

INTEGRATED POLICY

At **Panama Digital Gateway** we are committed to excellence, security and continuity in the provision of **colocation** services in our Data Center in Panama, guaranteeing the **high availability, continuity, quality and security** of the infrastructure that supports our customers' information.

To fulfill this commitment:

- We maintain a highly available infrastructure, with technical and organizational controls that guarantee the confidentiality, integrity and availability of information and the continuity of services.
- We comply with applicable legal, regulatory, contractual and normative requirements, as well as with the commitments made to our customers, ensuring traceability, reliability and compliance with service level agreements (SLAs).
- We promote a culture of quality and information security, ensuring that all our staff have safe working conditions, clearly defined roles and continuous training.
- We drive continuous improvement of our processes, services and controls, identifying and managing risks and opportunities that strengthen the sustainability of our business and stakeholder trust.
- We take advantage of Panama's strategic position as a digital hub, generating technological alliances and promoting innovation and digital transformation for the benefit of our clients and society.

In line with this policy, Panama Digital Gateway establishes quality and information security objectives that guide our actions towards continuous improvement, compliance with the commitments made and the generation of trust in our customers and stakeholders. These objectives constitute the practical guide to measure, evaluate and strengthen our organizational performance.

QUALITY OBJECTIVES

- Guarantee the availability of colocation services to ensure the operational continuity of customers, through 24/7 monitoring of critical infrastructure and the planned execution of preventive maintenance.
- Achieve a level of customer satisfaction equal to or greater than 90% to strengthen trust in PDG, through annual surveys, analysis of results and derived improvement plans.
- Resolve support tickets in a timely manner to meet service level agreements (SLAs), through efficient help desk management and response time tracking.
- Implement at least three continuous improvement initiatives each year to increase the efficiency and quality of services, by identifying opportunities and executing documented optimization projects.

INFORMATION SECURITY OBJECTIVES

- Protect the confidentiality, integrity and availability of information to safeguard critical customer and PDG assets, through the application of technical, physical and organizational controls aligned with ISO/IEC 27001.
- Effectively manage security incidents to reduce the impact on operations and maintain customer trust, by detecting, logging and responding within a maximum time of 24 hours.
- Comply with 100% of applicable legal, regulatory and contractual requirements to avoid sanctions and reputational risks, through the periodic updating of the legal matrix and compliance verification in internal audits.
- Foster a culture of information security across staff to minimize human risks, through annual training and induction programs that include access procedures, floor rules, and colocation standards.