



PIM V

SEGURANÇA DA INFORMAÇÃO

ACESSO ÚNICO AO SISTEMA GOVERNAMENTAL

Universidade de São Paulo (GAMA – DF)

2024



PIM V
SEGURANÇA DA INFORMAÇÃO

ACESSO ESPECÍFICO AO SISTEMA GOVERNAMENTAL

GUSTAVO NORBERTO BARROS

RA: 2341001

SEGURANÇA DA INFORMAÇÃO

SEMESTRE: 1º

Universidade de São Paulo (GAMA – DF)

2024

Resumo

O presente relatório tem como objetivo analisar o mundo digital durante o surto do vírus da COVID-19 observando a urgência de adaptação da sociedade brasileira para criar meios de comunicação e relacionamentos entre indivíduos e organizações no ambiente virtual. O mundo necessitou da utilização de diversos mecanismos virtuais para melhorar a vida em todas as áreas da população destacando entre eles, aplicativos de e-commerce, reuniões virtuais e acesso a aplicativos de banco com o uso do PIX e órgão governamental. A Segurança da Informação se tornou uma área crítica dentro da Tecnologia da Informação pelo risco que usuários passam a ter com a adoção da internet como o seu segundo ambiente profissional e pessoal pois com o aumento do acesso em massa na internet os ataques também cresceram de forma exacerbada evidenciando a criticidade em dispor de maiores investimentos e recursos de segurança cibernética. O Brasil destacou-se negativamente nesse cenário sendo amplamente visado por cibercriminosos que aproveitaram de brechas no sistema de proteção digital como vazamentos de dados, Pishing (roubo de dados via e-mail/sites falsos), engenharia social entre outros o que levou as empresas adotarem mecanismo de segurança como a adoção da VPN (Virtual Private Network) como uma das principais barreiras para proteger a navegação em redes públicas e privadas para buscar o anonimato. A urgência fez com que empresas implementassem de forma improvisada o que também abriu brechas de segurança. O relatório propõe um aplicativo multiplataforma com uma arquitetura de rede robusta e segura em conjunto com normas e políticas que devem ser implementadas nos sistemas digitais brasileiros e ambientes físicos para complementar a segurança e garantir o cumprimento da LGPD (Lei nº 13.709/2018) respeitando os princípios de finalidade, adequação, necessidade e segurança dos dados. Por fim, o relatório apresenta uma análise do impacto socioeconômico no Brasil durante esse período e os benefícios econômicos que podem ser alcançados com a utilização das medidas propostas.

Palavras chave: COVID-19; virtual; cibernética; VPN; aplicativo; socioeconômico.

Abstract

This report aims to analyze the digital world during the outbreak of the COVID-19 virus, observing the urgency of adapting Brazilian society to create means of communication and relationships between individuals and organizations in the virtual environment. The world has needed to use various virtual mechanisms to improve life in all areas of the population, including e-commerce applications, virtual meetings and access to banking applications using PIX and government agencies. Information Security has become a critical area within Information Technology due to the risk that users are taking with the adoption of the Internet as their second professional and personal environment, because with the increase in mass access to the Internet, attacks have also grown dramatically, highlighting the criticality of having greater investments and cybersecurity resources. Brazil stood out negatively in this scenario, being widely targeted by cybercriminals who took advantage of loopholes in the digital protection system such as data leaks, Phishing (data theft via email/fake websites), social engineering, among others, which led companies to adopt security mechanisms such as the adoption of VPN (Virtual Private Network) as one of the main barriers to protect browsing on public and private networks to seek anonymity. The urgency has led companies to implement them in an improvised way, which has also opened up security loopholes. The report proposes a multiplatform application with a robust and secure network architecture in conjunction with standards and policies that should be implemented in Brazilian digital systems and physical environments to complement security and ensure compliance with the LGPD (Law No. 13,709/2018) while respecting the principles of purpose, adequacy, necessity and data security. Finally, the report presents an analysis of the socio-economic impact in Brazil during this period and the economic benefits that can be achieved by using the proposed measures.

Palavras chave: COVID-19; cybersecurity; attacks; VPN; socio-economic;

SUMÁRIO

1. INTRODUÇÃO.....	5
2. DESENVOLVIMENTO	7
2.1 Proposta	7
2.2 Diretrizes técnicas e legais do desenvolvimento	11
2.3 Arquitetura de segurança de rede	13
2.4 Justificativa das ferramentas e medidas selecionadas	16
2.5 Impactos Socioeconômicos	19
3. CONCLUSÃO	22
REFERÊNCIAS	24

1. INTRODUÇÃO

Empresas e pessoas em todo o mundo foram praticamente obrigadas a adotarem de forma inesperada o modelo de trabalho remoto e modificarem sua utilização dos principais recursos sociais como banco, órgãos governamentais, comunicação entre outros para se adaptarem a chegada do isolamento social causado pela pandemia da COVID-19 que refletem até os dias de hoje. Essa mudança radical apresentou diversas fragilidades na infraestrutura de tecnologia da informação e comunicação brasileira, especialmente na área de segurança no acesso remoto aos dados e sistemas corporativos.

Esse crescimento não foi acompanhado da mesma velocidade de adoção de políticas de cibersegurança adequadas ou pela modernização das estruturas de proteção digital. Como consequência, diversos ataques cibernéticos foram registrados, expondo dados sensíveis de cidadãos e organizações, colocando em risco a privacidade, a integridade e a disponibilidade das informações.

O Brasil, infelizmente, destacou-se negativamente nesse contexto. Diversos relatórios e pesquisas apontaram o país como um dos principais alvos de crimes cibernéticos durante o período pandêmico. Tais ataques, muitas vezes, exploravam brechas em redes públicas, a ausência de criptografia em comunicações corporativas e a baixa maturidade dos usuários em relação a práticas seguras na internet. Casos de vazamento de dados, fraudes por phishing, golpes utilizando engenharia social e ataques direcionados a sistemas governamentais escancararam a necessidade urgente de investir em estratégias de proteção mais eficazes.

A Segurança da Informação passou a ter um papel estratégico nas organizações visto que problemas ocasionados pelos meios digitais não traziam somente prejuízos financeiros mas também de reputação, onde empresas com baixa segurança virtual poderiam vir à falência por falta de investidores e clientes. A utilização de rede privadas virtuais (VPNs) surgiu como um dos principais mecanismos de segurança para garantir a integridade nas conexões remotas ao prover uma camada extra de segurança estabelecendo túneis criptografados entre usuários e sistemas internos. Contudo com a ampla urgência por uso imediato as soluções foram implementadas de forma despadronizada o que apresentou riscos sobretudo quando utilizada sem uma política de acesso e autenticação forte.

O relatório propõe uma startup fictícia que vai desenvolver um app em parceria com o Governo Federal que gerencia acessos via VPN entre usuários e órgãos governamentais com arquitetura de rede segura e reforçada. A proposta tem o objetivo de estabelecer regras e políticas na startup para o desenvolvimento do app que devem seguir as diretrizes das normas ISO/IEC 27001 e 27002 além de padrões de desenvolvimento de software com base na ISO/IEC 9125, promovendo não apenas segurança técnica mas também conformidade legal e ética perante ao uso da tecnologia levando em consideração a Lei Geral de Proteção de Dados e a prevenção de riscos de má qualidade de software.

Por fim apresentar uma análise sobre os impactos sociais e econômicos durante a pandemia no Brasil e evidenciar os benefícios econômicos que podem ser alcançados ao aplicar na prática as medidas incluídas no relatório bem com retomar a confiança digital.

2. DESENVOLVIMENTO

2.1 Proposta

Durante a pandemia da covid-19, com a migração em massa de serviços para o digital e o home office se tornando a norma, surgiram uma série de vulnerabilidades como apresentado na figura 1, os atacantes estavam prontos para explorar. Muitas empresas e até órgãos públicos não estavam preparados para o aumento repentino de tráfego e, como consequência, ficaram expostos a uma série de ameaças cibernéticas.

Primeiro, um dos maiores riscos foi o uso de senhas fracas e a falta de autenticação multifatorial. Com muitas pessoas trabalhando remotamente, senhas simples (ou até a mesma senha para tudo) foram usadas em massa, criando um terreno fértil para ataques de força bruta e até phishing. Isso também gerou vulnerabilidades em sistemas de acesso remoto, onde qualquer brecha na autenticação permitia a invasão dos sistemas. Quando os atacantes conseguem acessar uma conta de um usuário, é só questão de tempo até que possam escalar privilégios e ter acesso a dados mais sensíveis.



Figura 1 – Comparativo entre os ataques cibernéticos e os casos de COVID-19 no Brasil em 2020.

Fonte: Infor Channel (2021).

Outro grande problema foi o aumento do tráfego em redes corporativas e governamentais, muitas vezes feitas de forma improvisada, o que deixou os sistemas ainda mais vulneráveis. Muitas redes não estavam devidamente segmentadas, o que significava que uma vez que os hackers conseguiam acessar uma parte da rede, poderiam facilmente se mover para outras áreas, roubando dados ou até interrompendo operações essenciais.

E, claro, o uso de softwares desatualizados e configurações inadequadas foi um prato cheio para os atacantes. Durante a correria, muitos sistemas não passaram por um processo adequado de auditoria e testes de segurança. Isso abriu portas para a exploração de vulnerabilidades conhecidas, como falhas em servidores web ou protocolos de rede que estavam mal configurados.

Esses ataques, na maioria das vezes, eram muito rápidos, com hackers usando ferramentas automatizadas para explorar brechas. Ransomware e phishing aumentaram muito durante esse período, com e-mails falsos tentando roubar credenciais ou fazer com que as pessoas clicassem em links maliciosos. E quando as empresas tentavam recuperar o que tinha sido comprometido, muitas não tinham backups atualizados ou planos claros de contingência. A falta de uma estratégia de recuperação de desastres fez com que a resposta fosse lenta, piorando a situação.

Pra mitigar esses problemas, é essencial pensar em vários pontos de defesa. Um deles é, claro, a criptografia dos dados tanto em trânsito quanto em repouso. Isso garante que, mesmo que um atacante consiga interceptar os dados, eles não consigam lê-los. Além disso, a autenticação multifatorial (MFA) deve ser a norma, não uma exceção. Isso cria uma camada extra de proteção, dificultando muito que um invasor consiga acessar o sistema, mesmo que tenha conseguido roubar uma senha.

Outro ponto crucial é a segmentação da rede. Ela ajuda a isolar áreas críticas e impede que um atacante, ao invadir um ponto da rede, consiga acessar outras partes de forma tão fácil. Além disso, a implementação de firewalls de próxima geração e sistemas de detecção de intrusão (IDS) é vital para monitorar comportamentos anormais e bloquear ataques antes que se espalhem.

É claro que backups são essenciais, mas não basta fazer uma cópia de vez em quando. O backup deve ser contínuo e automático, garantindo que qualquer alteração feita no sistema seja salva em tempo real. Isso vai permitir uma recuperação rápida

em caso de ataque ou falha. Sem isso, a recuperação pode demorar muito tempo, e os dados podem ser perdidos permanentemente.

A solução visa oferecer uma camada robusta de proteção, integrando criptografia de alto nível e múltiplos fatores de autenticação, além de seguir os princípios e diretrizes da norma de segurança da informação ISO/IEC 27001 e 27002 formada por três principais camadas de acesso. Na primeira, o usuário acessa o aplicativo a partir de seu dispositivo, seja ele móvel ou desktop. A segunda camada é responsável por estabelecer a conexão segura com a rede VPN, utilizando protocolos confiáveis como o OpenVPN, reconhecido pela sua eficiência em criar túneis criptografados que impedem a interceptação de dados. Por fim, a terceira camada se comunica diretamente com os sistemas públicos, respeitando uma política de firewall previamente ajustada para aceitar apenas conexões vindas da faixa de IPs da VPN, bloqueando qualquer tentativa de acesso externo pela internet convencional.

Para que o acesso ao sistema ocorra de maneira segura e controlada, será aplicado um modelo de autenticação multifatorial. O processo inicia-se com a inserção de um login e senha pessoais, representando o fator "algo que o usuário sabe". Em seguida, o aplicativo exigirá uma segunda confirmação, que pode ser feita por meio de um token gerado em tempo real, um código emitido por aplicativo autenticador. Essa etapa representa o "algo que o usuário tem". Por fim, como terceiro fator, será solicitada a validação biométrica como o reconhecimento facial para garantir que o usuário que está realizando o acesso é realmente quem afirma ser, encerrando com o "algo que o usuário é".

Com a implementação da arquitetura proposta, espera-se mitigar riscos frequentes como vazamentos de dados, acesso indevido, ataques de ransomware, e exposição dos sistemas a redes não confiáveis. Ao restringir as conexões aos túneis da VPN e exigir múltiplas formas de autenticação alcançamos um nível alto de proteção contra ataques maliciosos.

Além disso, uma estrutura segura exige atenção também à educação e à conscientização dos usuários. A arquitetura técnica mais avançada pode ser comprometida por um único clique errado de um colaborador mal instruído. Por isso, é indispensável investir em treinamentos regulares, simulações de phishing, e reforço de boas práticas, como o uso de senhas fortes, verificação de remetentes em e-mails e cuidado ao acessar sistemas em redes públicas.

Por fim, é importante destacar que, ao promover a digitalização segura dos serviços, o projeto contribui não apenas para a proteção de dados e sistemas, mas também para a modernização do setor público. Permitir que cidadãos acessem sistemas governamentais com segurança e confiabilidade fortalece a relação entre governo e sociedade, agiliza processos burocráticos, e possibilita maior inclusão digital, principalmente para aqueles que dependem de serviços públicos à distância.

2.2 Diretrizes técnicas e legais do desenvolvimento

A construção de um aplicativo que oferece acesso remoto a sistemas governamentais exige um compromisso rigoroso com padrões técnicos e legais que assegurem a confidencialidade, integridade, disponibilidade e qualidade das informações. Nesse sentido, o projeto aqui apresentado se fundamenta em três pilares principais: conformidade com a Lei Geral de Proteção de Dados (LGPD), aplicação das normas ISO/IEC 27001 e 27002 para gestão da segurança da informação, e adoção de boas práticas da norma ISO/IEC 9126 (atualmente substituída pela 9125) no que se refere à qualidade de software.

A LGPD (Lei nº 13.709/2018) determina princípios fundamentais para o tratamento de dados pessoais, como a finalidade, necessidade, transparência e segurança. No contexto do aplicativo, essas diretrizes são aplicadas na definição de acessos mínimos necessários por perfil de usuário, na coleta restrita de informações apenas para finalidades específicas e na utilização de mecanismos de consentimento explícito para cada tratamento realizado. A anonimização dos dados em determinadas situações e a capacidade de exclusão dos registros mediante solicitação também fazem parte do escopo técnico do app, garantindo a conformidade legal.

Complementarmente, o desenvolvimento e a operação do aplicativo são orientados pelas normas ISO/IEC 27001 e 27002, que estabelecem requisitos e controles para um Sistema de Gestão da Segurança da Informação (SGSI). A 27001 trata da estrutura gerencial da segurança, enquanto a 27002 descreve os controles específicos. No contexto deste projeto, foram considerados os seguintes pontos críticos:

Controle de acesso baseado em papéis (RBAC), com níveis hierárquicos claramente definidos.

Criptografia dos dados em repouso e em trânsito, utilizando padrões como AES-256 e TLS.

Gestão de riscos cibernéticos, com políticas de mitigação baseadas em análise contínua de ameaças.

Auditoria e rastreabilidade de atividades, assegurando que todos os eventos relevantes sejam registrados e passíveis de investigação.

Continuidade do serviço, com planos de recuperação diante de falhas ou ataques.

No que se refere à qualidade do software, são consideradas as diretrizes da ISO/IEC 9125, que evoluiu a partir da ISO 9126 e propõe um modelo de avaliação de qualidade baseado em seis características principais: funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade. Para o presente projeto, essas características são tratadas da seguinte forma:

Funcionalidade: o sistema atende aos requisitos de acesso seguro, autenticação robusta e comunicação com sistemas públicos, com validação criptográfica de usuários.

Confiabilidade: uso de protocolos maduros e testes de estresse garantem que o app funcione mesmo sob alto volume de acessos.

Usabilidade: a interface do aplicativo é pensada para ser simples e intuitiva, mesmo para usuários com baixo nível de letramento digital.

Eficiência: otimização dos processos de autenticação e conexão com VPN, reduzindo o consumo de dados e tempo de resposta.

Manutenibilidade: a arquitetura modular facilita atualizações e correções sem comprometer o núcleo do sistema.

Portabilidade: compatibilidade com os principais sistemas operacionais móveis e desktops, garantindo amplo alcance de uso.

Ao integrar essas diretrizes legais e técnicas desde a fase de projeto, o desenvolvimento do aplicativo reduz consideravelmente os riscos de não conformidade, falhas operacionais, vulnerabilidades de segurança e problemas de experiência do usuário. O resultado esperado é uma solução robusta, confiável e ética, capaz de promover a transformação digital com segurança e qualidade em ambientes que exigem o mais alto nível de proteção da informação.

Também foram previstas políticas voltadas à segurança do ambiente físico onde dados e sistemas sensíveis são processados ou armazenados. A proteção desse ambiente reconhece que vulnerabilidades no espaço físico podem comprometer toda a estrutura, mesmo com medidas digitais avançadas. Nesse sentido, o projeto prevê acesso físico altamente controlado, com autenticação multifatorial (biometria e cartões RFID), barreiras físicas, registro de entrada e saída, e monitoramento constante por circuito fechado de TV (CFTV) com retenção de imagens por período auditável.

2.3 Arquitetura de segurança de rede

A arquitetura de rede proposta neste projeto foi desenvolvida com foco em segurança, desempenho e conformidade com os principais padrões internacionais. Trata-se de uma estrutura baseada em uma VPN dedicada, capaz de estabelecer um túnel de comunicação seguro entre o aplicativo multiplataforma e os sistemas governamentais. O objetivo é evitar qualquer exposição direta à internet pública, restringindo o acesso apenas por meio da conexão autenticada na rede privada virtual.

A camada de rede responsável pela interconexão segura utilizará protocolos como OpenVPN, com suporte a criptografia de alto nível e autenticação via certificados digitais. Após a autenticação, o sistema gerará uma chave temporária vinculada ao usuário, que será validada por meio da chave pública do órgão público requisitado, assegurando que apenas usuários legítimos estabeleçam comunicação com os sistemas críticos.

Para assegurar a confidencialidade e a integridade das informações em trânsito, será empregada criptografia simétrica de alta segurança baseada no algoritmo AES com chave de 256 bits, amplamente reconhecido por sua resistência a ataques mesmo com grande capacidade computacional. A integridade dos dados será verificada por meio de funções de hash criptográficas como SHA-256 ou superiores, capazes de identificar qualquer alteração acidental ou intencional no conteúdo transmitido. A negociação da sessão ocorrerá utilizando o protocolo TLS na versão 1.3, que garante uma troca de chaves mais segura e eficiente, protegendo contra tentativas de interceptação e ataques *man-in-the-middle*. Em relação à autenticação de usuários, será adotada uma abordagem multifatorial que combina diferentes elementos de validação, incluindo credenciais convencionais como login e senha, a utilização de tokens gerados pelo aplicativo autenticador o Google Authenticator que fornece códigos temporários sincronizados via algoritmo TOTP, finalizando com o mecanismo biométrico de reconhecimento facial. Essa combinação fortalece substancialmente a proteção contra acessos indevidos, mesmo em casos de comprometimento parcial das credenciais.

A política de segurança inclui o uso de firewalls com regras extremamente restritivas. As conexões só serão aceitas a partir dos IPs definidos da VPN e mediante autenticação completa. A política de “negação por padrão” será adotada, permitindo apenas o tráfego essencial, com filtragem por porta, protocolo e origem. A

segmentação lógica da rede e o uso de inspeção com estado garantirão que apenas pacotes válidos e autorizados sejam encaminhados, mitigando riscos de ataques por invasão ou escaneamento.

Por fim, todo o ambiente será monitorado por meio de sistemas de detecção e prevenção de intrusos (IDS/IPS), integrados a mecanismos avançados de coleta e análise de eventos de segurança. A infraestrutura contará com o registro contínuo de logs, capturados por agentes instalados tanto no servidor VPN quanto nos endpoints de autenticação e comunicação. Serão mantidos registros detalhados de autenticações bem-sucedidas e mal-sucedidas, tentativas de conexão não autorizadas, atividades suspeitas, movimentações de dados fora do padrão e qualquer anomalia que possa indicar comportamento malicioso.

Os logs serão gerados e armazenados conforme as diretrizes da norma ISO/IEC 27002 (2022), que recomenda o uso de sistemas SIEM integrados a políticas de registro e análise contínua, especialmente em ambientes de alta criticidade.. O projeto será estruturado com base no modelo CEF (Common Event Format), facilitando a integração com ferramentas de análise como ELK Stack (Elasticsearch, Logstash, Kibana). Esses sistemas permitirão a correlação de eventos em tempo real, a identificação proativa de ameaças e a geração de alertas automáticos, além de manterem trilhas de auditoria criptografadas com controle de integridade para garantir que os registros não sejam manipulados. Para assegurar que o processo de monitoramento e resposta a incidentes evolua continuamente, será adotado o ciclo de melhoria contínua PDCA (Plan, Do, Check, Act), o qual será aplicado à gestão da segurança da informação como um todo.

Além disso, os logs conterão metadados essenciais como carimbo de data e hora sincronizado por NTP, endereço IP de origem, tipo de evento, aplicação envolvida, localização geográfica e dispositivo utilizado. Todos os dados serão armazenados em ambiente seguro, com controle de acesso baseado em função (RBAC) e retenção conforme as exigências da LGPD, assegurando rastreabilidade, não repúdio e resposta ágil a incidentes.

Em vez de backups tradicionais baseados em blocos ou agendamentos esporádicos, optou-se por backups contínuos em nível de transação, garantindo que toda ação realizada no sistema seja registrada e armazenada quase em tempo real.

Essa abordagem permite uma recuperação granular, inclusive de sessões específicas ou ações individuais de usuários.

Além da rigidez técnica, a arquitetura proposta incorpora uma visão estratégica da segurança como processo dinâmico, adaptável. A escolha por mecanismos distribuídos de autenticação, camadas independentes de defesa e registro em tempo real reflete o compromisso com uma abordagem de defesa em profundidade, onde cada elemento do sistema atua de forma integrada, porém autônoma, no combate a ameaças. Ao invés de depender exclusivamente de ferramentas, a estrutura valoriza a coerência entre tecnologia, processos e pessoas, reconhecendo que a segurança da informação não se limita à prevenção, mas envolve vigilância contínua, capacidade de resposta rápida e, sobretudo, aprendizado com cada tentativa de violação. Essa mentalidade orientada à resiliência, sustentada por normas internacionais e reforçada por mecanismos como o PDCA, garante que o ecossistema digital construído seja não apenas seguro, mas também sustentável diante da constante evolução dos riscos cibernéticos.

2.4 Justificativa das ferramentas e medidas selecionadas

A utilização de uma VPN dedicada no contexto deste sistema é uma medida essencial para garantir a confidencialidade, integridade e autenticidade das informações trafegadas entre o aplicativo e os sistemas governamentais. Ao encapsular todo o tráfego em um túnel criptografado, a VPN impede que dados sensíveis sejam expostos à internet pública, reduzindo drasticamente a superfície de ataque e os riscos associados a interceptações, escutas e ataques man-in-the-middle.

A escolha pela criptografia AES com chave de 256 bits para proteger a confidencialidade e integridade dos dados não é apenas uma medida de segurança padrão, mas uma escolha consciente baseada em sua comprovada resistência contra ataques. Esse algoritmo é amplamente adotado no mercado por ser extremamente robusto, mesmo em cenários de grande poder computacional. Além disso, a utilização de funções de hash como o SHA-256 proporciona uma camada adicional de segurança, garantindo que qualquer alteração nos dados seja detectada, seja ela acidental ou maliciosa sendo um método rápido e eficaz. Combinado com o protocolo TLS 1.3, que garante uma negociação de sessão mais eficiente e segura, considerando essas medidas temos uma comunicação robusta que resiste a tentativas de interceptação e ataques man-in-the-middle.

A autenticação multifatorial que adotei é uma medida que vai além das práticas convencionais. A combinação de login e senha, juntamente com tokens temporários gerados por aplicativos como o Google Authenticator, e a verificação biométrica por reconhecimento facial, eleva o nível de segurança ao ponto de ser quase impossível acessar as informações sem a verificação completa dos dados do usuário. Isso adiciona uma camada extra de proteção que assegura que apenas usuários devidamente autenticados possam interagir com o sistema, mesmo em cenários em que parte das credenciais possa estar comprometida.

O uso de OpenVPN como protocolo de rede para a interconexão segura é uma escolha bem fundamentada como apresentado na figura 3. Ele não só oferece criptografia de alto nível, como também permite a autenticação via certificados digitais, o que garante que os usuários que estabelecem a comunicação com os sistemas sejam de fato autorizados. A geração de chaves temporárias vinculadas ao usuário e validadas com a chave pública do órgão público requisitado acrescenta uma camada

adicional de verificação, fortalecendo ainda mais a segurança e impedindo a comunicação com usuários não autorizados.
























Nem um pouco seguro 	Alguns problemas de segurança 	Muito seguro 	O mais seguro 
PPTP  Ultrapassado  Facilmente hackeado	L2TP/IPSec  Considerado seguro se usado com AES  Suscetível a ataque MITM se usado com chave pré-compartilhada  Possível comprometimento pela NSA	IKEv2/IPSec  Muito rápido  Funciona bem em dispositivos móveis  Código fechado	OpenVPN  Código aberto  Bom padrão  Rápido
	SSTP  Possível vulnerabilidade a ataque Poodle  Código fechado	Wireguard  Código aberto  Extremamente rápido e seguro  Relativamente novo	
		SoftEther  Muito rápido  Bom para contornar censura  Seguro apenas após configuração manual	

Figura 3 Top10VPN. Protocolos VPN. Disponível em: <https://www.top10vpn.com/pt/o-que-e-uma-vpn/protocolos-vpn/>.

As políticas de segurança, que incluem firewalls extremamente restritivos e a abordagem de "negação por padrão", foram adotadas com o objetivo de garantir que apenas o tráfego necessário e autorizado seja permitido. A filtragem por porta, protocolo e origem assegura que o sistema seja protegido contra acessos indevidos e ataques. A segmentação lógica da rede e o uso de inspeção com estado permitem uma vigilância contínua e eficaz, minimizando a exposição a riscos externos.

O monitoramento contínuo por meio de sistemas IDS/IPS é essencial para a detecção proativa de atividades suspeitas. A integração com ferramentas de análise de eventos de segurança, como o ELK Stack, permite uma visão em tempo real das ocorrências no sistema, facilitando a identificação de ameaças e a geração de alertas. Essa infraestrutura é projetada para garantir que qualquer incidente seja tratado de

forma rápida e eficiente, com uma base sólida de registros e logs que servem como trilhas de auditoria e também como fonte de dados para futuras melhorias.

A escolha por armazenar logs detalhados, com metadados cruciais, e garantir que esses dados sejam armazenados de forma segura e de acordo com a LGPD, assegura que o sistema seja não apenas seguro, mas também em conformidade com as regulamentações de proteção de dados. A utilização de controles de acesso baseados em funções (RBAC) e a implementação de um ciclo de melhoria contínua (PDCA) demonstram o compromisso com a evolução constante da segurança e da gestão da informação, garantindo que o sistema se mantenha resiliente diante de novas ameaças e desafios.

2.5 Impactos Socioeconômicos

Os impactos da pandemia englobam tanto os aspectos sociais quanto os aspectos econômicos da sociedade. Como consequência as tecnologias foram integradas nas relações sociais e no mundo do trabalho, de forma que, mesmo após a pandemia, essa integração foi mantida. Um exemplo, a continuidade do trabalho remoto, o home office.

Os efeitos da pandemia nos aspectos sociais ainda são inestimáveis, devido aos diversos campos afetados na vida dos indivíduos como relacionamentos, saúde mental e física. Esses impactos podem continuar influenciando a vida de muitas pessoas que ainda se adaptam a um mundo pós-pandemia.

No que diz respeito aos impactos econômicos, o mundo inteiro perdeu a perspectiva de crescimento devido à indefinição sobre o que estava por vir e à dificuldade de lidar com um vírus altamente contagioso sem comprometer o mercado financeiro.

A economia mundial, incluindo a brasileira, passa por momento de elevado grau de incerteza em decorrência da pandemia de coronavírus, que está provocando desaceleração significativa da atividade econômica, queda nos preços das commodities e aumento da volatilidade nos preços de ativos financeiros. Nesse contexto, apesar da provisão adicional de estímulo monetário pelas principais economias, o ambiente para as economias emergentes tornou-se desafiador, com o aumento de aversão ao risco e a consequente realocação de ativos provocando substancial aperto nas condições financeiras (BACEN, 2020, p. 07).

O período da pandemia gerou diversos prejuízos e falências de empresas devido ao isolamento social como apresentado na figura 3. Uma das formas de diminuir esse impacto foi o modelo híbrido de trabalho, que mesmo no período pós-pandemia continuou sendo utilizado, embora somente após difíceis momentos de adaptação das ferramentas digitais. Segundo Baccarini (2021a), esse é um modelo que deve permanecer na realidade do mundo do trabalho.

Evolução da indústria, comércio e serviços em 2020

Base 100 = jan.2020

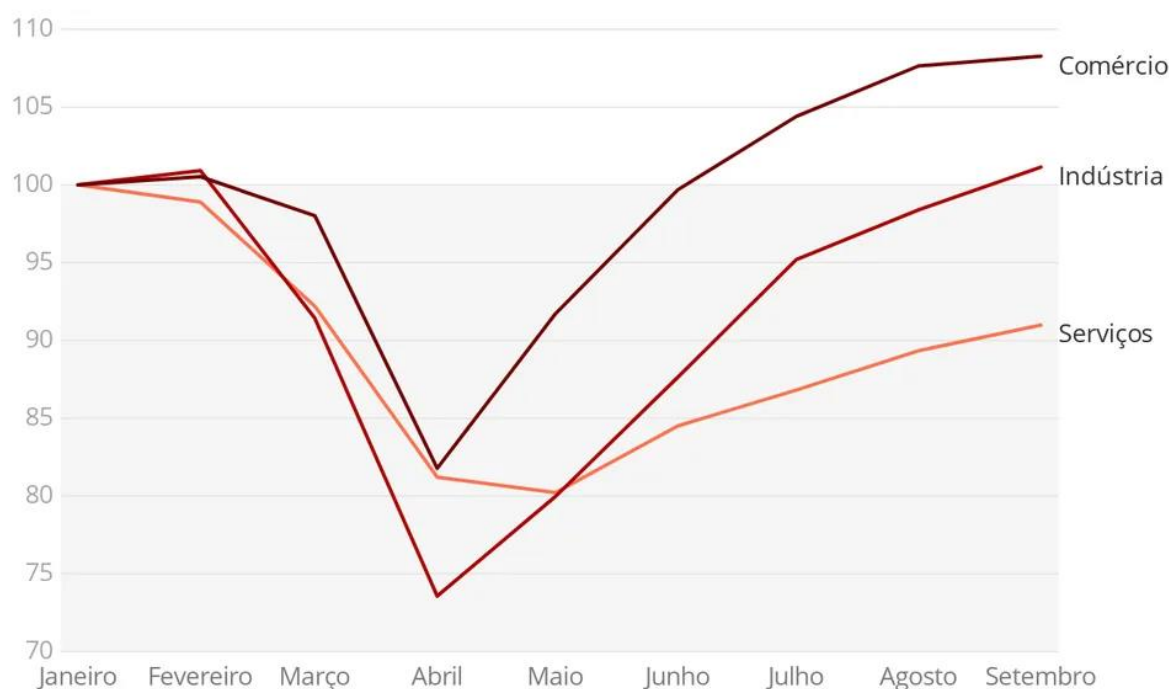


Figura 3 – Evolução da indústria, comércio e serviços no Brasil durante o ano de 2020.

Fonte: G1 Economia, com dados da 4E Consultoria e IBGE (2020).

A adoção do home office em diversas empresas durante a pandemia reafirmou a necessidade de uma política de segurança da informação específica para o acesso remoto externo por VPN. Isso devido à vulnerabilidade que as empresas que adotaram o modelo híbrido ficam em relação a proteção dos seus dados e sistemas. Como diz o especialista de segurança da informação, Denis Reviello:

A rápida adaptação ao modelo de trabalho remoto imposta pela necessidade de isolamento causada pela pandemia da COVID-19, trouxe uma série de desafios para as empresas brasileiras. Apesar da corrida por tecnologias que permitam e protejam esse modelo de trabalho, o cibercrime também adaptou seus alvos e agora foca no elo mais frágil dessa cadeia: as pessoas. O volume de ataques por engenharia social, quando o fraudador convence pessoas a executarem ações que possibilitem o golpe ou o acesso aos dados, já demonstra crescimento substancial de quase 100 mil tipos de fraudes online que usam a palavra coronavírus, por exemplo. (RIVIELLO, 2024)

Nesse cenário de transformação digital acelerada, marcado por incertezas econômicas e aumento expressivo nos crimes cibernéticos, soluções que reforcem a segurança da informação tornam-se fundamentais não apenas do ponto de vista técnico, mas também estratégico para a saúde financeira do país. A proposta de aplicação de uma arquitetura robusta de segurança em redes privadas virtuais (VPN), combinada com autenticação multifator, monitoramento contínuo e governança de dados, como descrita neste relatório, representa uma resposta direta à fragilidade digital exposta durante a pandemia. Ao reduzir drasticamente a superfície de ataque e mitigar falhas que permitem ações como roubo de dados, vazamentos e paralisação de serviços essenciais, os métodos implementados contribuem para a preservação da confiança digital e da continuidade dos negócios.

Com a aplicação de tecnologias bem estruturadas, empresas tendem a registrar menos perdas com incidentes de segurança, o que impacta positivamente na produtividade, na redução de custos com recuperação de danos e no fortalecimento da reputação institucional. Além disso, ambientes digitais mais seguros geram um efeito positivo em cadeia sobre a economia nacional, pois estimulam a inovação, a digitalização de serviços públicos e privados, e a inserção de novos negócios em ambientes online, com menor risco percebido. A segurança, portanto, deixa de ser um custo e passa a ser um fator de valorização econômica, contribuindo com a estabilidade necessária para sustentar modelos de trabalho remoto, acesso digital a serviços governamentais e a transformação digital como um todo.

3. CONCLUSÃO

A pandemia da COVID-19 trouxe à tona desafios sem precedentes para a sociedade moderna, revelando vulnerabilidades não apenas no sistema de saúde, mas também na forma como a informação é tratada, armazenada e protegida. Em um cenário marcado pelo isolamento social, pela transição abrupta para o trabalho remoto e pela digitalização acelerada de serviços essenciais, tornou-se evidente que a segurança da informação deixou de ser um diferencial técnico e passou a ocupar papel central na continuidade das operações, na proteção de dados pessoais e na estabilidade econômica de instituições públicas e privadas.

Ao longo deste relatório, foi possível demonstrar como a falta de preparo digital durante a pandemia resultou em consequências diretas para a economia e para o cotidiano da população, evidenciando uma lacuna significativa entre a velocidade da digitalização e a capacidade de proteger essa infraestrutura em expansão. Casos de vazamentos de dados, fraudes virtuais, ataques por engenharia social e interrupções de serviços se tornaram frequentes, gerando impactos econômicos consideráveis, perda de confiança da sociedade nas instituições e retrocessos em iniciativas de inovação.

Nesse contexto, a proposta de desenvolvimento de um aplicativo multiplataforma seguro, baseado em uma arquitetura de rede com VPN dedicada, autenticação multifator, criptografia robusta e políticas de firewall bem definidas, surge como uma resposta técnica e estratégica aos problemas identificados. Mais do que apenas uma solução funcional, trata-se de uma estrutura pensada a partir dos pilares da resiliência cibernética, da governança da informação e da conformidade com normas nacionais e internacionais, como a LGPD, a ISO/IEC 27001, 27002 e os parâmetros de qualidade definidos na ISO/IEC 9125.

A proposta se destaca por integrar segurança técnica com visão de continuidade operacional, ao passo que incorpora monitoramento ativo com SIEMs, controle de acesso baseado em função (RBAC), retenção adequada de logs estruturados em CEF, e melhoria contínua com base no ciclo PDCA. Essa combinação garante não apenas a proteção da informação, mas também a adaptabilidade do

sistema frente a novas ameaças, algo indispensável diante de um cenário digital cada vez mais dinâmico e sofisticado.

Do ponto de vista econômico, soluções como essa contribuem diretamente para a redução de prejuízos causados por incidentes de segurança, ajudam a manter a reputação institucional e impulsionam a digitalização de serviços com segurança e confiabilidade. Ao diminuir a exposição ao risco, as organizações passam a operar de forma mais eficiente, evitando gastos com recuperação de sistemas comprometidos e fortalecendo sua imagem diante de clientes e parceiros. Isso gera um efeito positivo sobre a economia nacional, promovendo crescimento sustentável, inovação e competitividade no mercado.

Portanto, este trabalho vai além da elaboração de um projeto técnico. Ele representa uma análise crítica e contextualizada sobre o papel da segurança da informação em um mundo pós-pandêmico, defendendo a construção de soluções que não apenas resolvem problemas imediatos, mas que se sustentem com base em normas, estratégia e visão de futuro. A tecnologia, quando bem aplicada, torna-se aliada da estabilidade econômica, da proteção dos direitos dos cidadãos e da construção de um ecossistema digital mais justo, seguro e confiável.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2022 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2022 — Tecnologia da informação — Técnicas de segurança — Código de práticas para controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 9125:2018 — Engenharia de software — Qualidade de produto de software. Rio de Janeiro: ABNT, 2018.

BACCARINI, M. Empresa adota sistema de trabalho híbrido e tem bons resultados. G1, 25 jul. 2021a. *Pequenas Empresas & Grandes Negócios*. Disponível em: <https://g1.globo.com/economia/pme/pequenas-empresas-grandes-negocios/noticia/2021/07/25/empresa-adota-sistema-de-trabalho-hibrido-e-tem-bons-resultados.ghtml>. Acesso em: 13 abr. 2025.

BACEN – BANCO CENTRAL DO BRASIL. *Relatório de inflação*, vol. 22, n. 1, 2020. Disponível em: <https://www.bcb.gov.br/content/ri/relatorioinflacao/202003/ri202003p.pdf>. Acesso em: 13 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 abr. 2025.

ELASTIC. ELK Stack: Elasticsearch, Logstash, Kibana. *Site oficial*. Disponível em: <https://www.elastic.co/what-is/elk-stack>. Acesso em: 12 abr. 2025.

GAMA NETO, R. B. Impactos da COVID-19 sobre a economia mundial. *Boletim de Conjuntura (BOCA)*, Boa Vista, v. 2, n. 5, p. 113–127, 2020. DOI: 10.5281/zenodo.3786698. Disponível em: <https://revista.ioles.com.br/boca/index.php/revista/article/view/134>. Acesso em: 13 abr. 2025.

G1 ECONOMIA. Como a pandemia bagunçou a economia brasileira em 2020. 2020. Disponível em: <https://g1.globo.com/economia/noticia/2020/12/12/como-a-pandemia-baguncou-a-economia-brasileira-em-2020.ghtml>. Acesso em: 14 abr. 2025.

GOOGLE. Google Authenticator. Disponível em: <https://support.google.com/accounts/answer/1066447>. Acesso em: 12 abr. 2025.

INFOR CHANNEL. Ataques cibernéticos no Brasil crescem 860% na pandemia. 2021. Disponível em: <https://inforchannel.com.br/2021/03/03/ataques-ciberneticos-no-brasil-crescem-860-na-pandemia/>. Acesso em: 14 abr. 2025.

OPENVPN. *Site oficial*. Disponível em: <https://openvpn.net>. Acesso em: 12 abr. 2025.

RIVIELLO, Denis. Funcionários em home office são os principais alvos de hackers. *Revista Empresários*, São Paulo, 28 mar. 2024. Disponível em: <https://revistaempresarios.net/site/funcionarios-em-home-office-sao-os-principais-alvos-de-hackers-por-denis-riviello-e-especialista-de-seguranca-da-compugraf/>. Acesso em: 13 abr. 2025.

Top10VPN. Protocolos VPN. Disponível em: <https://www.top10vpn.com/pt/o-que-e-uma-vpn/protocolos-vpn/>. Acesso em: 14 abr. 2025.