revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

Security and Defense of the Alcântara Launch Center: Insights from Strategic Corporate Security[1]

Segurança e Defesa do Centro de Lançamento de Alcantara: Insights da Segurança Corporativa Estratégica

Raimundo Felipe da Silva Costa
Master in Airspace Sciences (Universidade da Força Aérea). Officer of the Conscript Officers' Corps, Security and Defense Specialty, Brazilian Air Force. mestradosilvacosta@gmail.com. ORCID https://orcid.org/0009-0008-0839-6800

Luciano Vaz-Ferreira
Ph.D. in International Strategic Studies (Universidade Federal do Rio Grande do Sul). Professor at Universidade da Força Aérea and Universidade Federal de Pelotas. lvazferreira@gmail.com. ORCID https://orcid.org/0000-0002-7174-4109

[1] Recebido para Publicação xx/xx/xxxx. Aprovado para Publicação em xx/xx/xxxx.
DOI https://doi.org/10.5281/zenodo.18009408

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

Abstract

The development of Brazil's space sector is essential for technological autonomy and the consolidation of national sovereignty. The Alcântara Launch Center (CLA) stands out as a strategic infrastructure, integrating civil and military functions while requiring high standards of security and defense. Its geostrategic location offers competitive advantages while also presenting protection challenges. This exploratory research, based on literature review and documentary analysis, draws on Strategic Corporate Security (MANDARINI, 2005) to propose guidelines that integrate critical asset management, risk mitigation, and operational continuity, promoting a sustainable model of security and defense for the CLA.

Keywords: Space Industry, Alcântara Launch Center, Brazil, Strategic Corporate Security.

Resumo

O desenvolvimento do setor espacial brasileiro é fundamental para a autonomia tecnológica e soberania nacional. O Centro de Lançamento de Alcântara (CLA) destaca-se como infraestrutura estratégica, integrando funções civis e militares e demandando altos padrões de segurança e defesa. Sua posição geoestratégica proporciona vantagens competitivas, mas impõe desafios de proteção. Esta pesquisa, exploratória, na forma de uma revisão de literatura e análise documental, fundamenta-se na Segurança Corporativa Estratégica (MANDARINI, 2005) para propor diretrizes que integrem gestão de ativos críticos, mitigação de riscos e continuidade operacional, consolidando um modelo sustentável de segurança e defesa do CLA.

Palavras-chave: Indústria Espacial, Centro Espacial de Alcântara, Brasil, Segurança Corporativa Estratégica.

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

Introduction

The development of Brazil's space sector constitutes a central element in the country's pursuit of technological autonomy and the strengthening of national sovereignty. This trajectory extends beyond scientific research, encompassing the creation and operation of infrastructures capable of supporting complex space programs, ensuring control over strategic technologies, and consolidating Brazil's presence in the international launch market.

Alcântara Launch Center ("Centro de Lançamento de Alcântara" CLA) stands out as a key institution within Brazilian space policy. Its operations integrate civil and military dimensions, ensuring the execution of space programs with high standards of efficiency and security. Established in 1983 and subordinated to the Brazilian Air Force Command, the CLA has become the country's main launch facility, simultaneously performing military and commercial functions, which demands stringent criteria for reliability, governance, and protection.

The CLA's geostrategic position near the Equator provides significant competitive advantages, while also presenting complex security and defense challenges due to the sensitivity of its operations and international partnerships. The management of these activities requires a security system capable of balancing sovereignty, confidentiality, and cooperation, in compliance with national regulations and strategic agreements, such as the Technology Safeguards Agreement ("Acordo de Salvaguardas Tecnológicas" – AST) with the United States.

To analyze this reality, the research adopts an exploratory approach based on literature review and documentary analysis, with an emphasis on the norms and directives of the Brazilian Air Force that govern security and defense within its military organizations. The theoretical framework relies on the Strategic Corporate Security model proposed by Mandarini (2005), which views security as a systemic and strategic component of organizational management, oriented toward the protection of critical assets, risk mitigation, and operational continuity. This perspective enables the development of an analytical framework capable of integrating the various aspects of CLA security in a cohesive manner, adaptable to the particularities of the space environment.

The research is organized into three chapters. The first presents the institutional and historical context of the CLA. The second discusses the principles of Strategic Corporate Security and their application to the facility. The third proposes guidelines and measures to enhance security and defense, providing a foundation for the consolidation of a sustainable and strategic model for protecting Brazilian space operations.

The Alcântara Lanch Center

The consolidation of autonomy and national sovereignty in the Brazilian space sector has progressed through the strengthening of strategic infrastructures dedicated to the research, development, and operation of space systems. These systems, organized across the orbital, terrestrial, and link segments (USSF, 2020), enable a wide range of activities in the space environment. In this context, the Alcântara Launch

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

Center (CLA) serves as the primary terrestrial infrastructure of the Brazilian space system, functioning as a central hub for the country's scientific, technological, and operational development in the space domain.

The CLA, established by Decree No. 88,136 on March 1, 1983, is a military organization under the Brazilian Air Force Command. Its mission encompasses the execution and support of aerospace vehicle launches and tracking, as well as conducting tests and experiments of national defense interest. Its creation was directly linked to the Brazilian Complete Space Mission, conceived in 1980, and to the need to overcome operational limitations of the Barreira do Inferno Launch Center in Natal, Brazil, whose urban surroundings constrained operations.

Since its inception, the CLA has become the country's principal launch center, having conducted over five hundred operations and received investments exceeding R$ 1.3 billion from the Brazilian Space Agency ("Agência Espacial Brasileira" – AEB) and the Brazilian Air Force Command. Despite these advances, Brazil continues to pursue full autonomy in orbital launches, maintaining the CLA as a strategically significant facility under continuous development (UFMA, 2020). Future plans include expanding its capabilities as a Space Center to establish it as a regional and international reference in commercial launches (BRASIL, 2022).

The CLA's geostrategic value for Brazil and the international space community is heightened by its privileged location on the Maranhão coast, just 2°18" south of the Equator, which enables propellant savings and allows for the launch of larger payloads or less powerful vehicles (CHOAIRY, 2000; UFMA, 2020; BRASIL, 2022). The site offers a broad range of launch azimuths, initial trajectories over the ocean for enhanced safety, low air traffic density, stable climate, geological stability, low population density, and proximity to the capital, São Luís, facilitating logistics and reducing associated risks and costs. These characteristics make the CLA suitable for various orbital launches, including polar, inclined, and equatorial, consolidating its operational, scientific, and economic relevance.

The CLA's infrastructure is complex and organized into interdependent functional sectors that support every stage of the launch cycle, from preparation to tracking, each with distinct roles and high safety standards. The Preparation and Launch Sector manages the final assembly, integration, and launch of space vehicles, playing a crucial role in mission execution and point-zero operational safety. The Command and Control Sector supervises operations in real time, serving as the operational core that ensures flight safety and success. The Payload Preparation Building hosts testing, integration, and verification of satellites and other payloads, protecting strategic assets and ensuring confidentiality. The airport facilitates the arrival of large payloads and teams, serving as a key logistical hub and supporting the expansion of the center's operational capabilities. Additionally, the CLA maintains administrative and residential facilities in São Luís, a Redundant Telemetry Station in Raposa, and a remote base for launch operations and payload recovery on Ilha de Santana (BRASIL, 2022; BRASIL, 2016).

The CLA has intensified its operational pace, reinforcing its strategic importance and the need for rigorous security standards. In 2020, Brazil signed the Technology Safeguards Agreement (AST) with the United States, which establishes technical norms and procedures to protect U.S. technologies used in launches from the center. The agreement safeguards against unauthorized access to or replication of rockets, satellites, and components, preserving critical U.S. technology (BRASIL, 2019). Given that a significant proportion of global space launches incorporates U.S.-origin components, the AST represents a milestone for the CLA's integration into the international commercial launch market, enhancing its credibility

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

and operational reliability while expanding opportunities for cooperation and investment, all while maintaining Brazilian control and jurisdiction over its territory and operations (ANDRADE et al., 2018).

On March 19, 2023, the South Korean HANBIT-TLV rocket, developed by Innospace, was successfully launched during Operation Astrolábio using Brazilian technology from the inertial navigation system. This marked the first launch by a foreign private company from Alcântara and demonstrated the CLA's capacity to conduct national and international launches with precision. Future orbital launches are scheduled for 2025, carrying cubesats such as Golds-UFSC and Conasat-1 (BRASIL, 2023).

As the primary terrestrial infrastructure of the Brazilian space program, any compromise to the CLA's security would have profound repercussions for national space operations. Such an incident would carry serious strategic consequences, as the center ensures access to space, and it would also incur substantial economic losses, given the high value of its equipment and facilities, technological investments, and Brazil's role in the global space launch market (DURÃO; CEBALLOS, 2011). The ongoing internationalization of its activities further elevates security risks, highlighting the imperative of upholding rigorous operational standards in line with the AST and future international agreements.

This exposure to risk was tragically underscored on August 22, 2003, when the Brazilian Space Program suffered its most severe setback: the VLS-1 V03 Satellite Launch Vehicle exploded on the launch pad, resulting in the deaths of 21 technicians and engineers. The accident, which occurred three days before the scheduled launch, was attributed to premature activation of the first-stage engine, possibly caused by the early triggering of a detonator in the ignition system. The incident revealed significant vulnerabilities in the CLA's risk and safety management, prompting a comprehensive review of operational protocols (BRASIL, 2004).

The CLA is officially recognized as a national critical infrastructure under Decree No. 9,573/2018, which defines critical facilities and systems as those whose disruption could have severe impacts on national security (BRASIL, 2018). Protecting these infrastructures is essential for the country's defense and sovereignty due to their strategic significance (BRASIL, 2012).

As part of the Brazilian Armed Forces' military structure, under the Brazilian Air Force and Air Force Command, the CLA is subject to regulations governing the security and defense of military installations. According to the Air Force Command Directive on Security and Defense (DCA 205-4/2020), security is considered a necessity and an inalienable right, while defense comprises the actions required to ensure and protect these conditions. In this framework, security and defense involve coordinated measures designed to preserve the Brazilian Air Force's combat power, safeguarding installations, equipment, and personnel in line with the specific mission of each military organization (BRASIL, 2020).

From an organizational standpoint, the Brazilian Air Force Command oversees the Security and Defense System ("Sistema de Segurança e Defesa" – SISDE), established by Norm NSCA 205-3/2021, with the purpose of standardizing the planning and implementation of security and defense measures across its military organizations (BRASIL, 2021). The system is led by the Readiness Command ("Comando de Preparo" – COMPREP), headquartered in Brasília, which is responsible for developing doctrines, conducting strategic planning, coordinating operations, and overseeing training and performance evaluation. Operational implementation is carried out by the Security and Defense Units within each military organization, composed of Air Force Infantry contingents responsible for the physical protection of facilities, access control,

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

patrolling, surveillance, and incident response. At the CLA, these functions are performed by the Alcântara Security and Defense Group (GSD-AK).

Brazilian Air Force regulations establish the required infrastructure and measures to ensure security and defense, including perimeter barriers, control posts, electronic surveillance systems, vehicles, remotely piloted aircraft, and specialized personnel tasked with monitoring critical assets, supported by rapid-response teams with high mobility and operational readiness.

Recently, the Integrated Security Support System for Facilities ("Sistema de Suporte Integrado de Segurança das Instalações" – SISI), established under Directive DCA 205-9, was implemented. SISI integrates the security infrastructure of facilities with electronic security resources, including surveillance, access control, and intrusion detection, through an efficient command, control, and intelligence system. It links these capabilities to rapid-response teams equipped with ballistic protection, high mobility, and the capacity to apply force in a progressive and proportional manner (BRASIL, 2025).

The Brazilian Air Force has achieved notable progress in standardizing the security and defense of its military organizations, establishing clear guidelines to safeguard personnel, facilities, and strategic assets. Nevertheless, the CLA's unique operational profile poses distinct challenges, necessitating tailored approaches to address technological, operational, and strategic risks that differ from those faced by conventional military organizations.

The CLA is distinguished by its dual function: besides its strategic role for the Brazilian Air Force, it operates as a center for economic and commercial activities, maintaining close relations with private and international partners. This configuration necessitates security measures beyond the protection of military assets, encompassing the safeguarding of sensitive technologies and industrial secrets of partners, often in compliance with international standards. In this context, adopting strategic corporate security practices emerges as an effective solution, integrating multiple levels of protection to ensure both institutional security and the viability and resilience of the CLA's commercial and space operations.

Applying the principles of strategic corporate security to the Alcântara Launch Center

In the Brazilian context, a distinction is made between public security, responsible for the repression and investigation of crimes, a function predominantly attributed to police authorities, and non-public security, which is administered by the stakeholders themselves and subdivided into private security, focused on the protection of individuals, and corporate security, directed toward the protection of organizations (MANDARINI, 2005).

As part of Brazil's public administration and as a military organization under the Brazilian Air Force, the CLA holds police authority and prerogatives to adopt measures aimed at preserving internal order and discipline, as well as competencies to investigate and prosecute military crimes occurring within its premises (MODESTO; NEVES, 2025; ASSIS, 2020). Simultaneously, it is responsible for protecting its facilities against internal and external threats, not necessarily relying on the direct intervention of public security agencies.

Given these institutional particularities, it becomes relevant to analyze the incorporation of innovative corporate security principles and practices from a strategic perspective, without this constituting a private-sector approach. In this regard, the concept of corporate security has expanded to include organizational or institutional security, also applied to public entities in Brazil, aligning with initiatives

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

developed by bodies such as the Judiciary and the Public Prosecutor's Office (CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, 2019; CONSELHO DA JUSTIÇA FEDERAL, 2021).

Corporate security encompasses the protection of all organizational assets, whether human or material, tangible or intangible. Tangible assets include facilities, machinery, equipment, products, documents, information systems, and movable or immovable property, as well as financial resources such as funding, shares, and investments. Intangible assets cover social and institutional capital, including human resources, the environment, organizational image, secrets, planning, strategies, data, and knowledge, as well as commercial capital, which comprises know-how, processes, logistics, markets, brands, suppliers, clients, credibility, trust, and reputation (MANDARINI, 2005). In the case of the CLA, the scope of protected assets extends beyond financial resources to encompass strategic, sovereignty-related, and national security dimensions.

Strategic Corporate Security represents the most advanced stage in the evolution of organizational security, surpassing the traditional loss-prevention function to assume a central role in competitiveness and value creation. This model focuses on protecting productive activities and services, based on integrated planning, coordinated actions, and training programs aimed at strengthening the security culture (MANDARINI, 2005). Organic security, in turn, constitutes one of the pillars of strategic corporate security and is defined as an integrated set of defensive and preventive measures designed to protect institutional assets and ensure the safe operation of activities (ASSUMPÇÃO; COSTA, 2019).

For the CLA, a Strategic Corporate Security model can be structured around four interdependent segments: area and facility management security, personnel management security, process management security, and knowledge management security.

Area and facility management security can be defined as the set of standards, measures, and procedures designed to protect institutional facilities, particularly those housing classified information or sensitive materials, and must align with the identified risks (CARON; BUENO, 2019). Its objective is to safeguard the organization's tangible assets, preventing unauthorized access, damage, or interference, based on comprehensive risk assessments. Security entails access controls and differentiates measures according to the criticality of each area, aiming to protect people, assets, and processes while also considering potential impacts on the environment and society (MANDARINI, 2005).

Areas are classified according to their nature and sensitivity. Open areas are accessible to the general public, such as reception halls; restricted areas require access control, such as offices and meeting rooms; critical areas host essential infrastructures, such as servers, generators, and control rooms; and classified areas contain sensitive materials, documents, or information, with access restricted to specific credentials. Priority is given to mitigating human-origin threats to physical assets, such as sabotage, theft, or negligence, while also accounting for natural and unpredictable events (CARON; BUENO, 2019).

Mandarini (2005) proposes the Theory of Concentric Circles, which organizes protection into layers that become progressively more restrictive as they approach the most sensitive core. The model defines five levels, each specifying the type of area, authorized personnel, and credentialing requirements. This layered structure establishes a depth-based defense aligned with the criticality of the facilities.

Area and facility security relies on passive security actions characterized by a primarily defensive posture against potential or actual threats. Its effectiveness depends on the integration of four essential components: human surveillance services; physical security, which provides structural and artificial barriers;

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

electronic security, based on detection and monitoring technologies; and access control systems, which regulate the circulation of people and assets. In critical areas, multi-factor authentication is recommended. The synergy among these elements is decisive for consolidating a robust, layered protection system (MANDARINI, 2005; CARON; BUENO, 2019).

At the CLA, Mandarini's Theory of Concentric Circles can be applied considering the high criticality of technological handling areas and launch platforms. Security criteria and physical, electronic, and procedural barriers must be scaled to neutralize threats and protect high-value strategic and technological assets, including those subject to international safeguards such as the AST.

Given the nature of the CLA's operations, which involve high-value technologies, it is essential to adopt a preventive approach, reflected in substantial investments in physical, electronic, cyber, and personnel security. Risk management is also indispensable, either through insurance for payloads and commercial launches or by acknowledging that certain risks, such as catastrophic failures or extreme natural events, cannot be fully eliminated.

Risk management at the CLA involves continuous cost-benefit analysis to support strategic decisions and ensure operational continuity without compromising economic feasibility or international commitments. The integration of systems through a Security Operations Center allows the consolidation of information from sensors, cameras, access controls, intelligence, human surveillance, and cybersecurity, ensuring situational awareness and rapid response capability. Furthermore, the CLA's isolated location in Alcântara necessitates cooperation with agencies such as the police, the Brazilian Navy, and the Brazilian Intelligence Agency, enabling the Brazilian Air Force to act in a coordinated manner that balances discretion with deterrent strength.

Personnel management security aims to mitigate risks associated with human resources throughout their functional lifecycle. It seeks to ensure the physical and moral integrity of personnel, recognizing that the human factor represents both the main asset and the greatest vulnerability of institutional security. This process encompasses recruitment, background checks, credentialing, monitoring, and dismissal, thereby preventing insider threats such as information leaks, sabotage, or coercion, an especially relevant aspect for strategic organizations like the CLA (BANDEIRA, 2019; CARON; BUENO, 2019; MENEZES et al., 2022).

At the CLA, which brings together military personnel, civilian employees, contractors, and representatives of partner nations, secure personnel management is essential. The diversity of these actors increases potential vulnerabilities, demanding rigorous control and verification procedures to prevent fraud, theft, and information leakage. Recruitment, investigation, and credentialing must follow the Brazilian Air Force's intelligence guidelines, ensuring personnel reliability and the protection of sensitive operations and technologies. Moreover, clear protocols for registration, movement planning, definition of access zones, and continuous monitoring are fundamental to reducing risks and strengthening organizational security.

Process management security aims to protect the dynamics of institutional activities, covering all procedures and actions that lead to the delivery of the final product or service, including operations, planning, and input management (MENEZES et al., 2022).

Operational security seeks to protect an institution's essential activities, particularly those considered sensitive, due to their impact on functional continuity, and hazardous, due to associated physical risks (MANDARINI, 2005). At the CLA, the stages of preparation, integration, and launch of aerospace vehicles exhibit both characteristics, demanding maximum vigilance. Considering the high technological value and

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

risks associated with propellants and pyrotechnic systems, failures may lead to significant losses and jeopardize the institution's security, defense, and strategic objectives.

Planning security operates from the very conception of institutional activities, ensuring that the development and execution of plans occur under strict confidentiality and compartmentalization criteria (MANDARINI, 2005). At the CLA, this is particularly critical, as launch campaign planning and security plans involve highly sensitive information. It is necessary to control information access across teams, national entities such as the Brazilian Air Force, the Brazilian Space Agency, and the National Institute for Space Research (Instituto Nacional de Pesquisas Espaciais – INPE), and international partners, thus preventing leaks that could compromise missions and strategic agreements.

Input security extends corporate protection to all items used in production and service delivery, focusing particularly on those that are sensitive due to their value, business significance, or physical hazards. Each item's criticality must be assessed, taking into account both the risks to which it is exposed, such as theft or sabotage, and the risks it may pose, such as flammability or toxicity (MANDARINI, 2005). At the CLA, this dimension is reflected in the secure receiving, storage, and handling of materials, including propellants and aerospace technologies, and in its integration with area and facility security to safeguard warehouses and depots.

Input security also encompasses the logistical planning of material transport, including safety analysis, route definition, tracking, support points, armed escorts, driver registration, and contingency planning. CLA operations require secure transportation of rocket and satellite components, proper storage of propellants, and protection of sensitive technologies, as well as strict oversight in the acquisition and disposal of materials.

Knowledge management security aims to protect the organization's secrets, considered strategic assets and sources of competitive advantage. It is directly linked to the physical security of information and to digital and cyber protection (MANDARINI, 2005). The CLA's space operations involve large volumes of sensitive knowledge, including technical data on rockets and satellites, strategic mission information, and technologies protected under the AST. The rigorous application of knowledge management security through information classification, access control, cyber protection, and physical and communications security is essential to ensuring operational integrity. Any failure in this domain may compromise missions, national security, and Brazil's international credibility.

Proposals for enhancing the security and defense of the Alcântara Launch Center

Considering the distinctive characteristics of the CLA and the application of Strategic Corporate Security principles, this proposal aims to strengthen its protection and defense capabilities. The first step involves establishing a robust organizational security culture, ensuring that all participants in space operations, whether civilian or military, domestic or international, fully understand the components that constitute the CLA's security and defense framework.

Currently, technical personnel, new members, and partners of the Center are required to complete the Launch Operations Preparation Course ("Curso de Preparação para Operações de Lançamento" - CPOL), which is divided into theoretical and practical modules. However, the course content is primarily focused on technical and operational aspects and does not adequately address security and defense dimensions.

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

Therefore, it is necessary to establish a complementary training program that covers the doctrine and regulations of the Brazilian Air Force related to the area, as well as the principles of Strategic Organizational Security, specific protocols for physical security, information security, and emergency procedures, in addition to the requirements of the Brazilian Space Agency, the AST, and future international agreements linked to CLA operations.

The development and maintenance of a robust contingency planning and crisis management system are essential and inseparable components of the CLA's strategic corporate security. In this regard, it is crucial to develop contingency plans consistent with the four-phase cycle of disaster and emergency management: mitigation, which focuses on reducing or eliminating potential risks and impacts before a crisis occurs; preparedness, which involves building the capabilities and procedures required to respond effectively to potential emergencies; response, which entails the immediate implementation of actions following a crisis to minimize human, material, and environmental losses; and recovery, which seeks to restore normal operations while promoting physical, economic, and social reconstruction in a sustainable manner (ALEXANDER, 2002; COPPOLA, 2015).

Considering the sensitive and strategic nature of space operations, the CLA requires contingency planning capable of addressing a broad spectrum of adverse scenarios. These include major operational accidents resulting from launcher malfunctions, with the potential to cause explosions, toxic propellant dispersal, environmental contamination, and human casualties; incidents involving technology protected under the AST, which demand specific response protocols and coordinated communication with U.S. authorities; critical failures in essential systems such as tracking, telemetry, power, and communications, which may compromise operational safety and mission viability; natural disasters and extreme weather events that, due to the Center's coastal location, could damage facilities and disrupt activities; serious physical security incidents such as intrusion attempts, sabotage, or terrorist attacks; cyberattacks aimed at disrupting operations or exfiltrating strategic information; and medical or public health emergencies that could affect personnel or suspend operations.

To effectively address these contingencies, it is essential to establish specific plans integrated within a comprehensive contingency framework. This framework must clearly define chains of command and responsibility, internal and external alert and communication protocols, evacuation procedures, response teams and their respective duties, as well as the logistical resources and operational continuity strategies to be employed. The effectiveness of these plans depends on their broad dissemination among all relevant personnel, the regular execution of training sessions and realistic simulations to identify vulnerabilities, and the continuous enhancement of response capabilities. Such preparation strengthens the CLA's overall security and defense system, helping to minimize losses, protect lives, safeguard assets and the environment, preserve the institutional reputation of the Brazilian Air Force, and ensure the continuity of Brazil's strategic space activities.

Given the complexity and diversity of risks to be managed at the CLA, one alternative is the adoption of a modular planning and phased work strategy (MANDARINI, 2005). Modular planning allows security and defense to be structured in interconnected modules that are developed and implemented progressively, allowing each module to focus on specific aspects of security, such as perimeter protection of the main area, launch platform security, access control to sensitive areas, operational network cybersecurity, and contingency plans for propellant accidents. This approach allows prioritization of module implementation in

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

the most critical areas, including those affected by the AST or vital components for the Brazilian Space Program projects, without compromising the integrated view of the security system being sought.

Phased work complements modularity by defining a feasible schedule for research, development, acquisition, installation, testing, and operation of each module, considering budget constraints, availability of human and technological resources, interdependencies between modules, and the CLA launch operations calendar. This phased implementation facilitates resource management, allows lessons learned from previous stages to be incorporated, enables adjustments to planning based on partial effectiveness evaluations, and ensures that improvements in security and defense occur progressively, controlled, and sustainably.

At the CLA, this approach could be deployed in a first phase of diagnosis and prioritization, with a detailed risk analysis, identification of critical assets, and the development of a Strategic Security Master Plan defining the overall architecture and priority modules; followed by the implementation phase of critical modules, focused on the most urgent security measures, such as reinforcement of physical and electronic protection of areas related to the AST, modernization of access control to sensitive information, and strengthening of initial crisis response capabilities; and finally, subsequent phases aimed at gradual expansion to other areas, adoption of advanced surveillance and security command and control technologies, development of comprehensive training and security culture programs, as well as continuous improvement of already implemented modules.

Risk management at the CLA must begin with a comprehensive and continuous diagnosis capable of encompassing all critical elements for the safe operation of the center. Initially, it is essential to identify critical assets, including both tangible ones, such as launch platforms, launch vehicles, satellites, laboratories, control systems, and technology protected under the AST, and intangible ones, such as project information, telemetry data, flight plans, technical knowledge of personnel, and the reputation of the Brazilian Air Force and the Brazilian Space Program. This mapping must be exhaustive and dynamic, considering that the importance and criticality of assets may evolve with project progress and changes in international agreements.

Next, it is necessary to identify threats specific to the context of Alcântara and space operations, which go beyond generic threats. The analysis must encompass both corporate and non-corporate risks, continuously informed by security intelligence activities, considering direct and indirect threats, regional instabilities, and non-state actors with asymmetric capabilities.

The identification of CLA vulnerabilities is the subsequent step, based on audits, inspections, and detailed analyses, including aspects such as perimeter, access control, information security, personnel training, and dependence on critical systems. This process must be introspective and continuous, utilizing regular security audits, physical and logical penetration tests, analysis of previous incidents, even of minor impact, and feedback from operational personnel.

Risk analysis should assess each scenario combining asset, threat, and vulnerability, considering the probability of occurrence and potential impact. This evaluation must cover multiple dimensions of loss, including financial, operational, human, reputational, and opportunity-related, with particular attention to strategic impacts for the Brazilian Air Force, the Brazilian Space Program, Brazil's international credibility, and national security. The analysis should consider systemic interdependencies, in which failure in one component can generate cascading effects, compromising multiple operations and critical assets.

revista E-ISSN 1087-1260 ISSN1808-0259
Intellector
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

Finally, risk evaluation and prioritization should be carried out using a risk matrix adapted to the CLA specificities, classifying risks as low, medium, high, or critical, and directing resources to those with the highest potential to damage the strategic objectives of the Brazilian Air Force and the Center. This process should result in a clear, formalized action plan, periodically reviewed by the chain of command.

Risk treatment strategies at the CLA must be selected based on effectiveness and feasibility. The primary strategy is risk reduction through physical, logical, procedural, and human security controls, including strengthening the management of areas and facilities, personnel, processes, and knowledge, as well as implementing the Integrated Facility Security Support System (SISI), adapted to the CLA context. Risk treatment must be continuous and integrated into strategic and budgetary planning, with audits and proactive monitoring to anticipate vulnerabilities. Security education is essential, forming a conscious and trained workforce capable of monitoring and reporting anomalies, thereby strengthening the CLA security culture.

Intelligence activities are fundamental to CLA security and defense. The process involves planning information requirements, collecting data from open and protected sources, analyzing and integrating information, and disseminating actionable knowledge to decision-makers at the CLA and the command chain. Counterintelligence complements this process by protecting informational assets and ensuring operational security. Its actions include safeguarding sensitive knowledge through rigorous protocols for classification, handling, and storage of confidential information; neutralizing attempts at espionage, hostile surveillance, or personnel recruitment; and ensuring the security of communications and data systems in collaboration with IT specialists. The integration of CLA Intelligence with the Air Force Intelligence System and, more broadly, with the Brazilian Intelligence System is essential to enable the flow of relevant information and coordinate efforts against threats exceeding local analytical capacity, thereby strengthening the protection of critical assets and the effectiveness of security and defense.

The Strategic Security Master Plan for the CLA supports the consolidation and integration of the Center's security and defense management in alignment with the principles of Strategic Corporate Security, the guidelines of the Brazilian Air Force, and the Integrated Facility Security Support model. This plan should define normative and operational guidelines aimed at safeguarding critical assets, information, and processes. It must encompass governance, risk management, and the security of personnel, facilities, processes, and knowledge, as well as contingency planning, security education programs, and mechanisms for continuous improvement. The adoption of this instrument is essential to ensure integrated, strategic, and adaptable security and defense management, thereby strengthening the protection of the CLA and ensuring compliance with national and international security and technology obligations.

Conclusion

The analysis of the CLA demonstrates that the strengthening of strategic infrastructures extends far beyond the technical operation of space launches, constituting a central element for the consolidation of Brazil's national autonomy and sovereignty. The CLA not only embodies the country's capacity to sustain complex space programs but also functions as a multidimensional platform integrating science, technology, defense, and international cooperation, strategically and coherently aligning civil and military interests.

The study indicates that the security and defense of the CLA require an integrated and adaptable model capable of simultaneously protecting high-value tangible and intangible assets, such as technological knowledge, institutional credibility, and national sovereignty. The application of Strategic Corporate Security principles provides a robust framework, allowing protection to be structured across four complementary dimensions: facilities and infrastructure, personnel management, process management, and knowledge management. This approach not only strengthens physical and cyber protection but also ensures operational continuity in the face of operational, technological, environmental, and human risks.

The implementation of modular and phased strategies, combined with comprehensive contingency planning, demonstrates that operational efficiency can be reconciled with high security standards. The mapping of critical assets, detailed analysis of threats and vulnerabilities, and systematic prioritization of risks enable informed strategic decisions, mitigating impacts and preventing cascading effects that could compromise not only the CLA but also the Brazilian Space Program and the country's international reputation. The integration of intelligence and counterintelligence into the security system enhances response capabilities and strengthens institutional resilience, ensuring that sensitive information is protected and that international partnerships are conducted in accordance with regulatory and strategic requirements.

Considering this evidence, the consolidation of a Strategic Security Master Plan emerges as an indispensable measure to align normative, operational, and educational guidelines, promoting an organizational culture of informed and effective security. This plan represents the synthesis of the strategic security vision, articulating prevention, protection, response, and recovery, ensuring that the CLA maintains its role as critical infrastructure, an international launch hub, and a symbol of Brazilian technological sovereignty. Ultimately, the continuous strengthening of Strategic Corporate Security at the CLA not only safeguards critical assets but also consolidates Brazil's position as a relevant and reliable actor in the global space arena, translating into autonomy, credibility, and sustained innovative capacity.

References

ALEXANDER, D. Principles of emergency planning and management. New York: Oxford University Press, 2002.

ANDRADE, Israel de Oliveira et al. O Centro de Lançamento de Alcântara: Abertura para o mercado internacional de satélites e salvaguardas para a soberania nacional. Brasília, DF: Ipea, 2018. (Texto para Discussão, n. 2423).

ASSIS, Cirelene Maria da Silva Rondon de. A projeção do poder de polícia das Forças Armadas nas áreas adjacentes aos aquartelamentos. Curitiba: Editora CRV, 2020.

ASSUMPÇÃO, Marcelo Neival Hillesheim de; COSTA, Gustavo Monteiro Muniz. "Os desafios e oportunidades para a atividade de contrainteligência na era do conhecimento". *In*: CONSELHO NACIONAL DO MINISTÉRIO

PÚBLICO. Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro. Brasília: CNMP, 2019. p. 124-141.

BANDEIRA, Jerusa Capistrano Pinto. "A Contrainteligência no Ministério Público: Breves Considerações". *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro. Brasília: CNMP, 2019. p. 38-49.

BRASIL. Agência Espacial Brasileira. Espaçoporto de Alcântara entra no mercado de transporte espacial. 2023. Disponível em: https://www.gov.br/aeb/pt-br/assuntos/noticias/espacoporto-de-alcantara-entra-no-mercado-de-transporte-espacial. Acesso em: 22 out. 2025.

BRASIL. Agência Espacial Brasileira. PDI - CEA - Programa de Desenvolvimento Integrado para o Centro Espacial de Alcântara. Alcântara, MA: AEB, 2022.

BRASIL. Centro de Lançamento de Alcântara. Cartilha institucional do Centro de Lançamento de Alcântara. Alcântara, MA: CLA, 2016.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 340/GC3, de 13 de março de 2020. Aprova a reedição da DCA 205-4 "Segurança e Defesa no Comando da Aeronáutica". Boletim do Comando da Aeronáutica, Brasília, DF, n. 044, 17 mar. 2020.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria GABAER/GC3 nº 979, de 14 de maio de 2025. Aprova a DCA 205-9 "Implantação do Suporte Integrado de Segurança das Instalações nas Organizações Militares do COMAER". Boletim do Comando da Aeronáutica, Brasília, DF.

BRASIL. Comando da Aeronáutica. Comando de Preparo. Portaria COMPREP nº 91/COMPREP, de 9 de abril de 2021. Aprova a reedição da NSCA 205-3 "Sistema de Segurança e Defesa do Comando da Aeronáutica". Boletim do Comando da Aeronáutica, Brasília, DF, n. 081, 4 maio 2021.

BRASIL. Comando da Aeronáutica. Departamento de Ciência e Tecnologia Aeroespacial. Portaria DCTA/DCE nº 540, de 4 de outubro de 2024. Aprova a TCA 37-15 "Cursos do DCTA para o ano de 2025".

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF, 23 nov. 2018.

BRASIL. Decreto nº 10.220, de 5 de fevereiro de 2020. Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América sobre Salvaguardas Tecnológicas Relacionadas à Participação dos Estados Unidos da América em Lançamentos a partir do Centro Espacial de Alcântara, firmado em Washington, D.C., em 18 de março de 2019. Diário Oficial da União, Brasília, DF, 6 fev. 2020.

revista Intellector
E-ISSN 1087-1260 ISSN1808-0259
Centro de Estudos em Geopolítica e Relações Internacionais - Brasil

Ano XXI | Volume XXII | Nº 44 | Julho/Dezembro 2025 | Rio de Janeiro | ISSN 1807-1260

www.revistaintellectori.org.br

BRASIL. Comando da Aeronáutica. Relatório da Investigação do Acidente Ocorrido com o VLS-1 v03, em 22 de agosto de 2003, em Alcântara, maranhão. Brasília, DF, 2004.

BRASIL. Ministério da Defesa. Política Nacional de Defesa e Estratégia Nacional de Defesa. Brasília, DF: MD, 2012.

CARON, Ricardo; BUENO, Vani Antônio. "Inteligência e Segurança Institucional: uma abordagem sobre a segurança de áreas e instalações no Ministério Público". *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro. Brasília: CNMP, 2019. p. 68-94.

CHOAIRY, Antônio Cesar Costa. Alcântara vai para o espaço: a dinâmica da implantação do Centro de Lançamento de Alcântara. São Luís: EDUFMA: PROIN-CS, 2000.

COPPOLA, D. P. Introduction to international disaster management. 3. ed. Amsterdam: Elsevier, 2015.

CONSELHO DA JUSTIÇA FEDERAL. PORTARIA N. 269-CJF. Dispõe sobre o Plano de Segurança Orgânica do Conselho da Justiça Federal – PSO/CJF. Brasilia, 2021.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro. Brasília: CNMP, 2019.

DURÃO, Otavio Santos Cupertino; CEBALLOS, Décio Castilho. "Desafios Estratégicos do Programa Espacial Brasileiro". *In:* Presidência da República. Desafios do Programa Espacial Brasileiro, p. 41-58, 2011.

MANDARINI, Marcos. Segurança Corporativa Estratégica: Fundamentos. Barueri, SP: Manole, 2005.

MENEZES, Antônio Alberto Moraes de et al. Política de segurança orgânica: Polícia civil e polícia militar do Piauí. Teresina: Lamparina Editora, 2022.

MODESTO, Thiago de Souza; NEVES, Sérvio Alcântara. "A segurança orgânica e o poder de polícia do exército nas áreas adjacentes dos aquartelamentos". Revista do Ministério Público Militar, Brasília, a. 52, n. 46, p. 162-216, maio 2025.

UNITED STATES SPACE FORCE (USSF). Space Cap-stone Publication Spacepower*:* Doctrine for Space Forces. Washington, D.C.: United States Space Force, 2020.

UNIVERSIDADE FEDERAL DO MARANHÃO - UFMA. Contribuições da UFMA ao programa de desenvolvimento integrado do centro espacial de Alcântara PDI-CEA. São Luís: UFMA, 2020.