# **Cibersegurança Espacial: Protegendo a Fronteira Final na Era Digital**

## **Sumário Executivo**

Este relatório oferece uma análise exaustiva do mercado global de cibersegurança espacial, um setor em rápida expansão impulsionado pela crescente dependência de ativos espaciais e pela intensificação das ameaças geopolíticas e comerciais. À medida que a sociedade moderna se torna intrinsecamente ligada à infraestrutura orbital para comunicação, navegação, finanças e defesa, a proteção desses sistemas contra ataques cibernéticos evoluiu de uma preocupação de nicho para uma prioridade estratégica global.

Os principais achados deste relatório indicam um mercado dinâmico e em ponto de inflexão. O mercado de cibersegurança espacial foi avaliado em US$ 4,8 bilhões em 2024, com uma projeção de crescimento a uma robusta Taxa de Crescimento Anual Composta (CAGR) de 9,4% entre 2025 e 2034.1 Este crescimento é alimentado pela expansão exponencial de atividades espaciais comerciais, lideradas por megaconstelações, e pelo aumento contínuo do investimento governamental e militar na proteção de ativos estratégicos.

O cenário de ameaças não é mais teórico. Ataques de alto perfil, como o hackeamento dos serviços de internet via satélite da Viasat por agentes russos momentos antes da invasão da Ucrânia 3, demonstram que a cibersegurança espacial é um componente crítico da guerra moderna e da segurança nacional. Os sistemas espaciais são vulneráveis em três segmentos interconectados: solo, espaço e enlace de comunicação.4 O segmento terrestre, que inclui as estações de controle, continua a ser o vetor de ataque mais prevalente e acessível, como evidenciado por incidentes passados em agências como a NASA.5

Em resposta, a vanguarda tecnológica está avançando rapidamente. A defesa está evoluindo com a adoção de Inteligência Artificial (IA) para detecção preditiva de anomalias 7, o desenvolvimento de criptografia pós-quântica (PQC) para garantir a segurança contra ameaças futuras 9, e a implementação de arquiteturas de confiança zero (zero-trust), especialmente adequadas para as complexas redes de satélites.11

No contexto nacional, o Brasil está se posicionando de forma estratégica. A recente instituição da Política Nacional de Cibersegurança (PNCiber) 13 e a significativa integração da Agência Espacial Brasileira (AEB) ao Sistema Brasileiro de Inteligência (Sisbin) 14 sinalizam um reconhecimento formal da importância da cibersegurança para a soberania e segurança do programa espacial do país.

As recomendações estratégicas para os stakeholders incluem um foco rigoroso em "segurança por design" (security by design), o desenvolvimento de padrões de segurança unificados, o investimento contínuo em pesquisa e desenvolvimento de tecnologias resilientes e o fortalecimento da colaboração público-privada e internacional para o compartilhamento de inteligência sobre ameaças.

## **Introdução: A Criticidade da Cibersegurança na Nova Corrida Espacial**

A cibersegurança espacial emergiu como um dos domínios mais críticos e de mais rápida evolução na segurança global. Longe de ser apenas uma extensão da segurança de TI tradicional, ela é definida como um conjunto de medidas proativas para detectar, prevenir e responder a ciberataques contra toda a infraestrutura espacial.15 Isso inclui não apenas os satélites em órbita, mas também naves espaciais, veículos lunares, estações terrestres e os complexos dispositivos de telecomunicação que os conectam.16 A disciplina abrange tanto a segurança lógica, referente à proteção de software e dados, quanto a segurança física da infraestrutura, que pode ser comprometida por meios digitais.17

### **A Dependência Invisível**

A sociedade moderna opera sobre uma base de serviços espaciais que, embora muitas vezes invisível, é fundamental para seu funcionamento. A interrupção ou comprometimento de sistemas de posicionamento global (GPS), por exemplo, não afetaria apenas a navegação de carros, aviões e navios. Teria um efeito cascata paralisante sobre setores inteiros da economia: os mercados financeiros, que dependem da precisão de nanossegundos fornecida pelos relógios atômicos dos satélites para registrar transações; as cadeias de suprimentos globais, que coordenam frotas de transporte; as redes de telecomunicações, incluindo chamadas de celular, que usam sinais de satélite para sincronização; e a capacidade de responder a desastres naturais, que depende de imagens e comunicações espaciais.3 A perda desses serviços poderia, em alguns casos, regredir partes significativas da economia e da infraestrutura global a tecnologias da década de 1950.3

### **O Ponto de Inflexão: "New Space" e Geopolítica**

A paisagem espacial mudou drasticamente nas últimas duas décadas. A era do "New Space", caracterizada pela liderança do setor privado com empresas como SpaceX, Amazon e OneWeb, e pela proliferação de megaconstelações de satélites em órbita baixa (LEO), democratizou o acesso ao espaço.1 No entanto, essa expansão exponencial, combinada com crescentes tensões geopolíticas, transformou o espaço em um domínio congestionado e contestado.3 A suposição de que os sistemas espaciais, especialmente os comerciais, eram isolados de ameaças cibernéticas foi provada falsa.4 Hoje, governos e militares dependem fortemente de sistemas comerciais, tornando a segurança desses ativos uma questão de segurança nacional.4

Essa nova realidade fundamentalmente altera o conceito tradicional de ciberespaço, que por muito tempo foi visto como um domínio abstrato e não físico.20 A operação de ativos físicos em órbita, controlados inteiramente por meios digitais, cria uma ligação direta e tangível entre um ataque cibernético lógico e uma consequência cinética no mundo real. Uma linha de código comprometida pode agora alterar a trajetória de um satélite de bilhões de dólares, desativá-lo ou até mesmo usá-lo como arma, desfocando efetivamente a linha entre a segurança digital e a física.21 Consequentemente, as estratégias de defesa devem ser híbridas, considerando tanto a proteção das redes de TI tradicionais no solo quanto a resiliência de hardware e software em ambientes extremos e fisicamente inacessíveis.

## **Panorama de Ameaças e Vulnerabilidades no Domínio Espacial**

A percepção de que os ativos espaciais são imunes a ataques cibernéticos devido à sua distância física é uma falácia perigosa.19 A arquitetura de qualquer sistema espacial é composta por três componentes distintos e interligados, cada um com seu próprio conjunto de vulnerabilidades.4

### **A Arquitetura de Risco: Uma Análise Tridimensional**

* **Segmento Terrestre (Solo):** Este é o ponto de partida para a maioria dos ataques cibernéticos e o mais vulnerável. Inclui estações de controle, centros de processamento de dados e redes de comunicação que conectam a infraestrutura terrestre. Sua principal vulnerabilidade reside na sua conexão com redes de TI convencionais e na internet, expondo-os a vetores de ataque comuns.4 Um exemplo notório ocorreu em 2018, quando o Jet Propulsion Laboratory (JPL) da NASA foi invadido por meio de um computador Raspberry Pi não autorizado e inseguro conectado à rede. A falta de segmentação da rede permitiu que o invasor se movesse lateralmente e extraísse dados sensíveis de missões críticas, forçando outros centros da NASA a se desconectarem do JPL como medida de precaução.6
* **Segmento Espacial:** Contrariando a suposição de que são "isolados" 4, os satélites são essencialmente computadores sofisticados em órbita. Suas vulnerabilidades incluem:
  + **Satélites Definidos por Software (SDR):** A crescente tendência de usar software para definir a funcionalidade de um satélite permite que ele seja reprogramado em órbita. Embora isso ofereça uma flexibilidade sem precedentes, também cria uma nova superfície de ataque, onde um hacker poderia, teoricamente, assumir o controle total das funções do satélite.5
  + **Componentes Comerciais Prontos (COTS):** Para reduzir custos e acelerar a produção, especialmente em megaconstelações, os fabricantes utilizam componentes eletrônicos comerciais (COTS). Esses componentes podem ser facilmente adquiridos e analisados por atores mal-intencionados na Terra, que podem descobrir e explorar vulnerabilidades antes mesmo do lançamento do satélite.22
  + **Sistemas Legados:** Muitos satélites em operação hoje foram projetados e lançados antes que a cibersegurança fosse uma preocupação primordial. Esses sistemas legados carecem de proteções modernas, são extremamente difíceis de atualizar e, portanto, representam alvos fáceis.23
* **Segmento de Enlace (Link):** Refere-se aos canais de comunicação que conectam os segmentos terrestre e espacial (uplink, downlink) e os satélites entre si (crosslink). As principais ameaças neste segmento são:
  + **Jamming e Spoofing:** A interferência deliberada (jamming) ou a falsificação de sinais (spoofing) são ataques relativamente baratos e eficazes que podem interromper a comunicação ou, pior, enviar comandos falsos a um satélite.5
  + **Interceptação (Eavesdropping):** A captura de dados sensíveis transmitidos entre o satélite e a Terra é uma ameaça real, com registros de organizações militantes hackeando satélites para roubar dados de redes militares desde meados da década de 2000.27

### **Vectores de Ataque e Precedentes Históricos**

As ameaças à cibersegurança espacial não são mais hipotéticas; são uma realidade comprovada por incidentes de alto impacto.

* **Guerra na Ucrânia (2022):** O ataque cibernético russo à rede de satélites KA-SAT da Viasat, ocorrido uma hora antes da invasão terrestre, é o caso de estudo definitivo sobre o papel da cibersegurança espacial na guerra moderna. O ataque desativou dezenas de milhares de terminais de internet via satélite, não apenas prejudicando as comunicações militares ucranianas, mas também causando interrupções em serviços civis por toda a Europa, incluindo o controle remoto de milhares de turbinas eólicas na Alemanha.3
* **Exercício de Invasão da ESA (2022):** Em um exercício de segurança controlado, a empresa de tecnologia Thales demonstrou a capacidade de invadir o satélite OPS-SAT da Agência Espacial Europeia. Usando direitos de acesso padrão, os hackers éticos exploraram vulnerabilidades para inserir código malicioso, comprometer a integridade dos dados e até manipular as imagens capturadas pela câmera do satélite para ocultar suas atividades.28
* **Iniciativa Hack-a-Sat:** Reconhecendo a gravidade da ameaça, a Força Espacial dos EUA, em parceria com a famosa convenção de hackers DefCon, criou o evento "Hack-a-Sat". Nele, hackers éticos são convidados a tentar invadir um satélite real em órbita, o "Moonlighter", com o objetivo de descobrir e corrigir vulnerabilidades de forma proativa.19

Essa evolução significa uma mudança crítica na doutrina militar: a linha entre a guerra cibernética e a guerra espacial está efetivamente se dissolvendo. Um ciberataque que desabilita ou sequestra um satélite atinge o mesmo objetivo estratégico que um míssil antissatélite (ASAT) tradicional 18, mas oferece vantagens significativas: custo mais baixo, negação plausível e a ausência de detritos espaciais perigosos. Como confirmado por oficiais militares, ataques não cinéticos a satélites dos EUA já são uma ocorrência diária 30, forçando uma reavaliação do que constitui um ato de guerra no domínio espacial.

### **Atores de Ameaça e Motivações**

* **Nações-Estado:** Atores como a Rússia e a China estão desenvolvendo ativamente capacidades de guerra espacial, que incluem tanto armas cinéticas (mísseis ASAT) quanto não cinéticas (ciberataques, lasers, bloqueadores de radiofrequência).18 Seus objetivos variam desde espionagem e interrupção de serviços até a obtenção de uma vantagem estratégica decisiva em um futuro conflito.
* **Cibercriminosos e Hacktivistas:** Grupos com motivações financeiras ou ideológicas também representam uma ameaça. Há registros de criminosos brasileiros que sequestraram a largura de banda de satélites militares dos EUA para comunicações gratuitas, bem como de grupos que usaram satélites para transmitir propaganda.22

## **Análise de Mercado: Dimensão, Crescimento e Oportunidades**

O mercado de cibersegurança espacial está se consolidando como um setor de alto crescimento, impulsionado pela convergência de necessidades comerciais e imperativos de segurança nacional.

### **Dimensionamento e Projeções**

Análises de mercado recentes fornecem uma imagem clara da trajetória de crescimento do setor. O mercado global de cibersegurança espacial foi avaliado em **US$ 4,8 bilhões em 2024**. As projeções indicam uma robusta Taxa de Crescimento Anual Composta (CAGR) de **9,4% entre 2025 e 2034**.1 Para contextualizar, o mercado geral de cibersegurança, muito mais maduro, deve crescer a uma CAGR de 11,6% até 2030 32, o que demonstra que o nicho espacial, embora menor em valor absoluto, está crescendo a um ritmo comparável e vigoroso. Focando no mercado dos EUA, um dos maiores do setor, a projeção é de um crescimento de US$ 1,23 bilhão em 2025 para US$ 2,44 bilhões em 2033, a uma CAGR de 8,9%.33

Essa dinâmica ilustra uma transformação fundamental na forma como o mercado percebe a cibersegurança espacial. O que antes era visto predominantemente como um custo operacional ou uma apólice de seguro contra eventos de baixa probabilidade 5 está se tornando um investimento estratégico indispensável. A resiliência cibernética não é mais apenas uma medida defensiva; é um facilitador essencial para a continuidade dos negócios e a viabilização de novos modelos de receita, como o turismo espacial e as redes globais de internet. Consequentemente, a postura de segurança de uma empresa espacial é agora um indicador-chave de sua viabilidade e potencial de crescimento a longo prazo.

### **Principais Impulsionadores de Crescimento**

Dois fatores principais estão impulsionando essa expansão:

1. **Aumento do Investimento Governamental e Militar:** A defesa nacional continua sendo o principal motor do mercado. Reconhecendo que os sistemas espaciais são a espinha dorsal das operações militares modernas (para comunicações, inteligência, vigilância e reconhecimento - ISR), os governos estão alocando orçamentos significativos para sua proteção. A Força Espacial dos EUA, por exemplo, solicitou **US$ 700 milhões em seu orçamento de 2024** com o objetivo específico de aprimorar a cibersegurança de seus sistemas terrestres.1 Essa tendência reflete um esforço internacional para proteger a infraestrutura espacial crítica contra ameaças crescentes.
2. **Expansão Exponencial das Atividades Espaciais Comerciais:** A ascensão de megaconstelações de satélites está criando uma demanda massiva e sem precedentes por soluções de cibersegurança. Projetos como o **Projeto Kuiper da Amazon**, que planeja implantar 3.236 satélites em órbita baixa (LEO), e o Starlink da SpaceX, que já possui milhares de satélites operacionais, aumentam exponencialmente a superfície de ataque e a complexidade da rede.1 A proteção desses vastos e interconectados ativos comerciais é crucial não apenas para as empresas, mas também para os governos que dependem de seus serviços.

### **Oportunidades Emergentes para Pequenas e Médias Empresas (PMEs)**

O setor de cibersegurança espacial não é exclusivo dos gigantes da defesa. Ele está emergindo como um **nicho lucrativo e em rápida evolução**, repleto de oportunidades para empreendedores e pequenas e médias empresas.34 As PMEs podem capitalizar essa tendência de várias maneiras:

* **Desenvolvimento de Soluções Inovadoras:** Criar produtos e serviços de nicho, altamente especializados e adaptados aos desafios únicos dos sistemas de satélite, como software para ambientes de alta radiação ou algoritmos de detecção de ameaças para constelações LEO.34
* **Consultoria e Avaliação de Risco:** Oferecer serviços especializados de auditoria, avaliação de risco e conformidade regulatória para operadoras de satélite, fabricantes e agências governamentais.34
* **Liderança de Pensamento (Thought Leadership):** Posicionar-se como especialistas no setor por meio da publicação de conteúdo, webinars e participação em eventos, atraindo clientes e parceiros estratégicos.34

**Tabela 1: Projeção do Mercado de Cibersegurança Espacial (2024-2034)**

| Ano | Valor do Mercado Global (US$ bilhões) | Taxa de Crescimento Anual (CAGR) | Principais Impulsionadores |
| --- | --- | --- | --- |
| **2024** | $4.8 | - | Aumento do investimento militar; Início da implantação de megaconstelações comerciais. |
| **2025** | ~$5.25 | 9.4% (2025-2034) | Expansão contínua de constelações (Kuiper, Starlink); Aumento da dependência de serviços espaciais. |
| **2030** | ~$8.16 | 9.4% (2025-2034) | Maturidade dos mercados de turismo espacial e IoT via satélite; Adoção de IA e 5G. |
| **2034** | ~$11.66 | 9.4% (2025-2034) | Necessidade de tecnologias pós-quânticas; Regulamentações de segurança mais rigorosas. |
| Fonte: Baseado em dados e projeções de 1 |  |  |  |  |

## **Cenário Competitivo: Titãs da Indústria e Startups Inovadoras**

O mercado de cibersegurança espacial é caracterizado por uma coexistência dinâmica entre gigantes da defesa estabelecidos e startups ágeis e inovadoras. Essa estrutura oferece aos clientes uma gama diversificada de soluções, desde sistemas de segurança de ponta a ponta até tecnologias de nicho altamente especializadas.

### **Os Gigantes Estabelecidos (Incumbents)**

Um núcleo de grandes empresas de defesa e aeroespacial domina uma parcela significativa do mercado. Um grupo de cinco players principais — Thales, Lockheed Martin, General Dynamics, Booz Allen Hamilton e Northrop Grumman — responde coletivamente por **50-55% do mercado de soluções e serviços de cibersegurança espacial**.11

* **Thales (França):** Posicionada como líder em soluções de cibersegurança de ponta a ponta, a Thales oferece desde avaliação de risco até produtos de proteção de dados, como os criptografadores Mistral.35 Sua liderança foi reforçada ao ganhar o contrato para definir a arquitetura de cibersegurança para o sistema de satélites Galileo de Segunda Geração (G2G) da Europa.11
* **Lockheed Martin (EUA):** Com forte foco no setor de defesa, a Lockheed Martin utiliza Inteligência Artificial e Machine Learning para proteger redes de satélites militares dos EUA e sistemas terrestres associados, fornecendo detecção de ameaças em tempo real e redes resilientes.33
* **Northrop Grumman (EUA):** Especializada em hardware e software avançados, a Northrop Grumman desenvolve soluções como a Unidade de Criptografia Final Espacial (Space End Crypto Unit - ECU), projetada para defender redes de satélites interconectadas contra ameaças cibernéticas sofisticadas.33
* Outros players importantes que possuem forte presença em missões governamentais e de defesa incluem **Airbus, BAE Systems e Leonardo S.p.A.**.11

### **A Vanguarda das Startups (Disruptors)**

Paralelamente aos gigantes, um ecossistema vibrante de startups está introduzindo agilidade e inovação, focando em tecnologias de ponta para resolver os desafios emergentes do "New Space".

* **SpiderOak Mission Systems (EUA):** Uma das pioneiras na aplicação de arquiteturas de **confiança zero (zero-trust)** e baseadas em blockchain para o setor espacial. Sua plataforma **OrbitSecure** foi projetada especificamente para proteger as comunicações de dados em constelações LEO, assumindo que nenhuma entidade na rede é inerentemente confiável.11
* **Xage Security, Inc. (EUA):** Desenvolve arquiteturas de segurança descentralizadas, ideais para os complexos ambientes de computação de borda (edge computing) que estão se tornando comuns em constelações de satélites modernas.11
* **WISeKey (Suíça):** Por meio de sua subsidiária **WISeSat**, esta empresa está na vanguarda da segurança futura, planejando lançamentos de satélites equipados com chips e tecnologia de segurança **pós-quântica (PQC)** para proteger as comunicações da Internet das Coisas (IoT) contra a ameaça iminente da computação quântica.10
* **Loft Orbital (EUA):** Inovando no processamento de dados, a Loft Orbital foca em levar a computação de borda para o próprio satélite. Isso permite que o satélite processe dados e tome decisões autônomas a bordo, incluindo medidas de autoproteção, reduzindo a latência e a dependência de links de comunicação vulneráveis.37
* **21SoftWare (EUA):** Uma startup que desenvolve software e serviços de engenharia, como sua plataforma TSEL, para melhorar a segurança, a proteção e a confiabilidade das operações baseadas no espaço.38

Este cenário competitivo revela uma bifurcação na estratégia de mercado. Os gigantes da defesa operam em um modelo "top-down", aproveitando seus contratos governamentais para fornecer soluções de segurança de nível militar, holísticas e de ponta a ponta.11 Em contraste, as startups adotam uma abordagem "bottom-up", focando em resolver desafios tecnológicos específicos com soluções ágeis e de vanguarda, visando principalmente o dinâmico mercado comercial de constelações LEO.11 Essa dinâmica sugere um futuro de colaborações e aquisições estratégicas, onde os grandes players integrarão as inovações das startups para se manterem competitivos.

**Tabela 2: Principais Atores no Mercado de Cibersegurança Espacial**

| Empresa (País) | Categoria | Soluções/Especialidades Chave | Clientes-Alvo |
| --- | --- | --- | --- |
| **Thales** (França) | Titã da Indústria | Criptografia de nível militar, segurança de ponta a ponta (Galileo G2G) | Governos, Militares, Operadores de satélites críticos |
| **Lockheed Martin** (EUA) | Titã da Indústria | IA/ML para defesa, redes resilientes | Defesa dos EUA, Agências de Inteligência |
| **Northrop Grumman** (EUA) | Titã da Indústria | Hardware de segurança (Space End Crypto Unit), proteção de redes | Defesa dos EUA, Operadores de redes de satélites |
| **SpiderOak** (EUA) | Startup Inovadora | Arquitetura de Confiança Zero (Zero-Trust), Blockchain (OrbitSecure) | Operadores comerciais de LEO, Defesa |
| **WISeKey/WISeSat** (Suíça) | Startup Inovadora | Criptografia Pós-Quântica (PQC), Segurança para IoT via satélite | Setor de IoT, Logística, Agricultura |
| **Loft Orbital** (EUA) | Startup Inovadora | Computação de borda (Edge Computing) a bordo, Autoproteção de satélites | Operadores de sensores, Missões de resposta rápida |
| Fonte: Baseado em dados de 10 |  |  |  |  |

## **Inovações Tecnológicas na Defesa de Ativos Espaciais**

A crescente sofisticação das ameaças cibernéticas exige uma evolução constante nas tecnologias de defesa. O setor de cibersegurança espacial está na vanguarda dessa inovação, desenvolvendo e implementando soluções projetadas para os desafios únicos do ambiente espacial.

### **Inteligência Artificial (IA) e Machine Learning (ML): A Faca de Dois Gumes**

A Inteligência Artificial é talvez a tecnologia mais transformadora na cibersegurança moderna, atuando tanto como uma poderosa ferramenta de defesa quanto como uma arma para os atacantes.

* **IA como Ferramenta de Defesa:** A principal vantagem da IA na defesa espacial é sua capacidade de analisar volumes massivos de dados de telemetria de satélites em tempo real. Algoritmos de Machine Learning podem identificar anomalias sutis e padrões de ataque que seriam impossíveis de detectar para analistas humanos, permitindo uma resposta mais rápida e até preditiva.7 Um exemplo prático é o sistema  
  **NOSTRADAMUS**, desenvolvido pela agência espacial francesa (CNES), que utiliza um algoritmo de One-Class Support Vector Machine (OC-SVM) para detectar comportamentos atípicos na telemetria de satélites. O CNES já está trabalhando para implantar uma versão deste sistema diretamente a bordo dos satélites para detecção autônoma.8 Da mesma forma, o sistema  
  **ATHMoS** do Centro de Operações Espaciais Alemão (GSOC) utiliza ML para o monitoramento automatizado da saúde da telemetria.40
* **IA como Ferramenta de Ataque:** Por outro lado, atores mal-intencionados estão utilizando IA para criar ataques mais sofisticados e evasivos. Isso inclui a criação de malware que pode se adaptar para evitar a detecção e o desenvolvimento de campanhas de phishing e engenharia social altamente personalizadas e convincentes.43 Cenários de ataque realistas preveem o uso de IA para simular a voz de superiores e enganar operadores em estações terrestres para que realizem ações prejudiciais.22

### **Criptografia Avançada: A Corrida Contra a Ameaça Quântica**

A proteção de dados em trânsito e em repouso é a base da cibersegurança. Com o avanço da computação quântica, que ameaça quebrar os algoritmos de criptografia atuais, o setor espacial está investindo em novas fronteiras criptográficas.

* **Criptografia Quântica (QKD - Quantum Key Distribution):** Diferente da criptografia tradicional baseada em matemática, a QKD se baseia nas leis da física quântica. Ela permite a criação de chaves de criptografia que são teoricamente "invioláveis", pois qualquer tentativa de interceptar e medir as partículas de luz (fótons) que transportam a chave altera seu estado, alertando imediatamente os usuários da comunicação.9 O principal desafio da QKD é sua limitação de distância em fibras ópticas. No entanto, os satélites são vistos como a solução ideal para estender a QKD a uma escala global, transmitindo os sinais quânticos através da fina atmosfera em grandes altitudes, onde a interferência é mínima.9
* **Criptografia Pós-Quântica (PQC):** Enquanto a QKD se concentra na troca segura de chaves, a PQC refere-se a uma nova geração de algoritmos de criptografia projetados para serem executados em computadores clássicos, mas que são resistentes a ataques de futuros computadores quânticos. Startups como a **WISeSat** já estão na vanguarda, planejando lançar satélites equipados com chips PQC-ready para proteger redes de IoT.10
* **Criptografia Tradicional Robusta:** Enquanto as tecnologias quânticas amadurecem, algoritmos simétricos e assimétricos comprovados, como Advanced Encryption Standard (AES) com chaves de 256 bits (AES-256), Triple DES (3DES) e RSA, continuam a ser a espinha dorsal da segurança de dados para a maioria dos sistemas espaciais atuais, protegendo dados tanto em trânsito quanto em repouso.45

### **Arquiteturas de Confiança Zero (Zero-Trust)**

O modelo de segurança de confiança zero representa uma mudança de paradigma fundamental. Ele abandona a ideia ultrapassada de um perímetro de rede seguro e opera sob o princípio de "nunca confiar, sempre verificar". Em uma arquitetura de confiança zero, nenhuma entidade, seja dentro ou fora da rede, é automaticamente confiável. Cada usuário, dispositivo e aplicativo deve ser rigorosamente autenticado e autorizado antes de obter acesso a qualquer recurso, e esse acesso é concedido com o mínimo de privilégios necessários.12 Este modelo é particularmente adequado para as complexas, distribuídas e dinâmicas redes de megaconstelações de satélites, onde um perímetro tradicional simplesmente não existe. Startups como a

**SpiderOak** estão liderando a aplicação de conceitos de confiança zero para proteger as comunicações via satélite.11

Coletivamente, essas inovações marcam uma transição de uma postura de defesa passiva e baseada em perímetro para uma abordagem proativa, preditiva e distribuída. O antigo modelo de "fortificar o castelo" em torno de estações terrestres tornou-se obsoleto diante da vastidão e interconexão das redes espaciais modernas. O novo paradigma combina a inteligência preditiva da IA 7, a proteção de dados antecipatória da criptografia quântica e pós-quântica 9, e o controle de acesso granular e distribuído das arquiteturas de confiança zero.12

**Tabela 3: Comparativo de Tecnologias de Criptografia para Aplicações Espaciais**

| Tecnologia | Princípio de Funcionamento | Vantagens no Contexto Espacial | Desafios/Limitações | Status de Implementação |
| --- | --- | --- | --- | --- |
| **AES-256** | Criptografia simétrica baseada em blocos, padrão da indústria. | Maturidade, alta velocidade, baixo custo computacional, amplamente adotado. | Vulnerável a ataques de futuros computadores quânticos. | Padrão da indústria, usado em quase todos os sistemas seguros. |
| **RSA** | Criptografia assimétrica baseada na dificuldade de fatorar grandes números. | Permite a troca segura de chaves e assinaturas digitais. | Vulnerável a ataques de futuros computadores quânticos, computacionalmente intensivo. | Amplamente utilizado para troca de chaves e autenticação. |
| **Criptografia Pós-Quântica (PQC)** | Novos algoritmos matemáticos projetados para resistir a ataques de computadores quânticos e clássicos. | Proteção proativa contra ameaças futuras, pode ser implementada em software/hardware existente. | Algoritmos ainda em fase de padronização, podem ter maior sobrecarga computacional. | Em desenvolvimento e padronização; implementações iniciais por startups (WISeSat). |
| **Distribuição de Chave Quântica (QKD)** | Usa os princípios da mecânica quântica para troca de chaves; a interceptação é detectável. | Segurança teoricamente perfeita, baseada nas leis da física, não em complexidade matemática. | Limitação de distância (em fibra), alta complexidade, custo e sensibilidade a perturbações. | Prova de conceito; satélites são a principal esperança para implementação global. |
| Fonte: Baseado em dados de 9 |  |  |  |  |  |

## **O Cenário Regulatório e Político**

A rápida evolução tecnológica e o aumento das ameaças no domínio espacial estão superando a capacidade dos frameworks legais e políticos de se adaptarem. Isso cria um ambiente complexo e fragmentado que os operadores espaciais devem navegar.

### **Frameworks Internacionais: Um Vácuo Legal**

A pedra angular do direito espacial, o **Tratado do Espaço Sideral de 1967**, foi redigido em uma era pré-digital e, portanto, não faz qualquer menção à cibersegurança.18 Embora estabeleça princípios fundamentais como o uso pacífico do espaço e a proibição de armas de destruição em massa, ele deixa uma vasta área cinzenta no que diz respeito a ciberataques. Essa ausência de um framework legal internacional claro para a atribuição de responsabilidade, a definição de um ato de guerra cibernética no espaço e as regras de engajamento cria um ambiente volátil, onde um ataque pode ser facilmente mal interpretado e escalar para um conflito cinético.48

Iniciativas mais recentes tentam preencher essa lacuna, mas enfrentam desafios:

* O **Tallinn Manual 2.0**, um estudo acadêmico influente, dedica um capítulo específico à aplicação do direito internacional existente às operações cibernéticas no espaço. Ele conclui que princípios fundamentais, como a proibição do uso da força e o respeito à soberania, se aplicam ao domínio espacial, mas sua natureza não vinculante limita seu impacto prático.50
* A **Lei de Ciber-Resiliência da União Europeia** é um passo significativo. Ela estabelece requisitos mínimos de segurança para todos os produtos com elementos digitais vendidos no mercado europeu. Isso terá um impacto direto em fabricantes de satélites, componentes e software que desejam operar na UE, forçando a adoção de práticas de "segurança por design".51

### **A Estratégia Brasileira: Um Despertar para a Soberania Digital**

O Brasil, que segundo levantamentos sofre mais de 100 bilhões de tentativas de ataques cibernéticos anualmente 52, está tomando medidas concretas para fortalecer sua postura de cibersegurança, inclusive no domínio espacial.

* A instituição da **Política Nacional de Cibersegurança (PNCiber)** através do Decreto 11.856 em dezembro de 2023 foi um marco. A PNCiber tem como objetivo orientar a atividade de segurança cibernética no país, promover o desenvolvimento de tecnologias nacionais, garantir a confidencialidade e a integridade dos dados e fomentar a capacitação profissional na área.13
* Para implementar essa política, foi criado o **Comitê Nacional de Cibersegurança (CNCiber)**, um órgão multissetorial com representação do governo, da sociedade civil e do setor empresarial, coordenado pelo Gabinete de Segurança Institucional (GSI).13
* Um dos movimentos mais estratégicos e recentes foi a **integração da Agência Espacial Brasileira (AEB) como órgão associado ao Sistema Brasileiro de Inteligência (Sisbin)** em maio de 2025.14 Este é um passo de enorme significado. Ele formaliza o papel da AEB como uma entidade de relevância para a segurança nacional e a inteligência, concedendo-lhe acesso a canais de comunicação seguros, inteligência sobre ameaças e um framework de colaboração para proteger os ativos espaciais do país. A cibersegurança é explicitamente reconhecida como uma das áreas de atuação da AEB que são críticas para a Política Nacional de Inteligência.14

A governança da cibersegurança espacial está, portanto, evoluindo de um vácuo legal internacional para um mosaico de regulamentações nacionais e regionais. Neste contexto, os movimentos do Brasil representam passos decisivos para a afirmação de sua soberania digital e espacial. A integração da AEB ao Sisbin sinaliza que o Brasil não mais encara o espaço apenas como um domínio científico ou comercial, mas como uma infraestrutura crítica para a segurança nacional, exigindo proteção no mais alto nível de inteligência do Estado. Para as empresas que operam no Brasil, isso provavelmente significará requisitos de segurança mais rigorosos, alinhados com os padrões de defesa e segurança nacional.

**Tabela 4: Marco Regulatório e Político - Principais Instrumentos e Relevância**

| Instrumento | Âmbito | Relevância para a Cibersegurança Espacial | Principais Disposições ou Lacunas |
| --- | --- | --- | --- |
| **Tratado do Espaço Sideral (1967)** | Internacional | Estabelece princípios de uso pacífico e responsabilidade estatal, mas não aborda ciberataques. | **Lacuna:** Ausência total de menção a cibersegurança, ameaças digitais ou guerra de informação. |
| **Tallinn Manual 2.0** | Internacional (Não Vinculante) | Aplica o direito internacional existente às operações cibernéticas no espaço, afirmando que leis de conflito armado se aplicam. | Fornece um framework interpretativo, mas não tem força de lei e não cria novas obrigações. |
| **Lei de Ciber-Resiliência (UE)** | Regional (UE) | Impõe requisitos de segurança por design para todos os produtos digitais, incluindo componentes de satélites, vendidos na UE. | Focada em produtos, pode não cobrir todos os aspectos dos serviços e operações espaciais. |
| **Política Nacional de Cibersegurança (Brasil)** | Nacional (Brasil) | Orienta a estratégia nacional, promove P&D local e cria um comitê (CNCiber) para governança. | Define as diretrizes; o impacto dependerá da implementação efetiva e da criação de normas específicas. |
| Fonte: Baseado em dados de 13 |  |  |  |  |

## **Desafios Futuros e Recomendações Estratégicas**

Apesar do crescimento robusto e da inovação tecnológica, o setor de cibersegurança espacial enfrenta desafios significativos que exigirão ação coordenada de todos os stakeholders.

### **Principais Desafios**

* **O Paradoxo do "New Space":** A mesma tendência que impulsiona o crescimento do setor — a rápida proliferação de megaconstelações de satélites (como Starlink e Kuiper) que utilizam componentes comerciais de baixo custo (COTS) — também aumenta exponencialmente a superfície de ataque. Gerenciar a segurança de milhares de satélites interconectados, cada um um potencial ponto de falha, é um desafio de uma ordem de magnitude maior do que proteger alguns poucos satélites soberanos de alto custo.1
* **A Ameaça Persistente dos Sistemas Legados:** Muitos satélites e grande parte da infraestrutura terrestre em operação hoje foram projetados e lançados décadas atrás, em uma época em que a cibersegurança não era um requisito de missão.23 Esses sistemas são caros e, muitas vezes, impossíveis de atualizar, representando vulnerabilidades persistentes que os atacantes podem explorar com relativa facilidade.25
* **Falta de Padrões Unificados:** A ausência de padrões de cibersegurança globais e unificados para o setor espacial leva a uma abordagem fragmentada. A postura de segurança pode variar drasticamente entre diferentes operadores e nações, criando elos fracos na cadeia de segurança global e aumentando o risco sistêmico para todos.22

### **Recomendações Estratégicas para Stakeholders**

Para navegar neste cenário complexo e garantir um futuro espacial seguro e resiliente, são necessárias ações estratégicas direcionadas a cada grupo de atores.

* **Para Governos e Agências Reguladoras (como a AEB):**
  + **Fomentar Padrões de Segurança:** Liderar o desenvolvimento e a implementação de padrões de segurança mínimos obrigatórios para todos os sistemas espaciais operando sob sua jurisdição. Isso deve incluir requisitos para "segurança por design" e gestão de vulnerabilidades ao longo de todo o ciclo de vida do ativo, alinhando-se a frameworks internacionais como a Lei de Ciber-Resiliência da UE.51
  + **Investir em Pesquisa e Desenvolvimento (P&D):** Alocar financiamento público para pesquisas em tecnologias defensivas de ponta, como IA para detecção de ameaças, criptografia pós-quântica e arquiteturas resilientes. A PNCiber do Brasil já prevê esse fomento.13
  + **Fortalecer a Colaboração:** Utilizar plataformas como o CNCiber e a recém-formalizada integração da AEB no Sisbin para aprofundar a colaboração público-privada e a cooperação internacional. O compartilhamento ágil e seguro de inteligência sobre ameaças é fundamental para uma defesa coletiva eficaz.14
* **Para a Indústria (Fabricantes e Operadores):**
  + **Adotar "Security by Design":** Integrar a cibersegurança desde a fase de concepção dos satélites e sistemas terrestres. A segurança não pode ser uma camada adicionada posteriormente; deve ser um componente fundamental da arquitetura do sistema.59
  + **Construir Resiliência, Não Apenas Proteção:** Projetar sistemas que possam não apenas resistir a ataques, mas também operar de forma degradada durante um ataque e se recuperar rapidamente. Isso envolve o uso de redundância, segmentação de rede e arquiteturas de confiança zero.12
  + **Educação e Treinamento Contínuo:** Investir na capacitação constante das equipes de operações e engenharia para que possam reconhecer, responder e mitigar ameaças cibernéticas. Exercícios de simulação, como o "Hack-a-Sat", devem se tornar uma prática padrão na indústria.28
* **Para Investidores:**
  + **Due Diligence de Cibersegurança:** Incorporar a avaliação da postura de cibersegurança como um fator crítico na análise de risco de qualquer investimento no setor espacial. Uma empresa com segurança fraca representa um risco não apenas operacional, mas também financeiro, de reputação e de responsabilidade legal.
  + **Identificar Oportunidades de Crescimento:** Reconhecer que as empresas que lideram em inovação de cibersegurança espacial — sejam as startups ágeis ou os gigantes da defesa que se adaptam — representam uma oportunidade de investimento significativa. Dado o crescimento robusto e a criticidade do setor, a segurança é um facilitador direto do valor a longo prazo.34

#### Referências citadas

1. Tamaño, participación, tendencia y pronóstico del mercado de ..., acessado em julho 5, 2025, <https://www.gminsights.com/es/industry-analysis/space-cybersecurity-market>
2. Space Cybersecurity Market Size, Share, Trend & Forecast, 2034, acessado em julho 5, 2025, <https://www.gminsights.com/industry-analysis/space-cybersecurity-market>
3. IA e pirataria espacial: ciberataques no espaço ameaçam vida na ..., acessado em julho 5, 2025, <https://fastcompanybrasil.com/tech/ia-e-pirataria-espacial-ciberataques-no-espaco-ameacam-vida-na-terra/>
4. Ativos baseados no espaço não são imunes a ataques cibernéticos ..., acessado em julho 5, 2025, <https://itforum.com.br/ativos-baseados-no-espaco-nao-sao-imunes-a-ataques-ciberneticos/>
5. Comunicações por satélite são novo alvo de ataques cibernéticos - TD | O ecossistema da Transformação Digital, acessado em julho 5, 2025, <https://transformacaodigital.com/seguranca/tecnologia/comunicacoes-por-satelite-sao-novo-alvo-de-ataques-ciberneticos/>
6. The Ungoverned Space of US Space-Cyber Governance, acessado em julho 5, 2025, <https://www.cigionline.org/articles/the-ungoverned-space-of-us-space-cyber-governance/>
7. Cibersegurança na era da Inteligência Artificial: desafios e soluções - SiDi, acessado em julho 5, 2025, <https://www.sidi.org.br/pt-br/blog/ciberseguranca-na-era-da-inteligencia-artificial-desafios-e-solucoes>
8. AI for satellite anomaly detection: on-ground operational feedback and development of on-board experiments, acessado em julho 5, 2025, <https://iafastro.directory/iac/archive/browse/IAC-22/B6/2/71168/>
9. Segurança da era espacial como os satélites, acessado em julho 5, 2025, <https://w3b.com.br/seguranca-da-era-espacial-como-os-satelites-poderiam-estender-a-criptografia-quantica-globalmente/>
10. WISeSat.Space announces new 2025 satellite launches with post-quantum-ready technology | IoT Now News & Reports, acessado em julho 5, 2025, <https://www.iot-now.com/2025/02/07/149486-wisesat-space-announces-new-2025-satellite-launches-with-post-quantum-ready-technology/>
11. Space Cybersecurity Companies - Top Companies List of Space ..., acessado em julho 5, 2025, <https://www.marketsandmarkets.com/ResearchInsight/space-cybersecurity-companies.asp>
12. Cybersecurity in Orbit Empowering the Future of Space and Satellites Security, acessado em julho 5, 2025, <https://bisresearch.com/insights/cybersecurity-in-orbit-empowering-the-future-of-space-and-satellites-security>
13. Política Nacional de Cibersegurança já está vigorando no Brasil ..., acessado em julho 5, 2025, <https://agenciabrasil.ebc.com.br/geral/noticia/2023-12/politica-nacional-de-ciberseguranca-ja-esta-vigorando-no-brasil>
14. Agência Espacial Brasileira será órgão associado do Sisbin ..., acessado em julho 5, 2025, <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/agencia-espacial-brasileira-sera-orgao-associado-do-sisbin>
15. Glossário - CNCS, acessado em julho 5, 2025, <https://www.cncs.gov.pt/pt/glossario/>
16. Cibersegurança Espacial: A próxima fronteira - BPO Innova, acessado em julho 5, 2025, <https://bpoinnova-sp.com/ciberseguranca-espacial-a-proxima-fronteira/>
17. Cibersegurança: conceito, tipos e benefícios - PUCRS Online, acessado em julho 5, 2025, <https://online.pucrs.br/blog/public/ciberseguranca-conceito-tipos-beneficios>
18. Bombas orbitales y misiles antisatélite: una breve historia de la guerra en el espacio, acessado em julho 5, 2025, <https://www.lavanguardia.com/historiayvida/historia-contemporanea/20240220/9523413/bombas-orbitales-misiles-antisatelite-breve-historia-guerra-espacio.html>
19. Por que se importar com a cibersegurança de satélites? - Abrasat, acessado em julho 5, 2025, <https://abrasat.org.br/2022/03/24/por-que-se-importar-com-a-ciberseguranca-de-satelites/>
20. Cyberspace - Wikipedia, acessado em julho 5, 2025, <https://en.wikipedia.org/wiki/Cyberspace>
21. Cibersegurança no Domínio Espacial - CryptoID, acessado em julho 5, 2025, <https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/ciberseguranca-no-dominio-espacial/>
22. Cibersegurança no espaço | Blog oficial da Kaspersky, acessado em julho 5, 2025, <https://www.kaspersky.com.br/blog/cybersecurity-in-outer-space-2/18922/>
23. Sistemas legados: desafios, soluções e modernização digital - SoftDesign, acessado em julho 5, 2025, <https://softdesign.com.br/blog/desafios-e-solucoes-para-sistemas-legados-como-modernizar-e-garantir-competitividade/>
24. 10 ameaças cibernéticas emergentes para 2030 - HSC Labs, acessado em julho 5, 2025, <https://hsclabs.com/pt-br/10-ameacas-ciberneticas-emergentes-para-2030/>
25. Conheça 3 problemas com sistemas legados e como resolver! - Blog Cronapp, acessado em julho 5, 2025, <https://blog.cronapp.io/problemas-com-sistema-legado/>
26. The Need for Space Defence - ST Engineering Antycip, acessado em julho 5, 2025, <https://steantycip.com/blog/the-need-for-space-defence/>
27. Satélite artificial - Wikipedia, la enciclopedia libre, acessado em julho 5, 2025, <https://es.wikipedia.org/wiki/Sat%C3%A9lite_artificial>
28. Hackers invadem satélite da ESA e mostram vulnerabilidades do setor espacial, acessado em julho 5, 2025, <https://www.internationalit.com/post/hackers-invadem-sat%C3%A9lite-da-esa-e-mostram-vulnerabilidades-do-setor-espacial>
29. Guerra espacial - Wikipedia, la enciclopedia libre, acessado em julho 5, 2025, <https://es.wikipedia.org/wiki/Guerra_espacial>
30. La "guerra espacial" ya es una realidad y la están librando EEUU, Rusia y China con un arma particular: sus satélites - Xataka, acessado em julho 5, 2025, <https://www.xataka.com/espacio/guerra-espacial-realidad-estan-librando-eeuu-rusia-china-arma-particular-sus-satelites>
31. Ataque a los satélites: la creciente carrera armamentística en el espacio - Yahoo, acessado em julho 5, 2025, <https://es-us.noticias.yahoo.com/ataque-sat%C3%A9lites-creciente-carrera-armament%C3%ADstica-193458208.html>
32. Crescimento do Mercado de Cibersegurança, Compartilhar, Relatório para 2030, acessado em julho 5, 2025, <https://www.sphericalinsights.com/pt/reports/cybersecurity-market>
33. U.S. Space Cybersecurity Market Size | Industry Report, 2033, acessado em julho 5, 2025, <https://www.grandviewresearch.com/industry-analysis/us-space-cybersecurity-market-report>
34. Cibersegurança espacial: a próxima fronteira - Forbes Brasil, acessado em julho 5, 2025, <https://forbes.com.br/forbes-tech/2023/05/ciberseguranca-espacial-a-proxima-fronteira/>
35. Cybersecurity for Space | Thales Group, acessado em julho 5, 2025, <https://www.thalesgroup.com/en/cybersecurity-space>
36. WISeSat.Space Announces New 2025 Satellite Launches with Post-Quantum-Ready Technology - WISeKey, acessado em julho 5, 2025, <https://www.wisekey.com/press/wisesat-space-announces-new-2025-satellite-launches-with-post-quantum-ready-technology/>
37. California startup aims to give satellites minds of their own - Aerospace America - AIAA, acessado em julho 5, 2025, <https://aerospaceamerica.aiaa.org/california-startup-aims-to-give-satellites-minds-of-their-own/>
38. News - 21Software LLC, acessado em julho 5, 2025, <https://21sw.us/news/>
39. Inteligência Artificial na cibersegurança: a nova aliada das empresas | EY - Brasil, acessado em julho 5, 2025, <https://www.ey.com/pt_br/insights/cybersecurity/inteligencia-artificial-na-ciberseguranca-a-nova-aliada-das-empresas>
40. Applying Machine Learning to Routine Satellite Ground Segment Operations by Means of Automated Anomaly Detection, acessado em julho 5, 2025, <https://elib.dlr.de/196102/1/Applying_ML_to_Satellite_Ground_Segment_Operations.pdf>
41. An innovative AI-based framework for on-ground anomaly detection and root cause analysis - SpaceOps, acessado em julho 5, 2025, <https://star.spaceops.org/2023/user_manudownload.php?doc=336__vtj1ayxe.pdf>
42. Applying Machine Learning to Routine Satellite Ground Segment Operations by Means of Automated Anomaly Detection - eucass, acessado em julho 5, 2025, <https://www.eucass.eu/component/docindexer/?task=download&id=7118>
43. O impacto da inteligência artificial na cibersegurança - WeLiveSecurity, acessado em julho 5, 2025, <https://www.welivesecurity.com/pt/antimalware-day/o-impacto-da-inteligencia-artificial-na-ciberseguranca/>
44. O futuro da cibersegurança em tempos de inteligência artificial | TI INSIDE Online, acessado em julho 5, 2025, <https://tiinside.com.br/17/09/2024/o-futuro-da-ciberseguranca-em-tempos-de-inteligencia-artificial/>
45. Visão geral da criptografia do Azure | Microsoft Learn, acessado em julho 5, 2025, <https://learn.microsoft.com/pt-br/azure/security/fundamentals/encryption-overview>
46. Criptografia padrão em repouso | Documentation - Google Cloud, acessado em julho 5, 2025, <https://cloud.google.com/docs/security/encryption/default-encryption?hl=pt-br>
47. Satellite Encryption Techniques - Yesway Communications - Two Way Radio, acessado em julho 5, 2025, <https://yesway.co.uk/satellite-encryption-techniques/>
48. Cybersecurity in the Context of International Space Agreements, acessado em julho 5, 2025, <https://www.thesign.media/blog/cybersecurity-in-the-context-of-international-space-agreements>
49. Cybersecurity Challenges in Outer Space: Innovation, Collaboration and Legal Reforms - SciSpace, acessado em julho 5, 2025, <https://scispace.com/pdf/cybersecurity-challenges-in-outer-space-innovation-2cqxma3xmrfg.pdf>
50. Space law (Chapter 10) - Tallinn Manual 2.0 on the International ..., acessado em julho 5, 2025, <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/space-law/77A97C09EBA1C9541C40639CFCF7EEBE>
51. De babá eletrônica a games: Europa terá lei de garantia da cibersegurança - TeleSíntese, acessado em julho 5, 2025, <https://telesintese.com.br/de-baba-eletronica-a-games-europa-tera-lei-de-garantia-da-ciberseguranca/>
52. Política Nacional de Cibersegurança: um avanço para o Brasil - Lumiun, acessado em julho 5, 2025, <https://www.lumiun.com/blog/politica-nacional-de-ciberseguranca-um-avanco-para-o-brasil/>
53. Política Nacional de Cibersegurança (PNCiber) - Portal Gov.br, acessado em julho 5, 2025, <https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/politicas-nacionais/copy_of_politica-nacional-de-seguranca-da-informacao-pnsi>
54. CNCiber (Comitê Nacional de Cibersegurança) — Gabinete de Segurança Institucional, acessado em julho 5, 2025, <https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber>
55. Programação - SpaceBR Show, acessado em julho 5, 2025, <https://spacebrshow.com/programacao/>
56. Os desafios de um Sistema Legado - Go44, acessado em julho 5, 2025, <https://www.go44.co/os-desafios-de-um-sistema-legado/>
57. Europa propõe marco regulatório comum para atividades espaciais - TELETIME News, acessado em julho 5, 2025, <https://teletime.com.br/26/06/2025/europa-propoe-marco-regulatorio-comum-para-atividades-espaciais/>
58. Projeção de US$ 49,4 Bilhões: O Futuro da Cibersegurança até 2028 - International IT, acessado em julho 5, 2025, <https://www.internationalit.com/post/proje%C3%A7%C3%A3o-de-us-49-4-bilh%C3%B5es-o-futuro-da-ciberseguran%C3%A7a-at%C3%A9-2028>
59. Space security for Europe, acessado em julho 5, 2025, <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_29_0.pdf>
60. Devoteam Cyber Trust: tendências de cibersegurança para 2025 - APDC, acessado em julho 5, 2025, <https://www.apdc.pt/noticias/atualidade-internacional/devoteam-cyber-trust-tendencias-de-ciberseguranca-para-2025>