RELATORIO DE SUSTENTABILIDADE 2020

GENTE E INOVAÇÃO
CONFIANÇA NO FUTURO E NO CRESCIMENTO SUSTENTÁVEL

Algar Telecom

Compliance and risk management

Set up in order to comply with Brazilian legislation and pursue anticorruption initiatives in our environment, ***Algar Telecom***'s *Compliance* Program is divided into three fronts: prevention, detection and remediation.

Our executives have a crucial role for the Program: leading by example and showing coherence between discourse and practice, as well as providing irrefutable support for both planning and executing initiatives. In addition, in our organizational structure, *Compliance* has its own budget and reports directly to the vice-executive officer of finance. Monthly reports are submitted to our senior management, Chief Executive Officer, Audit and Risk Committee and officers show measures taken in the period.

There is a normative framework, with a hierarchical structure between documents. At the top of the regulatory chain is ***Algar*** Group's Code of Conduct, which describes all policies to be adopted by the company and how conformity must be maintained. The Code of Conduct guides expected behavior in relationships with different segments or stakeholders and is shared with everyone who joins our company. Every year our employees formally certify that they have been informed of the guidelines, thus ensuring that periodic revisions made to the document do not go unnoticed and that everyone is properly updated. The Code of Conduct addresses topics such as anticorruption measures, digital conduct rules, labor relations and human rights, including non-acceptance of child, forced or slave labor by our company or by our partners.

The Code is followed by Policies, Regulations, Procedures and Work Instructions, which complement and detail everything that has been decided, thus ensuring compliance and execution of the company's processes, while respecting pre-determined principles. The entire normative framework is available through our intranet in a public channel of communication for all employees. There is also a Code of Conduct exclusively for our suppliers, which sets forth behaviors and best practices we expect from them, as well as anticorruption clauses and the need for integrity mechanisms so that they are eligible to provide services for us. All documents are fully compliant with the Anticorruption Law, Bidding Law, Auction Law and the Differentiated Public Procurement Regime Law, among others.

On the prevention side, we also conduct a Compliance Risk Assessment (CRA), mapping Compliance risks and identifying those to which we are exposed in order to mitigate them. This process is extremely important since it affords a comprehensive overview of all our business activities and risks, which is required to ensure the Compliance Program's validity and effectiveness.

The Program's efficacy is not restricted to the organization's internal behavior. Suppliers, business partners, representatives and others must undergo a due diligence process so that we may assess their history in each case before entering into a contractual relationship.

To spread our *Compliance* practices, we offered 2,658 hours of related training in 2020. Likewise, we use our communication channels to address issues such as Brazil's level of corruption and its

perception, diversity and inclusion, compliance policy and rules, our Ombudsman Channel and disciplinary measures for misconduct.

Anyone detecting practices that could involve deviation from the Code of Conduct and/or laws and regulations may report the situation to our Ombudsman, which assesses the complaint's source, status and criticality to investigate and handle any incidents. Confirmed deviations are reported to our Integrity Commission. We guarantee confidentiality and ensure identity is preserved; we will not tolerate any kind of retaliation.

We have a Policy for Managing Consequences that allows for disciplinary measures in cases received by the Ombudsman Channel to be applied fairly and equitably. Remediation of all reports of misconduct is based on this policy and managed through our Integrity Subcommittee.

Commitments

Algar Telecom has partnered Instituto Ethos and adhered to the Business Pact for Integrity and Against Corruption, whose objective is to work for a more honest and ethical market and eradicate any possibility of bribery and corruption. By becoming signatories to the pact, we committed to inform our employees and stakeholders about Brazil's anticorruption legislation to help ensure that it is fully complied with.

In addition, we are committed to banning any form of bribery and working for legality and transparency in all transactions, as an example for sponsorships and donations, also striving for transparency of information and collaboration in investigations, when necessary.

Risk management

Risk management is coordinated by ***Algar Telecom***'s Vice-Executive Officer of Finance, who coordinates this work with the other areas of the Company and under the supervision of the Audit and Risk Management Committee – an advisory body to the Board of Directors. ***Algar Telecom***'s Corporate Risk Management Policy sets forth the general guidelines for this process, which is based on (but is not limited to) the "COSO-ERM – Committee of Sponsoring Organizations of Treadway Commission" model, an internationally recognized standard.

The process comprises the following steps: identifying risk factors (causes); mapping Internal controls, assessing impact and probability of occurrence; defining risk limits and implementing action plans. Internal controls are periodically monitored by the Risk Management and Internal Controls area based on evidence of execution of these controls by the responsible areas, and monthly meetings are held with those responsible for each risk to assess the exposure and status of action plans.

One of the instruments that support the prioritization of risks to be addressed is the Risk Matrix, which provides a comparative view of risks by classification of impact and probability.

Risks are classified into five categories: strategic (digital disruption and innovation), financial (accelerated debt and cash flow etc.), *entity level* (global risks, planning and budgeting, financial statements), operational (information security, service availability, supply chain and logistics, etc.) and compliance (litigation, legal, environmental, public bidding, corruption and bribery, etc.). The main risks include:

DIGITAL DISRUPTION /INNOVATION

We are operating in a dynamic business segment and new technology may disrupt consolidated markets. Changing consumer behavior not only impacts new products we may offer but also alters market dynamics; for example, new collaborative platforms impact public transport and hotels. Alignment with digital transformations tends to introduce innovations. We have an ICT Services Journey area, we are founding partners of Brain, an Institute of Science and Technology inspired by the open innovation model, and we run the Estação project to change our employees' mindsets.

GLOBAL RISKS

This risk arises from external factors, such as the spread of the Covid-19 pandemic, capable of disrupting local and global logistics and supply chains and causing shortages of essential products and services. There is also the risk of technology suppliers such as Huawei being affected by other governments retaliating and intervening in trading conditions, so Huawei may be prevented from marketing their products and services. Our management periodically monitors these risks and takes timely decisions to reduce any impacts on business results.

INFORMATION SECURITY

Some systems in our ecosystem are exposed to cybersecurity risk. To mitigate these risks, we have solutions in place to protect us from intentionally or accidentally contaminated malware and antivirus; structures for detecting anomalies in our internal and external network, cyber-attacks and anomalous traffic; and confidential data access control tools. As per Law 13.709 (General Data Protection Law), we have adjusted our processes and policies and strengthened communication at all levels. We have a system to prevent data leakage in order to meet legal requirements and enhance our cybersecurity environment.

SERVICE AVAILABILITY

Availability of our services depends on technologies, systems, processes and people, so any faults may limit our ability to provide proper services for our customers. To reduce the risk of downtime and unavailability of services, we identify key internal or external factors and prepare action plans. Network element and service availability is continuously monitored by a Network Operations Center using technologies, systems and professionals trained to identify and handle incidents as soon as possible, thus reducing downtime and impacts for customers and our company.