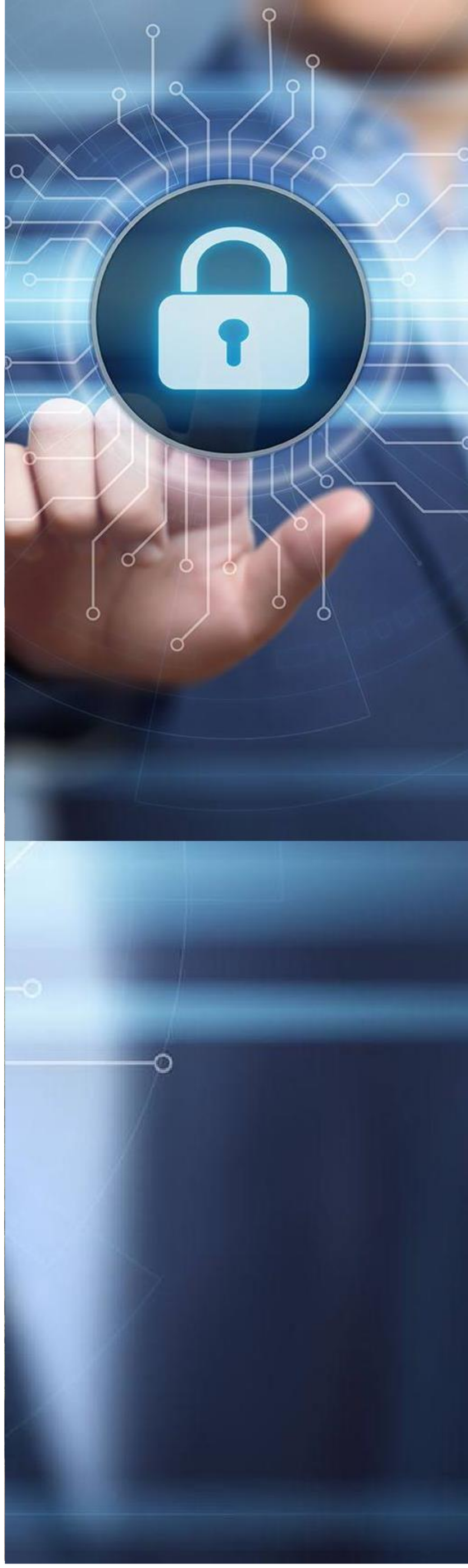
INFORMATION AND CIBERSECURITY POLICY



COLBUN IS A COMPANY THAT ASPIRES TO BE A LEADER IN THE ENERGY INDUSTRY AND OUR PURPOSE IS TO CONTRIBUTE WITH THE BEST ENERGY TO THE FUTURE OF OUR REGION. THUS, INFORMATION SECURITY AND CYBERSECURITY RISK MANAGEMENT ARE IMPORTANT ACTIVITIES WITHIN OUR VALUE CREATION MODEL. THEREFORE, WE ARE COMMITTED TO ENFORCE THE NECESSARY MEASURES TO MITIGATE RISKS ORIGINATED BY THE DIGITAL WORLD WITH WHERE THE COMPANY INTERACTS, RELATED PRIMARILY TO PEOPLE, PHYSICAL ASSETS, FACILITIES, INFORMATION AND OPERATIONAL CONTINUITY.

THIS POLICY IS COMMUNICATED TO ALL EMPLOYEES, CONTRACTORS, DIRECTORS, AND SUBSIDIARIES, THEREFORE, EVERYONE IN THE COMPANY HAS THE RESPONSIBILITY TO APPLY THE PRINCIPLES DESCRIBED BELOW.

1. CULTURE AND AWARENESS

- Conscious of the risks and impacts related to information security and cybersecurity in our activities, at Colbu we strive to build up culture and awareness in the proper use of information, resources and technological platforms through ongoing consciousness-raising and training programs that provide knowledge, skills, experiences and capabilities to all company employees.
- Security of information and cybersecurity is the responsibility of all those who work for the company; this is why everyone must be an active promoter of these areas in the development of their daily activities.

2. MONITORING AND PRACTICE IMPLEMENTATION

All individuals, management and committees that constitute the company's information security and cybersecurity governance model must:

- Enhance identification, protection, detection, response and recovery capabilities under world-class standards, when faced with events and incidents that may compromise information, data, cyber assets, availability of operations, reputational damage, loss of competitive advantage or other negative impact to the company.Informar a las gerencias respectivas y adoptar medidas de recuperación urgentes ante la ocurrencia de infracciones o eventos que atenten contra la seguridad de la información o ciberseguridad.
- Report to the corresponding management and adopt urgent recovery measures in the event of breaches or events that threaten information security or cybersecurity.
- Mitigate risks by applying logical and physical controls, based on the principle of least privilege.
- Agile adaptation to the changing conditions of the technological environment and new threats, through processes, procedures and tools that allow us to respond quickly and innovatively to the needs of the company.
- Comply with requirements established in current legislation, regulatory standards, technical standards, policies and procedures.
- Collaborate with organizations, regulators and relevant industry associations to contribute to the global improvement of information security and cybersecurity.

José Ignacio Escobar T.

Chief Executive Officer - Colbun

- This policy has been approved by the Board of Directors of Colbun on August 30, 2022.
- The members of the company's security and cybersecurity governance model are responsible for managing compliance with the guidelines described herein.