

ICT MANAGEMENT
Cybersecurity 2025

UENAVENTURA

Mineros peruanos trabajando por el país

Information Security Management

At Buenaventura, we manage cybersecurity as an integral part of our risk management system, with the aim of protecting the confidentiality, integrity and availability of information, while ensuring the continuity of our operations.

Key documents for ICT management

General Information Security Policy

Business Continuity Policy

Malware Protection Standard

Information Security Incident Management Standard

General Cyber Incident Response Plan

2025 Highlights



0 significant cybersecurity incidents or breaches



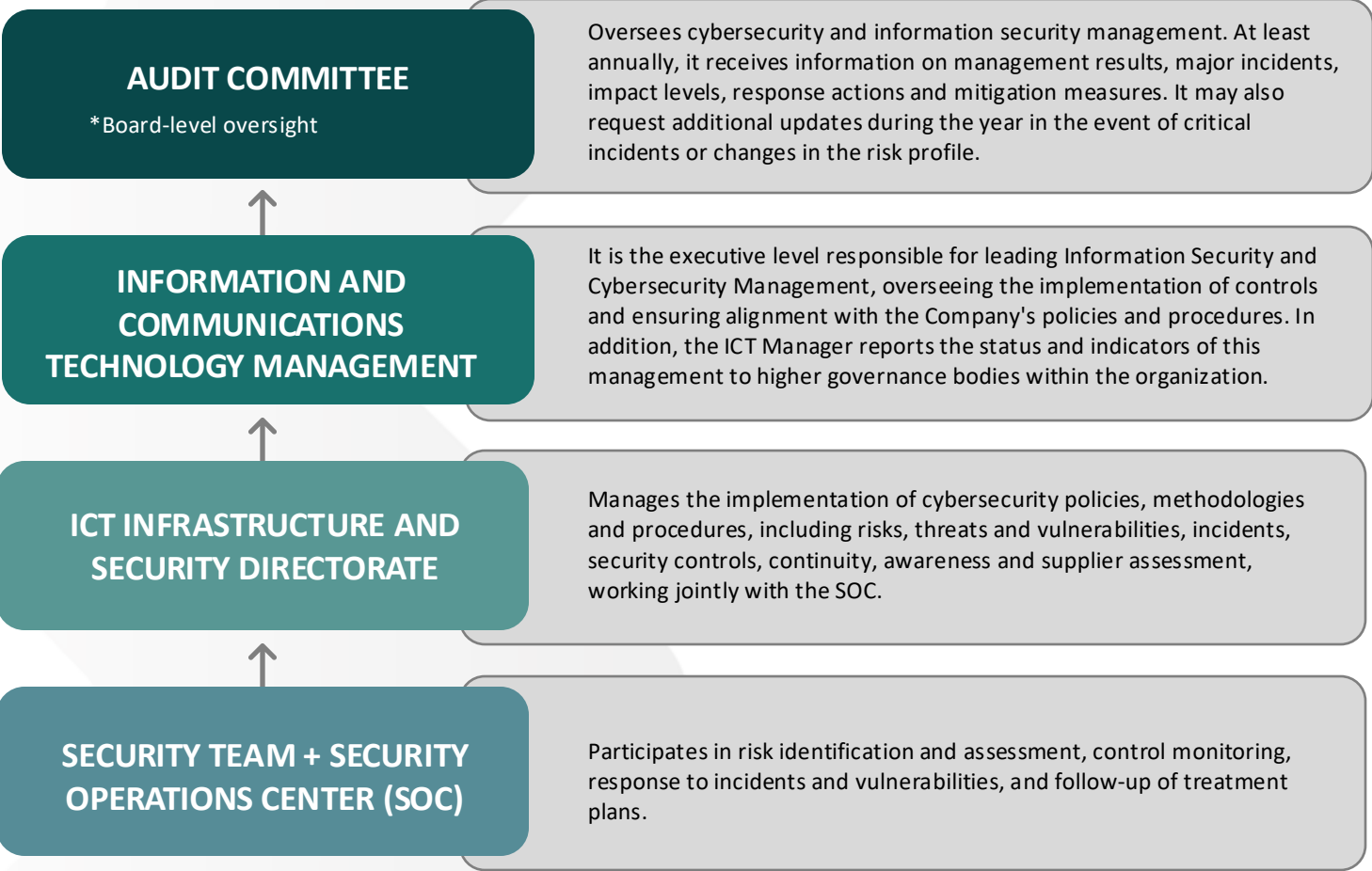
5 audits conducted on information security matters



Implementation of the information security training program

1. Cybersecurity Governance

We have an oversight and leadership structure to manage cybersecurity risks and incidents.



Reference

- M-COR-TI-01-01: ORGANIZATION AND FUNCTIONS MANUAL (MOF) – Version 07, May 2026
- Presentation to the Audit Committee: Cybersecurity Management and Incidents 2025

2. Information Security Policy

The General Information Security Policy establishes the framework for protecting Buenaventura's information and managing associated risks, defining controls and responsibilities applicable to employees and third parties.

CONTINUOUS IMPROVEMENT OF THE SYSTEM

The Policy and its supporting documents are periodically reviewed and updated as appropriate. In addition, the GISP requires a review at least annually or upon significant changes to ensure its continued suitability, adequacy and effectiveness.

INFORMATION PROTECTION AND INTEGRITY

Our management aims to preserve the confidentiality, integrity and availability of information. The Policy addresses information classification, masking of sensitive data, access controls, protection against unauthorized disclosure or modification, and security requirements from system development onward.

MONITORING AND RESPONSE TO THREATS

Users must report security events or incidents through established channels. The Information Security area assesses incidents based on their impact and sets priorities for analysis, containment and eradication; high-impact incidents require an immediate response.

SHARED RESPONSIBILITY

The Policy is mandatory for all personnel and suppliers. It establishes responsibilities to protect information, participate in training and comply with security controls, including confidentiality agreements and contractual requirements for third parties.

	POLÍTICA GENERAL DE SEGURIDAD DE INFORMACIÓN P-COR-TI-01.01	VICEPRESIDENCIA DE FINANZAS Y ADMINISTRACIÓN	
		Versión 08	Página 1 de 10

Política General de Seguridad de Información

2026

Actualizado por:	Revisado por:	Revisó:	Aprobado por:
 Michael Aparcana Analista de Aseguramiento de Calidad TIC	 Gustavo Bazalar Director de Infraestructura y Seguridad TIC	 Juan Buhytron Gerente TIC	 Daniel Domínguez Vicepresidente de Finanzas y Administración
Fecha: 30/04/2026	Fecha: 30/04/2026	Fecha: 30/04/2026	Fecha: 30/04/2026

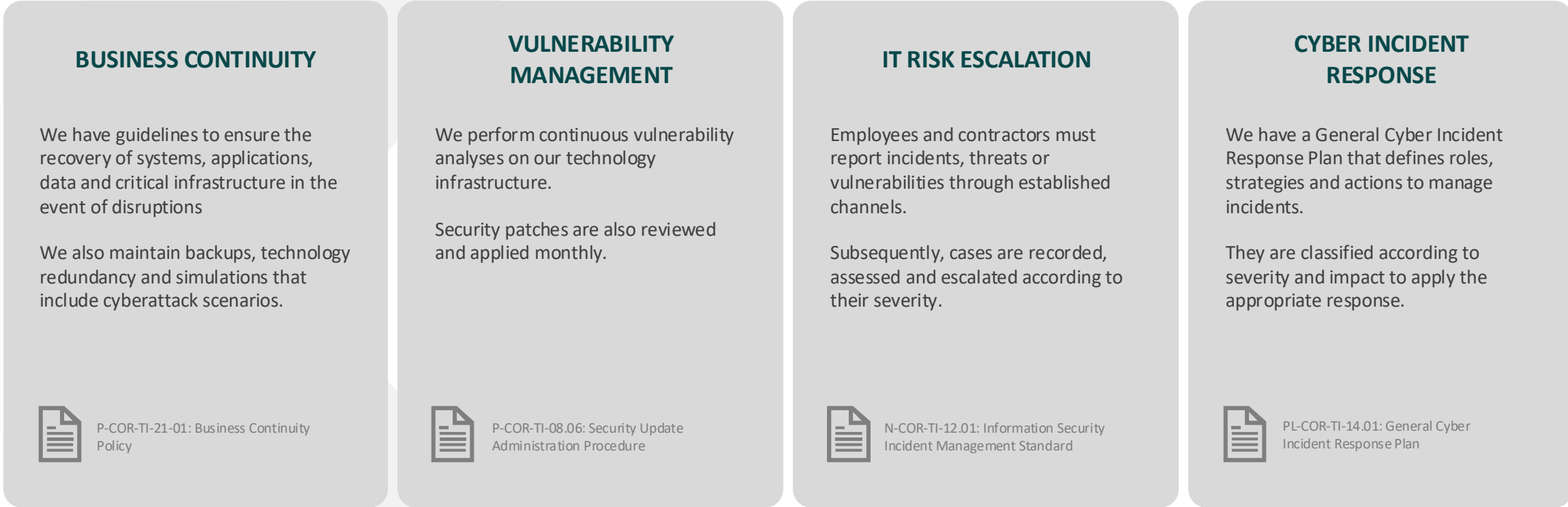
REGISTRO DE CAMBIOS

Fecha	Versión	Referencia de cambios y modificaciones	Autor del cambio
04/06/2024	06	5.37 Grabación de reuniones en Teams	Analista de Aseguramiento de Calidad TIC
13/01/2025	07	5.38 Revisión y actualización de la Política General de Seguridad de la Información (PGSI)	Analista de Aseguramiento de Calidad TIC
29/04/2026	08	5.39–5.41 Incorporación y fortalecimiento de lineamientos para el uso de herramientas de Inteligencia Artificial (IA)	Analista de Aseguramiento de Calidad TIC



3. Information Security Culture

We implement measures to prevent, detect and respond to information security risks and incidents, ensuring the continuity of our operations.



3. Information Security Culture

We implement measures to prevent, detect and respond to information security risks and incidents, ensuring the continuity of our operations.

ICT TRAINING

ICT Management maintains awareness initiatives to strengthen secure behaviors and reduce risks associated with human factors and social engineering.

In 2025, mandatory information security training was provided through the BVN 360 platform.

We disseminate periodic communications and informational capsules on cybersecurity risks and good practices.

AUDIT AND ASSESSMENT

We assess our infrastructure and processes to ensure compliance with controls and continuous improvement.

- **During the period, 5 internal audits on information security matters were conducted.**
- Assessment mechanisms: SOX and LPDP audits, social engineering tests and Ethical Hacking.

These procedures allow us to identify opportunities for improvement and strengthen our controls.

CONTINUOUS IMPROVEMENT

We monitor incidents, anomalies and risks to act promptly and continuously strengthen our defenses.

- Continuous monitoring of security events through our **SOC (CyberSOC)**.
- Incidents are recorded, classified, managed and documented.
- After each incident, lessons learned and corrective actions are implemented to prevent recurrence.

In 2025, we recorded no significant cybersecurity incidents or breaches

4. Responsible Artificial Intelligence Management

At Buenaventura, we are progressively strengthening our governance for the responsible and secure use of Artificial Intelligence, incorporating initial controls into our Information Security framework and advancing the development of specific AI guidelines. Our General Information Security Policy (GISP) already establishes AI guidelines focused mainly on three aspects:

AUTHORIZED USE OF AI

- AI use involving corporate information is carried out exclusively through tools and licenses authorized by ICT.
- Its use must ensure the confidentiality, integrity and availability of information.

PROTECTION OF CORPORATE INFORMATION

- The use of public, open or non-corporate-licensed AI tools to process Buenaventura information is prohibited.
- Corporate information must not be processed or stored outside the Company's control.

RESPONSIBLE USE OF AI

- Authorized users are responsible for the proper use of corporate AI tools.
- Their use must comply with the General Information Security Policy and other internal rules in force.



At Buenaventura, we are designing and implementing our AI governance model and developing specific guidelines focused on responsible use, risk management, information protection, regulatory compliance and oversight of AI-based solutions, with approval and publication planned for December 2026.



Reference

- P-COR-TI-01.01: GENERAL INFORMATION SECURITY POLICY – Version 08, April 2026