ESCOLA SUPERIOR DE GUERRA

EVERT LEAL RAMOS

SISTEMA DE ENLACE SEGURO ENTRE NAÇÕES AMIGAS:

proposta de um framework nacional de comunicação estratégica

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Prof. Ricardo Ferre Lacerda Ferreira

Rio de Janeiro
2024

CSSDC2023 ESG

Documento assinado digitalmente
gov.br
EVERT LEAL RAMOS
Data: 23/10/2024 14:25:28-0300
Verifique em https://validar.iti.gov.br

_____

EVERT LEAL RAMOS

RESUMO

O presente ensaio discute a importância da cibersegurança nas comunicações estratégicas entre nações amigas, abordando a necessidade de ferramentas robustas e seguras para garantir a integridade e a confidencialidade das informações trocadas em contextos de crise. Baseando-se no *National Institute of Standards and Technology Cybersecurity Framework*, o estudo explora soluções de código aberto, como o Nextcloud e o Element, que oferecem criptografia ponta a ponta e descentralização, assegurando alta segurança. Além disso, destaca-se a relevância de um framework nacional de segurança da informação como elemento estratégico geopolítico, capaz de posicionar o Brasil como um ator central na cibersegurança global, promovendo normas nacionais, confiança diplomática e acordos comerciais. A criação de parcerias público-privadas e a implementação de auditorias contínuas são recomendadas para garantir o aprimoramento contínuo das políticas e práticas de segurança.

Palavras-chave: cibersegurança; framework de segurança; código aberto; comunicações estratégicas.

ABSTRACT

This essay discusses the importance of cybersecurity in strategic communications between allied nations, emphasizing the need for robust and secure tools to ensure the integrity and confidentiality of information exchanged during crises. Based on the National Institute of Standards and Technology Cybersecurity Framework the study explores open-source solutions such as Nextcloud and Element, which provide end-to-end encryption and decentralization, ensuring high levels of security. Furthermore, it highlights the relevance of a national cybersecurity framework as a geopolitical strategy, positioning Brazil as a central actor in global cybersecurity, promoting national standards, diplomatic trust, and trade agreements. The creation of public-private partnerships and the implementation of continuous audits are recommended to ensure ongoing improvement of security policies and practices.

Keywords*: cybersecurity; security framework; open source; strategic communications.*

1. INTRODUÇÃO

No contexto de um mundo cada vez mais interconectado e dinâmico, onde os eventos globais se desdobram com uma velocidade sem precedentes, a necessidade de respostas rápidas e coordenadas se torna essencial. Crises internacionais, como pandemias, ameaças terroristas, conflitos armados e emergências climáticas, requerem, dos líderes mundiais, estratégias de comunicação específicas para resoluções pacíficas, conforme afirma Asențe (2023). Nesses cenários, a cibersegurança desempenha um papel fundamental, garantindo que a comunicação imediata e segura entre líderes seja possível para a tomada de decisões estratégicas e a coordenação de ações conjuntas.

Como destaca a Casa Branca em seu relatório nacional de estratégias de cibersegurança:

> A cibersegurança é essencial para o funcionamento básico da nossa economia, a operação de nossa infraestrutura crítica, a força da nossa democracia e instituições democráticas, a privacidade de nossos dados e comunicações, e para a nossa defesa nacional (*United States*, 2023, tradução nossa).

Dessa forma, a cibersegurança transcende preocupações técnicas, assumindo papel estratégico na governança nacional e nas relações internacionais. Ao assegurar a integridade das infraestruturas críticas, como redes de energia, sistemas financeiros e comunicações, torna-se um pilar fundamental para a estabilidade global.

Além disso, a cibersegurança é fundamental para a defesa dos processos democráticos e a proteção da soberania nacional, especialmente em um cenário onde ataques cibernéticos podem desestabilizar governos e comprometer a segurança coletiva, conforme pontua Timmers (2019). A proteção da confidencialidade e a integridade das informações trocadas entre líderes e nações se revela, portanto, vital para a gestão de crises e a manutenção da paz.

A interseção entre cibersegurança e política internacional destaca a necessidade de cooperação entre Estados, empresas e organizações multilaterais para mitigar riscos e promover um ambiente global mais seguro e resiliente.

Isso envolve não apenas a implementação de tecnologias avançadas de criptografia, mas também a criação de políticas, legislações e estruturas organizacionais que sustentem a segurança da informação de forma abrangente.

Considerando a crescente necessidade de fortalecer a segurança nas comunicações entre chefes de estado, este estudo propõe uma ferramenta para ampliar a proteção dessas interações críticas.

Este estudo se concentra em explorar as principais diretrizes de cibersegurança, com base nas recomendações do Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* - NIST), para desenvolver ou adaptar aplicações de comunicações que exigem alta confiabilidade e segurança. Em particular, busca-se propor uma solução que garanta a proteção das comunicações entre líderes mundiais, mitigando riscos associados a espionagem e outras ameaças cibernéticas, contribuindo para a segurança diplomática em um cenário global cada vez mais complexo.

2. REFERENCIAL TEÓRICO

A cibersegurança é uma disciplina complexa que envolve mais do que apenas implementação de novas tecnologias, abrangendo também políticas, processos e práticas destinadas à proteção da informação contra acessos não autorizados, interrupções e destruições. Essa integração de disciplinas organizadas e estruturadas é o que Taherdoost (2022) denomina como um *framework*.

Conforme discutido por Taherdoost (2022), framework de segurança cibernética é um guia abrangente que define a estrutura necessária para se proteger contra ataques cibernéticos. Esse modelo oferece flexibilidade aos usuários, permitindo que adotem partes específicas ou o framework inteiro. Além disso, Taherdoost destaca que tais frameworks buscam harmonizar políticas, abordagens e soluções tecnológicas para enfrentar e mitigar problemas e riscos associados à segurança digital, garantindo a resiliência cibernética e a proteção de dados em diversos setores.

Complementando essa visão, a Estrutura de Cibersegurança do NIST (NIST *Cybersecurity Framewor*k - NIST CSF) proporciona uma abordagem igualmente

abrangente para a gestão de riscos cibernéticos. Ele oferece uma taxonomia de resultados de segurança que pode ser adaptada por qualquer organização, independentemente do setor, para aprimorar suas práticas de segurança e gerenciar ameaças de forma mais eficaz (*National Institute of Standards and Technology,* 2024).

Somando às diretrizes amplas fornecidas pelo NIST CSF (*National Institute of Standards and Technology*, 2020a), o NIST SP 800-53 oferece uma abordagem detalhada e estruturada para o gerenciamento de riscos de segurança e privacidade em organizações. Este documento apresenta um conjunto abrangente de controles de segurança e privacidade propostos como essenciais na proteção de informações sensíveis e continuidade das operações organizacionais.

O NIST SP 800-53 reforça ainda a importância de uma abordagem estruturada para gerenciamento de riscos de segurança e privacidade, recomendando que organizações estabeleçam programas de gerenciamento de riscos, por meio de controles de segurança e privacidade adequados às necessidades de missão e negócios.

A Agência da União Europeia para a Cibersegurança (*European Union Agency for Cybersecurity* - ENISA) enfatiza a necessidade de diretrizes claras para proteção de infraestruturas críticas, tanto em escala nacional quanto internacional. A agência destaca que setores como telecomunicações, energia, saúde e transporte dependem fortemente de sistemas de informação e são frequentemente alvos de ciberataques. (*European Union Agency For Cybersecurity*, 2024)

Além disso, a prática de cibersegurança é continuamente corroborada por órgãos como a Agência de Segurança de Cibersegurança e Infraestrutura (*Cybersecurity & Infrastructure Security Agency* - CISA), que destaca a necessidade de fortalecer as comunicações críticas. O Plano Estratégico 2023-2025 da CISA pontua, diversas vezes, a importância de aprimorar o sistema de comunicação para enfrentar ameaças à segurança da infraestrutura e proteger comunicações de emergências. Como evidenciado nas citações a seguir:

> Para melhorar a proteção da infraestrutura crítica contra ameaças, perigos e riscos, a CISA fornece aos interessados orientações e assistência em segurança e mitigação de riscos. Para aprimorar e expandir nosso impacto na redução de riscos, ofereceremos expertise e medidas práticas para lidar

> com ameaças à segurança da infraestrutura e fortalecer os sistemas de comunicações de emergência.
>
> A CISA medirá a eficácia e a adoção das orientações de segurança física, comunicações de emergência e cibersegurança da CISA para os interessados.
>
> Para atender melhor às suas necessidades, precisamos dimensionar adequadamente os principais programas da CISA e as ofertas relacionadas a riscos em cibersegurança, segurança da infraestrutura e comunicações de emergência para atender à crescente demanda de nossos interessados (*Cybersecurity And Infrastructure Security Agency*, 2022, tradução nossa).

Essas diretrizes enfatizam a necessidade de uma abordagem integrada à segurança das comunicações de emergência, o que é particularmente relevante no contexto de interações diplomáticas de alto nível em caso de crise, por exemplo.

A escolha do NIST como base para este estudo se deve à sua ampla aceitação e adaptabilidade. Desenvolvido em parceria com o setor privado e agências governamentais dos Estados Unidos, o NIST CSF é um dos frameworks mais robustos e flexíveis, permitindo que organizações de diferentes portes e setores adotem e adaptem suas diretrizes conforme necessidades específicas.

Outro fator relevante é a natureza orientada a resultados do framework. O NIST não apenas descreve como implementar soluções de segurança, mas fornece diversas práticas que permitem as organizações priorizem esforços e melhorem continuamente suas defesas contra ameaças cibernéticas.

Essa abordagem flexível facilita a adaptação às diferentes realidades organizacionais, sendo aplicável em cenários diplomáticos, militares, empresariais e de infraestrutura crítica. Assim a implementação do NIST CSF e suas diretrizes possibilita a construção de políticas públicas e sistemas resilientes que atendam às exigências de segurança de missão crítica como as comunicações estratégicas entre nações amigas.

2.1. Estrutura de Cibersegurança do NIST (NIST Cybersecurity Framework - NIST CSF)

Este framework pode ajudar as organizações a gerenciar e reduzir seus riscos ao iniciar ou melhorar seu programa de cibersegurança, conforme NIST (2024).

Figura 1 - Representação das Funções do NIST CSF em formato de roda, destacando a relação interdependente entre Governança, Identificação, Proteção, Detecção, Resposta e Recuperação.

Fonte: *National Institute of Standards and Technology*, 2024

O NIST CSF descreve resultados específicos que as organizações podem alcançar para enfrentar os riscos, integrando-se perfeitamente com as diretrizes de segurança das comunicações como destacadas pelo CISA. O NIST CSF fornece uma estrutura organizada em seis funções essenciais, conforme figura 1: Governança, Identificação, Proteção, Detecção, Resposta e Recuperação. Essas funções cobrem todas as etapas necessárias para uma gestão eficaz da cibersegurança, desde a criação de políticas até a recuperação de incidentes.

Essas funções essenciais do NIST CSF ganham ainda mais relevância quando analisadas à luz das discussões teóricas sobre frameworks de segurança cibernética.

Posthumus e Solms (2004, tradução nossa) observam que "integrar a segurança da informação à governança corporativa por meio de um framework de governança de segurança da informação (ISG) é crucial para garantir comunicações seguras."

Outros autores reafirmam que a importância de um framework de segurança se torna ainda mais evidente quando consideramos a vulnerabilidade dos serviços web, onde a alta exposição a ataques pode resultar em consequências catastróficas para os serviços implantados (Oliveira *et. al*., 2020). O NIST CSF, com sua abordagem estruturada e abrangente, pode ajudar a mitigar esses riscos, garantindo a segurança das comunicações e a integridade dos serviços implantados.

A importância de implementar o NIST CSF se destaca em diversos contextos, onde a adaptabilidade e a atenção às questões de segurança e privacidade são cruciais, como afirmam Mothukuri *et. al*. (2021).

A flexibilidade do NIST CSF permite que ele seja integrado a diferentes soluções tecnológicas, incluindo aquelas baseadas em software de código aberto. De fato, o framework incentiva o uso de ferramentas que não apenas fortalecem a segurança cibernética, mas também promovem transparência e colaboração – características fundamentais dos Software de Código Aberto (*Open Source Software* - OSS). Nesse contexto, a utilização de OSS se destaca como uma estratégia eficaz para implementar as diretrizes do NIST CSF, especialmente devido à sua flexibilidade, personalização e capacidade de auditoria pública.

2.2. Software de Código Aberto

Linåker *et. al*. (2023) destacam que apesar do crescente uso do Software de Código Aberto (*Open Source Software* - OSS) por grandes empresas em escala global, sua maturidade no setor público ainda é limitada. Os autores observam que enquanto o OSS se consolidou como um componente fundamental em soluções comerciais e infraestruturas digitais compartilhadas, sua adoção no setor público permanece em estágio embrionário. Isso se deve a uma série de barreiras regulatórias, culturais e de capacidade institucional que dificultam sua plena incorporação. Por fim concluem Linåker *et. al.* que embora a presença do OSS seja amplamente encontrada em indústrias privadas, ainda há um caminho significativo a ser percorrido para que o setor público possa explorar todo o seu potencial transformador.

O sistema operacional Linux é um exemplo do sucesso do OSS. Conforme relatado por Torvalds e Diamond (2001), o Linux foi criado em 1991 por Linus Torvalds, um estudante de ciência da computação da Finlândia, que inicialmente desenvolveu o núcleo do sistema (kernel) como um projeto pessoal. Inspirado pelo sistema operacional Unix, Torvalds tinha o objetivo de criar uma alternativa gratuita e aberta que pudesse ser usada e modificada livremente por outros desenvolvedores.

Com a abertura do código-fonte para a comunidade, o Linux rapidamente evoluiu, contando com contribuições de programadores ao redor do mundo. Essa colaboração aberta se tornou um marco para o desenvolvimento de software de código aberto, levando o Linux a ser amplamente utilizado em servidores, dispositivos móveis e infraestruturas críticas.

Além de sua flexibilidade e capacidade de adaptação, o OSS, exemplificado pelo Linux, apresenta vantagens significativas em termos de segurança cibernética. Cowan (2003) destaca que o código aberto permite que tanto defensores quanto atacantes tenham maior controle sobre a segurança do sistema, mas tecnologias de aprimoramento de segurança podem capacitar os defensores a melhorar suas medidas de proteção.

O desenvolvimento do kernel do Linux, conforme descrito por Moon e Sproull (2000), demonstra como um modelo colaborativo e distribuído pode ser altamente eficiente para a criação de software robusto e seguro. Linus Torvalds, ao abrir o código para contribuições globais, estabeleceu uma base técnica sólida que permitiu à comunidade de desenvolvedores identificar e corrigir vulnerabilidades rapidamente. Essa abordagem promoveu a criação de um sistema de alto desempenho e resiliente, capaz de competir com alternativas proprietárias e, ao mesmo tempo, atender a necessidades críticas, como as de segurança em infraestruturas sensíveis.

A adoção do Linux como solução OSS demonstra que o código aberto pode oferecer níveis de confiabilidade e segurança comparáveis, ou até superiores, aos softwares proprietários, consolidando-se como uma escolha estratégica para sistemas que exigem altos padrões de segurança cibernética (Yaswinski; Chowdhury; Jochen, 2019).

Além das vantagens intrínsecas do OSS, seu alinhamento com frameworks de segurança como o NIST CSF fortalece ainda mais sua aplicabilidade, uma vez que este framework oferece uma abordagem estruturada para gerenciar riscos de segurança cibernética, e o OSS, encaixa-se perfeitamente nesse contexto. O NIST CSF recomenda o uso de soluções flexíveis e adaptáveis que possam ser personalizadas para diferentes contextos. O código aberto, com sua transparência e capacidade de adaptação contínua, atende aos requisitos do framework, proporcionando um nível elevado de controle sobre a segurança e a integridade das comunicações críticas, especialmente em situações de alta sensibilidade entre nações amigas.

Adicionalmente, o NIST CSF destaca a importância da identificação e mitigação contínua de ameaças emergentes, algo intrinsecamente facilitado pelo modelo colaborativo de desenvolvimento do OSS. Ferramentas de código aberto, auditadas globalmente, permitem não apenas uma rápida resposta a vulnerabilidades, mas também o desenvolvimento de soluções inovadoras que podem ser aplicadas em ambientes diplomáticos e de segurança, garantindo que as comunicações estratégicas estejam sempre protegidas contra ataques cibernéticos. Assim, o OSS, quando bem implementado, torna-se um elemento central nas estratégias de segurança de estados e organizações internacionais.

2.3. Soluções Recomendadas

Com base nas vantagens do software de código aberto, como o Linux, e sua compatibilidade com frameworks de segurança como o NIST CSF, é possível identificar ferramentas OSS específicas que oferecem alto nível de segurança e adaptabilidade. Dentre elas, destacam-se o Nextcloud e o Element, soluções que oferecem funcionalidades robustas para comunicações estratégicas e colaboração segura, e que serão discutidas a seguir.

i. NextCloud (nextcloud.com)

O Nextcloud é uma plataforma de código aberto (OSS) para armazenamento, colaboração em nuvem e comunicação, licenciada sob a GNU *Affero General Public License v3.0* (AGPLv3)[1]. Essa licença permite que o código-fonte seja modificado para uso interno, sem a necessidade de compartilhar as alterações publicamente.

A segurança das comunicações e do armazenamento no Nextcloud é implementada com criptografia ponta a ponta (E2EE). Nesse modelo, os arquivos são criptografados diretamente no dispositivo do usuário antes de serem enviados para o servidor, assegurando que apenas os destinatários autorizados possam acessá-los. Isso garante que, mesmo que terceiros interceptem os dados durante a transmissão, não poderão decifrá-los sem as chaves de criptografia apropriadas, as quais são mantidas pelos usuários.

O Padrão de Criptografia Avançada (*Advanced Encryption Standard* - AES-256) é o algoritmo utilizado na criptografia de arquivos do Nextcloud, sendo considerado um dos padrões de segurança mais robustos. Ele é amplamente utilizado em protocolos de segurança, como o Segurança da Camada de Transporte. (*Transport Layer Security* - TLS), conforme padronizado pela Força-Tarefa de Engenharia da Internet (The Internet Engineering Task Force – IETF) nos memorandos RFC 5246 (The Internet Engineering Task Force, 2008) e RFC 8446 (The Internet Engineering Task Force, 2018) e documentado pelo OpenSSL[2], que é um conjunto de ferramentas e bibliotecas para implementar protocolos de segurança, como TLS, utilizado para criptografar comunicação na internet, garantindo a segurança e a privacidade dos dados transmitidos entre servidores e clientes.

Para comunicações de áudio e vídeo, o Nextcloud utiliza Comunicação em Tempo Real pela Web (*Web Real-Time Communication* - WebRTC), tecnologia que permite a comunicação em tempo real diretamente no navegador. O WebRTC implementado pelo NextCloud é protegido por criptografia Protocolo de Transporte em Tempo Real Seguro (*Datagram Transport Layer Security e Secure Real-Time*

[1] https://www.gnu.org/licenses/agpl-3.0.en.html
[2] https://openssl.org/

Transport Protocol - DTLS-SRTP), buscando garantir a segurança de ponta a ponta nas comunicações.

Além da proteção criptográfica, o NextCloud permite que as organizações implementem sua própria infraestrutura de hospedagem, seja de forma auto-hospedado (*self-hosted)* ou local (*on-premise)*, garantindo soberania total sobre os dados. Essa arquitetura oferece controle absoluto sobre o armazenamento e processamento de informações sensíveis, assegurando que nenhuma entidade externa tenha acesso aos dados, o que é essencial para organizações que buscam autonomia e segurança em seus sistemas de comunicação e colaboração.

O Nextcloud também oferece criptografia em repouso (*server-side encryption*), que protege os arquivos armazenados contra acessos não autorizados. Mesmo em caso de comprometimento do servidor, os dados permanecem criptografados, garantindo que informações sensíveis estejam sempre seguras, conforme descrito na documentação oficial do Nextcloud (2024).

De acordo com informações do site oficial da Nextcloud ([2024?]), a plataforma é utilizada por órgãos da União Europeia, como o Ministério do Interior da França e ITZBund, provedor de TI central do governo federal alemão (Informations Technik Zentrum Bund, [202-]).

ii. Element (element.io)

O Element é uma plataforma de código aberto (OSS) voltada para a comunicação segura e descentralizada, baseada no protocolo Matrix[3], que é protocolo de código aberto que permite a comunicação em tempo real, como mensagens instantâneas, chamadas de voz e vídeo, projetado para ser descentralizado e interoperável, permitindo que diferentes serviços e plataformas se comuniquem entre si. Um dos principais diferenciais do Element é sua arquitetura, que permite a troca de mensagens de forma segura e sem depender de um servidor central único. Cada organização ou usuário pode hospedar seu próprio servidor Matrix, garantindo que

[3] https://matrix.org/

comunicações fiquem sob total controle da entidade responsável, o que é essencial para governos e instituições que precisam de alta privacidade.

A segurança das comunicações no Element é garantida por meio de criptografia ponta a ponta (E2EE), método de criptografia que garante que apenas os comunicantes (remetente e destinatário) possam acessar e ler mensagens trocadas. Mesmo que os dados sejam interceptados por terceiros (como provedores de serviço ou *hackers*), eles não conseguirão decifrar o conteúdo, pois não possuem as chaves necessárias para a criptografia. Isso assegura a privacidade e a segurança das comunicações.

O sistema utiliza Olm e sua extensão Megolm[4], protocolo de criptografia de ponta a ponta (E2EE) projetado para o Matrix, desenvolvido especificamente para o uso em larga escala, como conversas em grupo. Esses protocolos garantem que as mensagens sejam criptografadas diretamente no dispositivo do usuário e só possam ser descriptografadas pelos destinatários autorizados. Isso impede que intermediários, incluindo servidores, possam acessar o conteúdo das mensagens, oferecendo uma camada de proteção robusta contra espionagem e interceptações.

Além disso, o Element integra a capacidade de verificação de identidade entre dispositivos, permitindo que os usuários confirmem as identidades uns dos outros através de códigos de segurança ou QR codes. Essa funcionalidade reforça a confiança nas comunicações, pois assegura que o remetente e o destinatário estão usando dispositivos autenticados. Isso é especialmente importante para comunicações sensíveis, como em negociações diplomáticas ou operações governamentais, onde a segurança da autenticidade do interlocutor é crítica.

A descentralização do Element também fortalece sua resiliência contra ataques cibernéticos. Como não depende de um único servidor central, o sistema é mais resistente a tentativas de censura, interrupções ou ataques direcionados a uma única infraestrutura. Cada servidor Matrix pode se comunicar com outros, criando uma rede interconectada, o que permite que as comunicações fluam mesmo em cenários onde partes da rede estão inacessíveis. Essa arquitetura distribuída é ideal para

[4] https://matrix.org/docs/matrix-concepts/end-to-end-encryption/

comunicações estratégicas entre nações amigas, onde é essencial que as trocas de informação permaneçam seguras e ininterruptas.

De acordo com o site da Element.io, o foco na segurança, a natureza de software de código aberto (OSS) e a alta capacidade de adaptação da plataforma têm atraído diversas organizações governamentais e de defesa. Isso permite que essas instituições criem suas próprias soluções de comunicação seguras, adaptadas às suas necessidades específicas, aproveitando o código aberto da plataforma para garantir que a privacidade e segurança sejam totalmente controladas internamente (Element, 2024).

Um exemplo notável de aplicação dessa customização é o desenvolvimento do NI2CE Messenger pela OTAN. Este aplicativo foi criado com base no Element.io para garantir a segurança das comunicações entre seus membros e parceiros. O NI2CE é hospedado localmente, o que assegura que a organização tenha controle total sobre os dados, e implementa criptografia ponta a ponta para proteger as informações sensíveis, garantindo que apenas os destinatários autorizados possam acessar os dados (NATO Innovation Hub, [2024?]).

Apesar de mencionarmos o Nextcloud como uma opção viável, para os fins deste trabalho optamos pelo Element.io devido à sua especialização em comunicações seguras e sua robustez na criptografia. O Element utiliza criptografia ponta a ponta (E2EE) especialmente projetada para proteger mensagens e colaborações em tempo real, tornando-o uma escolha mais adequada para comunicação estratégica.

Além disso, a recente implementação[5] da Vodozemac, biblioteca de software de código aberto que fornece uma implementação do protocolo Matrix em Rust, oferece melhorias substanciais em relação à versão anterior em C++, com um desempenho mais rápido e maior segurança, devido ao gerenciamento de memória mais eficiente da linguagem Rust. Isso torna o Element.io uma solução ainda mais confiável para proteger comunicações sensíveis e garantir a integridade dos dados.

[5] https://element.io/blog/meet-element-r-our-new-unified-crypto-implementation/

2.4. Implementação de Camadas Adicionais de Segurança em Soluções de Código Aberto

A implementação de soluções de código aberto, como o Element, para comunicações estratégicas seguras oferece inúmeras vantagens, principalmente no que diz respeito à flexibilidade, segurança e transparência. Essas plataformas não apenas permitem auditorias independentes, mas também possibilitam a personalização conforme as necessidades específicas de segurança nacional.

Apesar de ambas as soluções apresentadas possuírem criptografias robustas, como preconiza o NIST:

> A criptografia pode ser utilizada para apoiar uma variedade de soluções de segurança, incluindo a proteção de informações classificadas e informações não classificadas controladas, a provisão e implementação de assinaturas digitais, e a aplicação da separação de informações quando indivíduos autorizados possuem as devidas permissões, mas não têm as aprovações formais necessárias (*National Institute of Standards and Technology*, 2020b, tradução nossa).

Cowan (2003) destaca que a adição de camadas sobre um software *open source* aprimora a segurança do sistema.

Dado que o Element é uma plataforma de código aberto, sua flexibilidade permite adaptação para inserção de nova camada de criptografia com algoritmo de estado, garantindo que a solução possa se adequar às exigências específicas do governo brasileiro.

A criptografia de estado refere-se a algoritmos desenvolvidos ou aprovados por governos para proteger informações classificadas, conforme normas de segurança nacionais. A Agência Brasileira de Inteligência (ABIN) possui algoritmo de estado implementado em softwares como CriptoGOV e o cGOV2[6].

A integração dessas ferramentas no Element pode ser feita aplicando-se o algoritmo de criptografia de estado tanto no nível de comunicação (dados em trânsito) quanto no armazenamento de informações (dados em repouso), reforçando a proteção contra interceptações e acessos não autorizados.

> Zero trust é um paradigma de cibersegurança focado na proteção de recursos e na premissa de que a confiança nunca é concedida implicitamente, mas

[6] https://www.gov.br/abin/pt-br/assuntos/tecnologia/criptogov-e-cgov

> deve ser continuamente avaliada. A arquitetura de zero trust é uma abordagem de ponta a ponta para a segurança de recursos e dados empresariais, que abrange identidade (entidades humanas e não humanas), credenciais, gerenciamento de acesso, operações, pontos finais, ambientes de hospedagem e a infraestrutura interconectada. O foco inicial deve ser na restrição de recursos àqueles que têm necessidade de acesso e na concessão apenas dos privilégios mínimos necessários para realizar a missão (*National Institute of Standards and Technology*, 2020c, tradução nossa).

A citação do NIST SP 800-207 define o Zero Trust como um paradigma de cibersegurança centrado na proteção de recursos, onde a confiança nunca é concedida implicitamente, mas deve ser continuamente avaliada. Essa abordagem enfatiza uma visão de segurança de ponta a ponta que cobre todos os aspectos de uma infraestrutura de TI, desde a gestão de identidades e credenciais até a segurança de *endpoints*, ambientes de hospedagem e as infraestruturas interconectadas.

O conceito baseia-se no princípio de que nenhum usuário, dispositivo ou sistema deve ser considerado confiável por padrão, independentemente de estar dentro ou fora da rede corporativa. Em vez disso, todas as tentativas de acesso devem ser verificadas e monitoradas continuamente, reduzindo a superfície de ataque e melhorando a resiliência contra ameaças cibernéticas, uma abordagem especialmente crítica em ambientes empresariais complexos e distribuídos.

A implementação do modelo Zero Trust no Element reforçaria significativamente a segurança das comunicações estratégicas, especialmente quando combinada com camadas adicionais de criptografia. Ao integrar uma abordagem Zero Trust, o Element garantiria que cada solicitação de acesso — seja a dados em trânsito ou em repouso — seja continuamente verificada e autenticada, restringindo o acesso apenas às identidades autorizadas. Isso adicionaria uma camada crítica de segurança ao sistema, minimizando a possibilidade de acessos indevidos e fortalecendo a proteção contra ameaças internas e externas.

Além disso, ao aplicar o princípio de privilégio mínimo, o Element poderia limitar o acesso de cada entidade (usuário ou dispositivo) somente ao que é estritamente necessário para realizar sua função, aumentando ainda mais a resiliência da plataforma em ambientes complexos e distribuídos. Essa abordagem é reforçada pela visão de outros autores:

> A crescente complexidade das ameaças cibernéticas exige abordagens inovadoras para proteger ativos digitais e informações sensíveis. O paradigma Zero Trust oferece uma solução transformadora ao desafiar os modelos de segurança convencionais e enfatizar a verificação contínua e o acesso com o mínimo de privilégios (Ghasemshirazi; Shirvani; Alipour, 2023, tradução nossa).

Outro ponto relevante é a implementação dessas aplicações em um ambiente seguro. Recomenda-se o isolamento do sistema em uma rede fechada, como uma Rede Privada Virtual (*Virtual Private Network* - VPN), fora da superfície da web. Essa abordagem não apenas evita acessos não autorizados, mas também reduz significativamente o risco de interceptações externas.

Embora a VPN ofereça isolamento da superfície da web, o conceito Zero Trust pode ser aplicado para garantir que cada acesso dentro da rede seja autenticado e monitorado continuamente, reforçando a segurança em cada camada do sistema.

NIST enfatiza essa estratégia ao destacar a importância de uma estrutura em camadas:

> Implementar funções de segurança como uma estrutura em camadas, minimizando as interações entre as camadas do design e evitando qualquer dependência das camadas inferiores em relação à funcionalidade ou correção das camadas superiores (*National Institute of Standards and Technology,* 2020b, tradução nossa).

Adicionalmente, Zhang *et. al.* (2019) ressaltam que a adição de camadas de segurança, tanto física quanto digital, como o uso de firewalls e criptografia, melhora o desempenho geral de sigilo, protegendo redes contra interceptações e invasões externas. Ao aplicar esses conceitos a sistemas de comunicação baseados em software de código aberto, reforça-se ainda mais a resiliência e eficiência desses sistemas, especialmente em ambientes críticos.

Com essas estratégias integradas — criptografia robusta, arquitetura Zero Trust, VPNs seguras e camadas de segurança adicionais — o uso de soluções de código aberto como o Element pode oferecer um ambiente de comunicação altamente protegido, adequado para comunicações sensíveis e críticas entre nações.

3. CONSIDERAÇÕES FINAIS

A adoção de um framework nacional de segurança da informação vai além do fortalecimento das capacidades cibernéticas do Brasil, é também uma estratégia de relevância geopolítica que pode gerar repercussões significativas. Ao estabelecer um padrão de segurança robusto, o Brasil consolida-se como um ator relevante no cenário global de cibersegurança, aprimorando sua imagem como um parceiro confiável e seguro em comunicações estratégicas.

A implementação de um framework bem estruturado, como o NIST *Cybersecurity Framework*, adaptado às necessidades nacionais, oferece ao Brasil a oportunidade de criar normas que podem, eventualmente, transformar-se em referências regionais ou internacionais. Com essa estrutura o país assegura não apenas a integridade de suas informações estratégicas, mas também exerce influência na maneira como outros países abordam a cibersegurança.

A colaboração entre o setor público e privado é crucial para o sucesso da implementação do framework de segurança cibernética. Estabelecer parcerias público-privadas (PPPs) não só incentiva o desenvolvimento de soluções tecnológicas locais, mas também cria um ambiente propício para a troca de inteligência sobre ameaças cibernéticas.

A definição de padrões nacionais claros de segurança cibernética pode gerar um ambiente de maior confiança entre nações, especialmente no que diz respeito ao diálogo diplomático e à cooperação em temas sensíveis. A confiança é um pilar essencial nas relações internacionais, e garantir a segurança e a privacidade das comunicações é crucial para negociações eficazes e para a construção de alianças estratégicas.

A padronização dos processos de segurança cibernética no Brasil pode, portanto, atuar como um mecanismo de fortalecimento das relações internacionais, promovendo um ambiente de maior colaboração entre países que compartilham interesses comuns em segurança cibernética.

Além disso, a segurança da informação tem implicações diretas em acordos comerciais e investimentos. À medida que a proteção de dados sensíveis se torna uma prioridade global, países e empresas que adotam padrões rigorosos de

cibersegurança são vistos como parceiros mais atraentes e confiáveis. Isso pode atrair investimentos estrangeiros, além de proporcionar uma vantagem competitiva em negociações comerciais.

Um framework de segurança da informação também pode facilitar a coordenação entre países para enfrentar ameaças cibernéticas globais, como ataques de hackers, espionagem e campanhas de desinformação. A cibersegurança é um desafio transnacional que requer uma resposta colaborativa. Ao adotar padrões comuns e práticas de segurança, os países podem trabalhar juntos de forma mais eficaz para identificar, mitigar e responder a ameaças cibernéticas, reduzindo a probabilidade de incidentes e minimizando seu impacto quando ocorrerem.

Por fim, é essencial implementar um sistema de auditoria regular para avaliar a eficácia das medidas de segurança cibernética baseadas no framework. A auditoria contínua garante que políticas e tecnologias de cibersegurança permaneçam eficazes contra ameaças emergentes e que quaisquer vulnerabilidades sejam identificadas e corrigidas prontamente. Esse processo de avaliação e melhoria contínua é vital para manter a confiança e a integridade do sistema de segurança, assegurando que ele evolua em paralelo com o cenário de ameaças cibernéticas.

Em última análise, a criação e implementação de um framework nacional robusto de segurança da informação tem o potencial de fortalece a segurança interna do Brasil, mas também posicionar o país como um ator influente e confiável no cenário internacional, com implicações positivas para a diplomacia e comércio, criando oportunidades de liderança e cooperação em um mundo cada vez mais dependente da tecnologia.

Para garantir que essas iniciativas avancem de forma coordenada e eficaz, é necessário estabelecer um grupo de trabalho interministerial que reúna representantes dos principais órgãos envolvidos, como o Ministério das Relações Exteriores, Casa Civil, Gabinete de Segurança Institucional (GSI), Agência Brasileira de Inteligência (ABIN), Ministério da Defesa e outros atores estratégicos. Esse grupo seria responsável por alinhar políticas, identificar prioridades e desenvolver um plano integrado para a implementação do framework de segurança da informação.

Adicionalmente, caberá a esse grupo definir a autoridade central responsável pela gestão e supervisão contínua do framework, assegurando que haja uma governança clara e eficaz para sua execução e atualização conforme as demandas emergentes.

REFERÊNCIAS

ASENȚE, Tănase. Online communication strategy of world political leaders during the Ukraine crisis (February 24 - December 24, 2022). **Technium Social Sciences Journal**, v. 39, 2023. Disponível em: https://doi.org/10.47577/tssj.v39i1.8220. Acesso em: 7 out. 2024.

COWAN, C. Software security for open-source systems. **IEEE Security & Privacy**, v. 1, p. 38-45, 2003. Disponível em: https://doi.org/10.1109/MSECP.2003.1176994. Acesso em: 25 de setembro de 2024.

ELEMENT. Customers. [*S. l.*]: Element, 2024. Disponível em: https://element.io/customers. Acesso em: 13 out. 2024.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **CISA Strategic Plan 2023-2025**. Washington, DC: CISA, 2022. Disponível em: https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf. Acesso em: 28 set. 2024.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Critical information infrastructure and service**. Attiki: ENISA, 2024. Disponível em: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services. Acesso em: 11 out. 2024.

GHASEMSHIRAZI, S.; SHIRVANI, G.; ALIPOUR, M. **Zero trust**: applications, challenges, and opportunities. Ithaca, NY: Cornell University, 2023. Disponível em: https://doi.org/10.48550/arXiv.2309.03582. Acesso em: 13 out. 2024.

INFORMATIONS TECHNIK ZENTRUM BUND. **SIB-Box**. [*S. l.*]: ITZBUND, [202-]. Disponível em https://www.itzbund.de/DE/itloesungen/standardloesungen/sibbox/sibbox.html. Acesso em: 13 out. 2024.

THE INTERNET ENGINEERING TASK FORCE. **The Transport Layer Security (TLS) protocol version 1.2**. RFC 5246. [*S. l.*]: IETF, 2008. Disponível em: https://datatracker.ietf.org/doc/html/rfc5246. Acesso em: 13 out. 2024.

THE INTERNET ENGINEERING TASK FORCE. **The Transport Layer Security (TLS) Protocol Version 1.3**. RFC 8446. [*S. l.*]: IETF, 2018. Disponível em: https://datatracker.ietf.org/doc/html/rfc8446. Acesso em: 13 de outubro de 2024.

LINÅKER, J.; ROBLES, G.; BRYANT, D.; MUTO, S. Open Source Software in the Public Sector**. IEEE Softw**, v. 40, n. 4, 2023. Disponível em https://doi.org/10.1109/MS.2023.3266105. Acesso em: 12 out. 2024

MOTHUKURI, V.; PARIZI, R.; POURIYEH, S.; HUANG, Y.; DEHGHANTANHA, A.; SRIVASTAVA, G. A survey on security and privacy of federated learning. **Future Generation Computer Systems,** v. 115, p. 619-640, Feb. 2021. Disponível em: https://doi.org/10.1016/j.future.2020.10.007. Acesso em: 25 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Estrutura de Segurança Cibernética (CSF) 2.0 do NIST. NIST CSWP 29 por.** Gaithersburg, MD: NIST, 2024. Disponível em: https://doi.org/10.6028/NIST.CSWP.29.por. Acesso em: 11 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)**. Version 2.0. ed. Gaithersburg, MD: NIST, 2020a. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: 11 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Security and Privacy Controls for Information Systems and Organizations (SP 800-53)**. 5. ed. Gaithersburg, MD: NIST, 2020b. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Acesso em: 11 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Zero Trust Architecture (ZTA).** NIST Special Publication 800-207. Gaithersburg, MD: NIST, 2020c. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. Acesso em: 13 out. 2024.

NATO INNOVATION HUB. **NI2CE Messenger**. Norfolk: NATO Innovation Hub, [2024?] Disponível em: https://innovationhub-act.org/ni2ce-messenger/. Acesso em: 13 out. 2024.

NEXTCLOUD. **Encryption details**. [*S. l.*]: NextCloud, 2024. Disponível em: https://docs.nextcloud.com/server/30/admin_manual/configuration_files/encryption_details.html. Acesso em: 13 out. 2024.

NEXTCLOUD. **Government**. [*S. l.*]: NextCloud, [2024?].Disponível em: https://nextcloud.com/government/. Acesso em: 13 out. 2024.

OLIVEIRA, R.; RAGA, M.; LARANJEIRO, N; VIEIRA, M. An approach for benchmarking the security of web service frameworks. **Future Generation Computer Systems,** v. 110, p. 833-848, Sept. 2020. Disponível em: https://doi.org/10.1016/j.future.2019.10.027. Acesso em: 25 set. 2024.

POSTHUMUS, S.; SOLMS, R. A framework for the governance of information security. **Computers & Security,** v. 23, n. 8, Dec. 2004. Disponível em: https://doi.org/10.1016/j.cose.2004.10.006. Acesso em: 25 set. 2024.

MOON, Jae Yun; SPROULL, Lee. Essence of distributed work: The case of the Linux kernel. **First Monday**, [*S. l.*], v. 5, n. 11, 2000. DOI: 10.5210/fm.v5i11.801. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/801. Acesso em: 15 out. 2024.

TAHERDOOST, Hamed. Understanding Cybersecurity Frameworks and Information Security Standards - A Review and Comprehensive Overview. **Electronics**, v.11, n. 14, p. 2181, 2022. Disponível em: https://doi.org/10.3390/electronics11142181 - Acesso em: 19 set. 2024.

TIMMERS, P. Ethics of AI and Cybersecurity When Sovereignty is at Stake. **Minds and Machines**, 29, 635 – 645, 2019. Disponível em: https://doi.org/10.1007/s11023-019-09508-4. Acesso em: 15 out. 2024.

TORVALDS, L.; DIAMOND, D. **Just for Fun**: the story of an accidental revolutionary. New York: HarperBusiness, 2001.

UNITED STATES. The White House. **National Cybersecurity Strategy.** Washington, DC: White House, 2023. Disponível em: https://www.whitehouse.gov/oncd/national-cybersecurity-strategy/. Acesso em: 28 set. 2024.

YASWINSKI M. R.; CHOWDHURY M. M.; JOCHEN M. Linux Security: A Survey**.** *In*: IEEE INTERNATIONAL CONFERENCE ON ELECTRO INFORMATION TECHNOLOGY (EIT), 2019, Brookings, SD. **Proceedings** […]. New York; IEEE, 2019. p. 357-362. Disponivel em: http://dx.doi.org/10.1109/EIT.2019.8834112. Acesso em: 28 set. 2024.

ZHANG, W.; CHEN, J.; KUO, Y.; ZHOU, Y. Artificial-Noise-Aided optimal beamforming in layered physical layer security**. IEEE Communications Letters**, v. 23, p. 72-75, 2019. Disponível em: https://doi.org/10.1109/LCOMM.2018.2881182. Acesso em: 25 set. 2024.