados 7

2.0: DECLARACIONES Y PRINCIPIOS DE LA POLÍTICA..... 8

2.1. Declaraciones de la Política..... 8

2.2. Principios de seguridad de la información 8

2.2.1.Responsabilidad individual 8

2.2.2.Responsabilidad de la unidad de negocios 8

2.3. Tres líneas de defensa 12

2.4. Plan de comunicación de la Política 12

Anexo A: Glosario 12

Information Security Policy

This policy includes, among other things:

- ✓ 2.1. Policy Statements The Group will employ reasonable means to ensure the confidentiality of information under its custody, guarantee its integrity and non-repudiation, and ensure the availability and continuity of application systems and technological infrastructure. These objectives must be achieved at a cost commensurate with business risks and in a manner consistent with both the need for reliable information and the need to provide an appropriate level of service through various channels—continuously meeting or exceeding business and customer expectations—while complying with legal, regulatory, or contractual requirements.
- ✓ 2.2. Information security principles.
 - 2.2.1. Individual responsibility: All employees, temporary staff, supervisors, and directors are responsible for protecting information—whether proprietary information or information entrusted to the Group by clients, suppliers, or other business partners—by complying with this Information Security Policy and any policy, rule, standard, or process/procedure relevant to their roles. Individuals must exercise the care, diligence, and skill expected of a reasonably prudent person when handling sensitive information and must report any concerns regarding suspicious security-related events to the appropriate superior through the chain of command (refer to the Information Security Governance Framework for detailed responsibilities).
 - 2.2.2. Business Unit Responsibility (extract)
 - - Third-party risk management: External providers—including companies contracted for workforce augmentation and any subcontractors—must be required, via contract or agreement, to implement and continuously enforce Information Security procedures and practices, and to comply with the requirements of this Information Security Policy...
 - - Data protection...
 - - Awareness and training...
 - - Assessment and improvement...
 - - Risk appetite
 - - Maintenance of information technology assets
 - - Incident management.
 - - Others,



SARAS - ENVIRONMENTAL AND SOCIAL ISSUES

DESCRIPCIÓN DEL PROCESO



SISTEMA DE ADMINISTRACIÓN DE RIESGOS AMBIENTALES Y SOCIALES (SARAS)



Fecha: 11 de septiembre de 2026

Versión: 10.0

In general, without this meaning that it is limited to these aspects; environmental factors and social problems to be identified, managed and mitigated are the following:

Environmental	Social	Governance
Water management (including wastewater)	Local communities (including health and safety)	Licenses, certifications, permits
Energy management	Indigenous peoples	Policies related to: Environmental and social management, human resources, community management.
Input and hazardous material management	Involuntary resettlement	Legal and regulatory compliance (environmental and social)
Waste and pollution management	Landscape Impacts	Structure - Person responsible for socio-environmental management
Animal health	Cultural Heritage	Business ethics and transparency (environmental and social)
Biodiversity, forests, protected and high conservation value areas and % of deforestation	Labor	
Natural hazards	Labor conditions	
Atmospheric emissions and air quality	Occupational health and safety	

Material Topic (Extract). Among the material topics, not limited to these, are:

- Moderate to High Risks or negative impacts on the environment, community health and safety, biodiversity, cultural heritage and involuntary resettlement.
- Child and forced labor, as well as aspects that cover gender discrimination, equal opportunities, health and safety and the risk of gender violence and sexual harassment, etc.
- Problems related to working conditions, such as lack of drinking water supply in plantations/workplaces.



12. Integral Risk Matrix

The comprehensive risk matrix covers the main risk categories in which the Banking Group has its most significant exposures.

All risks must be catalogued in the integral risk matrix according to the risks defined as main risks, for their respective management and control.

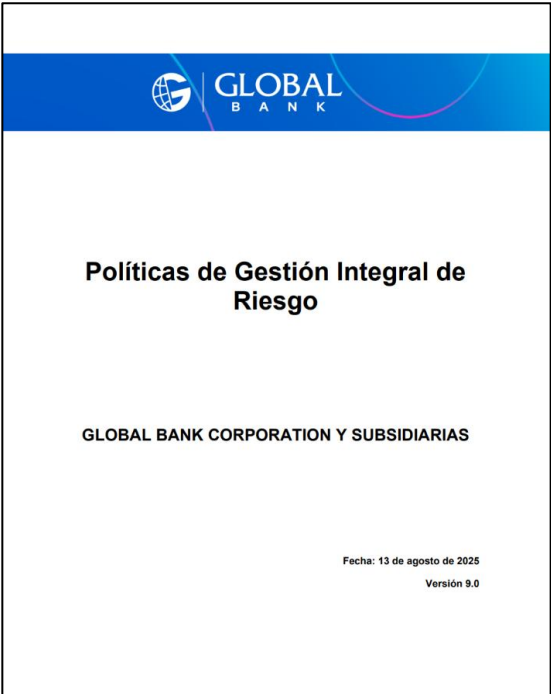
Risks are grouped into four (4) categories as follows: Business Risks, Financial Risks, Operational Risks and Compliance Risks.

Página 10 de 30

Aprobado por: Comité Directivo de Riesgo
Ratificado por: Junta Directiva
Unidad de Administración de Riesgo

02 de agosto de 2023
23 de agosto de 2023
Versión: 7.0

Cover of the
Integral Risk
Management
Policy



Integrated Risk Management Policies

At its first level, the comprehensive risk matrix includes the following risks:

Business Risks:

- **Strategic Risk:** Defined as the possibility of incurring losses due to decisions of the Banking Group's senior authorities associated with the creation of sustainable competitive advantages. It is related to failures or weaknesses in market analysis, trends and uncertainties in the environment, key competencies of the Banking Group and in the process of value generation and innovation.
- **Contagion Risk:** Possibility of loss that the Banking Group may suffer directly or indirectly due to adverse occurrences in companies of its own economic group, or of companies that carry out similar activities in its location or in the financial system of another country.
- **Climate Related Risk:** The actual or potential negative impacts that may arise from climate change or efforts to mitigate climate change. These impacts include economic and financial consequences on an entity or organization. These risks can be classified into physical, transitional and liability risks.
 - **Physical Risks:** These are risks arising from potential losses caused by the occurrence of extreme weather events or by gradual and long-term changes in weather patterns. Physical risks can be acute or chronic.
 - **Transition Risks:** These are those associated with the transition to a low-carbon economy, which may generate political, technological and market changes to address climate change-related mitigation and adaptation measures. Depending on the nature, speed and focus of these changes, transition risks may entail risks of different levels for organizations.
 - **Climate-Related Legal Liability Risks:** These are those arising from potential losses that may be generated by actions or omissions that cause losses or damages associated with climate change and that through legal proceedings seek compensation by repairing the damage caused, implementing prevention and mitigation measures, and assuming the corresponding costs.



Integral Risk Management Policy - Extract

Table 1. Communications Plan by Risk Type to the Risk Steering Committee

Tabla 1. Plan de Comunicaciones por Tipo de Riesgo a Comité Directivo de Riesgo	
Tipo de Riesgo	Periodicidad de Comunicación
Riesgos de Negocios	
• Riesgo Estratégico	Anual
• Riesgo de Contagio	Anual
• Riesgo Relacionado con el Clima	Anual
Riesgos Financieros	
• Riesgo de Capital	Trimestral
• Riesgo de Crédito	Trimestral
• Riesgo de Contraparte	Trimestral
• Riesgo de Liquidez	Trimestral
• Riesgo de Precio	Trimestral
• Riesgo de Tasa de Interés	Trimestral
• Riesgo de Tipo de Cambio	Anual
• Riesgo País	Trimestral
• Riesgo de Concentración	Trimestral
Riesgos Operativos	
• Riesgo Operativo	Trimestral
• Riesgo de Tecnología de la Información	Trimestral
Riesgos de Cumplimiento	
• Riesgo de Reputación	Anual
• Riesgo Legal	Trimestral
• Riesgo Normativo	Anual
• Riesgo de Blanqueo de Capitales, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva	Semestral
• Riesgo Social y Ambiental	Semestral
• Riesgo de Protección de Datos	Semestral

Página 22 de 30

Aprobado por: Comité Directivo de Riesgo
Ratificado por: Junta Directiva
Unidad de Administración de Riesgo

02 de agosto de 2023
23 de agosto de 2023
Versión: 7.0

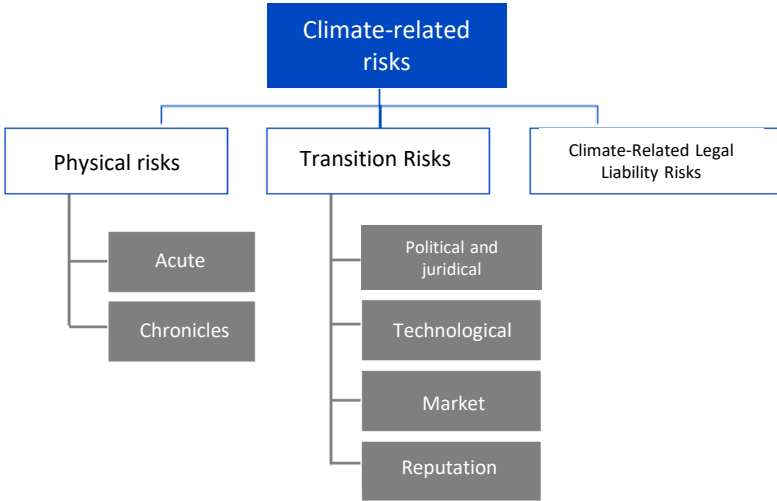
Depending on the type of risk, these have a communication periodicity (quarterly, half-yearly and annual).

It is important to mention that within the business risks there are Climate Related Risks, which have their own taxonomy, aligned with Agreement No. 011-2022 of the Superintendency of Banks of Panama “Which adds paragraph 13 to article 4 of Agreement No. 8-2010, on Comprehensive Risk Management”

Annexes - 1. Comprehensive Risk Matrix

Anexos	
1. Matriz Integral de Riesgo	
ENFOQUE INTERNO	
14	MATRIZ INTEGRAL DE RIESGO [20]
Riesgos de Negocios [3]: • Riesgo Estratégico • Riesgo de Contagio • Riesgo Relacionado con el Clima	Riesgos Operativos [2]: • Riesgo Operativo • Operaciones de Seguros • Riesgo de Tecnología de la Información • Ciberriesgos
Riesgos Financieros [9]: • Riesgo de Capital • Riesgo de Crédito • Riesgo de Contraparte • Riesgo de Liquidez • Riesgo de Precio • Riesgo de Tasa de Interés • Riesgo de Tipo de Cambio • Riesgo País • Riesgo de Concentración	Riesgos de Cumplimiento [6]: • Riesgo de Reputación • Riesgo Legal • Riesgo Normativo • Riesgo de Blanqueo de Capitales, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva • Riesgo Social y Ambiental • Riesgo de Protección de Datos Personales

Taxonomy of Climate Risks





MANUAL DE PROCESO



MANUAL DE PREVENCIÓN DE RIESGOS LABORALES



Fecha: 13 de junio de 2025

Versión: 2.0

Occupational Risk Prevention Manual

Page 7: General Principles and Controls for Chemical Handling and Storage.

Page 8: General Principles and Controls for Updating the Legal Framework.

Page 9: General Principles and Controls for Personnel Using Headsets.

Page 10: General Principles and Controls for Emergency Signage.

Page 11: General Principles and Controls for Irregular Situations Within the Facilities. Page 12: General Principles and Controls for OHS Training.

Page 13: General Principles and Controls for Housekeeping | Fire Prevention.

Page 14: General Principles and Controls for Fire Prevention.

Page 15: General Principles and Controls for Ladder Use.

Pages 16-17: General Principles and Controls for Hot Work.

Page 18: General Principles and Controls for Work at Heights and Confined Spaces.

Pages 19-24: Occupational Risk Identification Process.

Pages 25-29: Process for Handling Accidents and Occupational Illnesses.

Pages 30-33: Process for Maintaining Permissible Risk Levels.

Pages 34-38: Worker Health Surveillance Process.

Pages 39-41: First Aid Kit Management Process.

Pages 42-44: Personal Protective Equipment Selection and Use Process.

Pages 45-52: Vehicle Accident Management Process.

Pages 53-56: Force Majeure/Major Unforeseen Event Management Process.

Pages 57-61: Fire Detection, Control, and Suppression System Maintenance Process.

Pages 62-66: Safe Work Analysis Process.

GUÍA DE USUARIO



PLANES DE EMERGENCIA



Fecha: 26 de mayo de 2023

Versión: 1.0

Document: User Guide - Emergency Plans

- ✓ Page 3: How to carry out an egression in general and How to combat a fire outbreak
- ✓ Page 4: How to act in the event of a public demonstration
- ✓ Page 5: How to act when starting a seismic movement. How to proceed in case of natural disaster alerts
- ✓ Page 6: How to proceed in case of a Bomb Threat call
- ✓ Page 7: How to proceed if you receive suspicious mail or find an abandoned suspicious object
- ✓ Page 8: How to proceed in the event of a flood outside of working hours
- ✓ Page 9: How to proceed in the event of a flood during working hours
- ✓ Page 10: How to act in case of a medical emergency. What to do if you move to hard-to-reach areas
- ✓ Page 11: How to complete the Post – Emergency report
- ✓ Page 12: How to use the Automatic External Defibrillator



Goals

Occupational Health and Safety (OHS)

TYPE OF OBJECTIVE	DESCRIPTION	
Strategic Objectives	1	Guarantee and protect the health of employees by promoting a culture of occupational risk prevention at the organizational level in coordination with the different functional units, ensuring the implementation of the measures, plans and programs required to mitigate or reduce occupational risks arising from work processes.
Operational Objectives	2	Training and advice on occupational risk prevention issues.
	3	Ensure that new and remodeling projects comply with standards related to the Human Safety Code, indoor air quality standards, ergonomics and occupational hygiene, and NFPA.
	4	Ensure the implementation of emergency plans in all locations of the organization.
	5	Participate as risk manager for the organization's contingency plan.
	6	Manage the budget allocated to the department.
	7	Investigate and analyze work accidents, occupational diseases, vehicular accidents and post-emergency incidents.
	8	Follow up on prevention plans and programs in conjunction with area managers.
	9	Supervise, follow up and support the SISO team in the management of occupational risk prevention programs.
	10	Ensure the proper functioning of fire detection and firefighting systems.
	11	Develop, keep updated and ensure the implementation of programs focused on mitigating occupational risks detected in conjunction with the area managers.
Information Objectives	12	Maintain the operational risk database up to date.
	13	CSS Accident Reports
Compliance Objectives	14	Comply with the norms established by the Ministry of Health, Social Security Fund and Fire Department.
	15	Keep updated the legal framework that applies to the operation.



Privacy and Data Protection Policy for the Global Bank Group



Política de Privacidad y Protección de Datos para el Grupo Global Bank



Fecha: agosto 2025

Versión: 3

Propiedad de Global Bank

Privacy and Data Protection Policy

Page 3: Scope

The principles and provisions contained in these policies apply to:

- All Group personnel (temporary or permanent) who, within the scope of their responsibilities, safeguard, process, or have access to personal data—whether belonging to employees, clients, prospective clients, or suppliers.
- Contractors and external parties providing outsourcing services to the Group—under any contractual arrangement—who capture, process, or store personal data of employees, clients, prospective clients, and suppliers.
- Any Group database containing confidential, personal, or sensitive information regarding our clients, employees, and suppliers that is safeguarded by the Bank, whether acting as the data controller or the data processor.

Pages 5-7: Privacy and Personal Data Protection Governance. This section describes the roles and responsibilities within the Personal Data Protection Governance Model, illustrating both top-down and bottom-up communication. It includes: Board of Directors and General Management, Risk Management, Internal Audit, Privacy and Data Protection Manager, Technology, Information Security, Marketing, Human Resources, and Customer Service.

Pages 7-11: Privacy and Personal Data Protection Policy Statements and Principles. This section includes: General guidelines for Group employees; guidelines for clients to exercise their rights; non-compliance with this policy; data storage; data usage; data accuracy; client requests; data disclosure for other reasons; provision of information; and communication and management of personal data security incidents.



23. USE OF ARTIFICIAL INTELLIGENCE (Pages 54 and 55)

		NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
Versión	1.7	Cliente	Seguridad de la Información	Aprobación	Enero 2012
		Página	4 de 146		
21.SOFTWARE AUTORIZADO				51	
22.LDAPS (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL – SECURE).....				52	
23.USO DE INTELIGENCIA ARTIFICIAL.....				54	
ESTÁNDARES DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD				56	

**Normas y
Estándares de
Seguridad de la
Información y
Ciberseguridad**



Versión: 1.7

The purpose of this policy is to establish guidelines and restrictions for the use of artificial intelligence (AI) technology within the Bank, with the aim of protecting information security, ensuring data privacy, and mitigating risks associated with the uncontrolled use of AI.

Includes:

- 1. General Requirements for AI Use:** Requires prior approval, compliance with applicable regulations, and risk assessment before implementing AI solutions.
- 2. Restrictions on AI Use:** It establishes clear limits on the use of AI, prohibits autonomous decisions without human oversight, and restricts the processing of sensitive information in uncontrolled environments.
- 3. Privacy and Data Protection:** Includes prior authorization, anonymization or pseudonymization, encryption, and access controls.
- 4. Auditing and Monitoring:** Traceability, auditable records, continuous monitoring, and periodic reviews
- 5. Training and Awareness**
- 6. Justification for Restrictions:** Identify risks associated with AI, including cybersecurity, privacy, algorithmic bias, transparency, accountability, automated decision-making, and regulatory compliance.





Primero la gente