INOVA | FECOMERCIOSP

SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS DE PEQUENO E MÉDIO PORTES

FORTALEÇA A CIBERSEGURANÇA E PROTEJA O NEGÓCIO CONTRA AMEAÇAS DIGITAIS

SUMÁRIO

INTRODUÇÃO

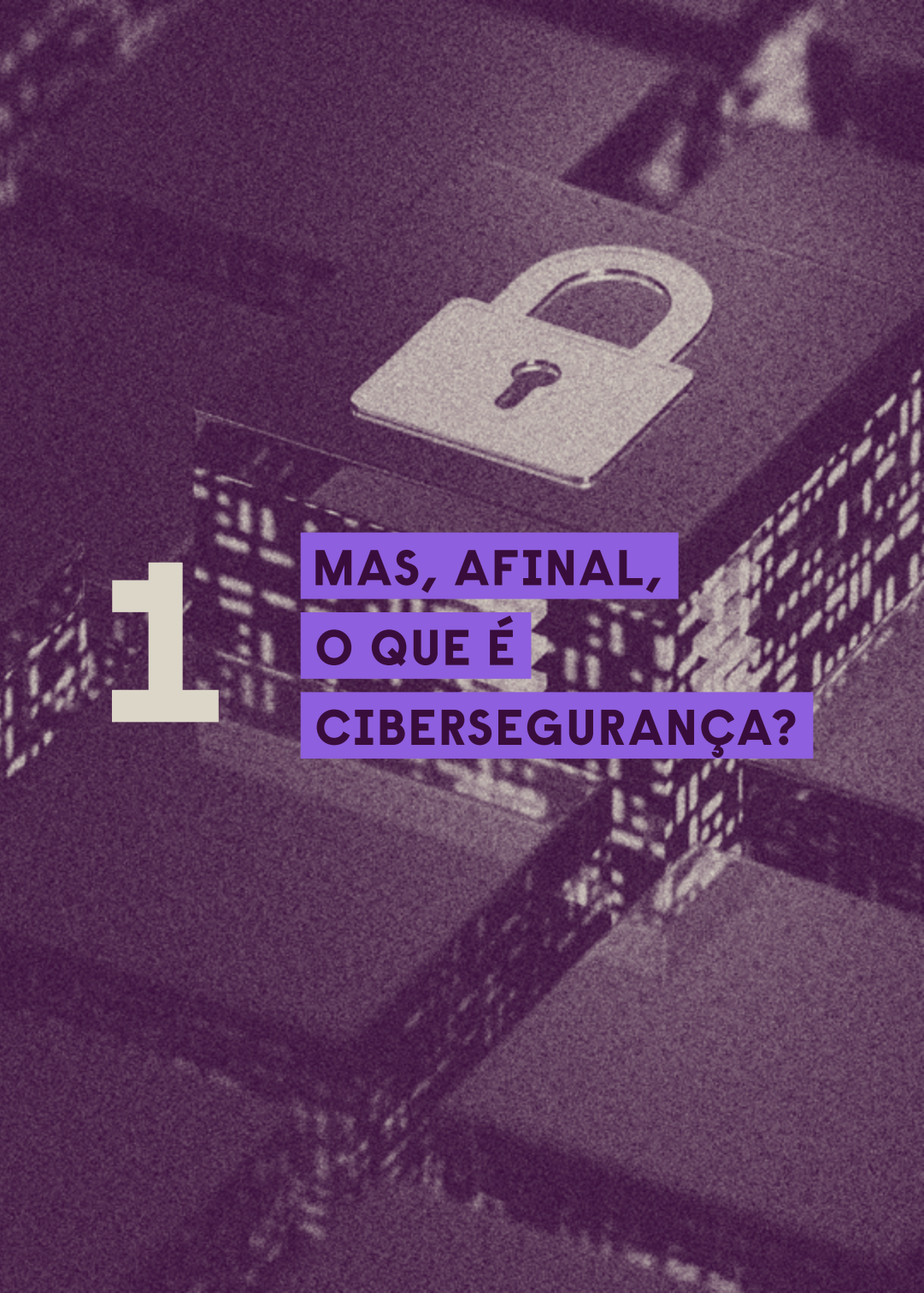
Pequenas empresas são alvos frequentes de ataques cibernéticos. De acordo com o relatório Report on the State of IT for Small and Medium-Sized Businesses, em 2023, 43% dos ataques digitais tiveram como foco pequenos negócios. As consequências podem ser devastadoras, pois 60% das empresas afetadas fecham as portas em até seis meses após um ataque. Além dos custos elevados de recuperação, que podem chegar a milhões de reais, há o risco de os danos à reputação e à confiança de clientes e parceiros comprometerem seriamente a continuidade do negócio.

Essas ameaças, no entanto, não se limitam ao prejuízo imediato. O ambiente regulatório está cada vez mais rígido, com normas gerais e setoriais exigindo que as empresas adotem padrões mais sólidos de segurança digital. O não cumprimento dessas exigências pode resultar em sanções administrativas e até responsabilização civil.

Um baixo nível de maturidade em cibersegurança e o impacto de uma falha vai além dos riscos regulatórios, pois pode afetar diretamente a viabilidade e a confiança do seu negócio.

Além disso, a crescente digitalização e o aumento da troca de dados eletrônicos tornam a cibersegurança uma questão crítica para a proteção de qualquer empresa. As ameaças digitais estão em constante evolução — e, para pequenas empresas, os perigos podem ser ainda mais intensos. Adotar medidas efetivas de segurança não apenas protege os dados do seu negócio, como também garante a continuidade das operações e a confiança dos seus clientes.

Salvaguardar a empresa contra ciberataques não é mais uma escolha, mas uma necessidade. Nesse sentido, nesta cartilha, você vai conhecer os principais riscos e adotar medidas essenciais de segurança. Assim, você estará protegido, evitando danos, tanto financeiros quanto reputacionais. ■



1 MAS, AFINAL, O QUE É CIBERSEGURANÇA?

Cibersegurança é um conjunto de práticas e estratégias adotadas para proteger os ativos de uma organização, como sistemas, redes, informações e dados contra ameaças. O objetivo principal é garantir a segurança da informação e o bom funcionamento dessas infraestruturas, prevenindo acessos não autorizados, incidentes e danos. A cibersegurança busca assegurar três pilares fundamentais: confidencialidade, integridade e disponibilidade.

- A **CONFIDENCIALIDADE** envolve a proteção de informações, garantindo que apenas pessoas ou sistemas autorizados possam acessar dados específicos. Isso é imprescindível para evitar vazamentos e assegurar que dados pessoais, financeiros ou estratégicos não sejam expostos a indivíduos não autorizados.

- A **DISPONIBILIDADE** assegura que as informações e os sistemas estejam disponíveis sempre que necessário, permitindo que os usuários autorizados tenham acesso a dados e recursos sem interrupções inesperadas ou falhas que possam prejudicar as operações.

- A **INTEGRIDADE** refere-se à garantia de que informações e sistemas não tenham sido alterados de forma indevida ou não autorizada. Isso significa proteger os dados contra modificações e corrupções ou evitar que esses sejam destruídos, garantindo que as informações permaneçam precisas e completas. ■

2

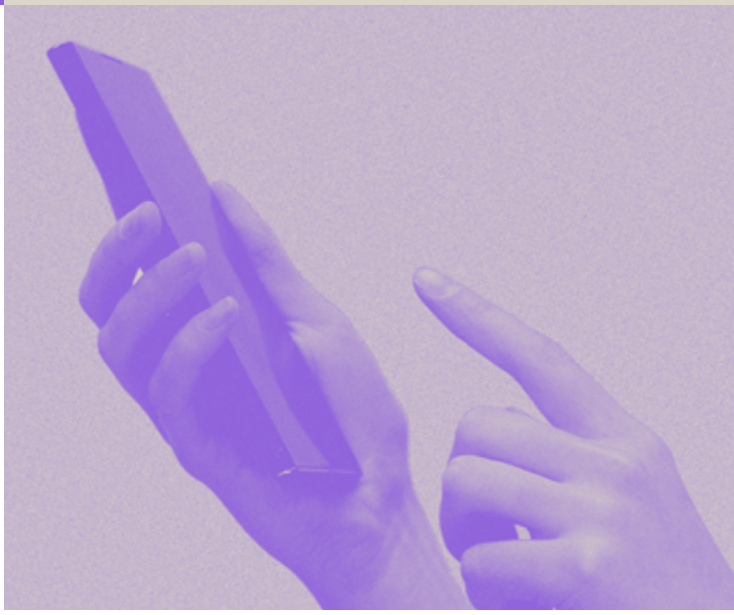
O QUE PODE ACONTECER SE AS MEDIDAS DE CIBERSEGURANÇA NÃO FOREM ADOTADAS?

Além dos riscos diretos para o negócio, a ausência de medidas adequadas de segurança pode acarretar consequências regulatórias.

Mesmo não havendo ainda um marco legal específico para a cibersegurança, cuidar de forma segura dos segredos de negócios, informações de clientes e de dados pessoais dos indivíduos é medida necessária conforme: (i) leis mais abrangentes, como o Código Civil, o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet, a Lei de Propriedade Industrial e a Lei Geral de Proteção de Dados (LGPD); (ii) normalmente, exigido de forma contratual; e (iii) em diversos setores regulados, como o Financeiro, o de Telecomunicações e o de Seguros e Saúde.

Para dados pessoais, a LGPD é uma das principais normas que **regulamenta** a cibersegurança no Brasil, exigindo que as empresas tratem os dados pessoais com o devido cuidado e segurança, respeitando as expectativas dos seus titulares.

Se a empresa não implementar as práticas de segurança necessárias, o tratamento dos dados será considerado irregular, o que pode resultar em **sanções da Autoridade Nacional de Proteção de Dados** (ANPD). Dentre as pena-



lidades, destacam-se o bloqueio do tratamento de dados até que as falhas sejam corrigidas — o que pode paralisar as operações — e multas de até 2% do faturamento da empresa, descontados os impostos.

Os riscos não param por aí. O S**uperior Tribunal de Justiça** (STJ) recentemente reforçou o conceito de **responsabilidade proativa**. Isso significa que, ao não adotar medidas de segurança adequadas, a empresa pode ser responsabilizada civilmente pelos danos causados por incidentes de segurança, incluindo ciberataques. ■

3 COMO PROTEGER A SUA EMPRESA?

Antes de tudo, é fundamental compreender que a cibersegurança não é uma solução imediata, mas uma questão de **gerenciamento de riscos**. Não existe uma "bala de prata" que resolva todos os problemas de uma vez. Os riscos e as capacidades de cada empresa variam, influenciando diretamente as **medidas de segurança digital** a serem adotadas. Isto é, a estratégia de cibersegurança deve ser personalizada de acordo com as particularidades do negócio, considerando o porte, os dados tratados e as possíveis ameaças a que está exposto.

A **ANPD** publicou um manual e um checklist específicos para os agentes de tratamento de pequeno porte, como a Pequenas e Médias Empresas (PMEs). O documento traz orientações detalhadas sobre as ações que devem ser implementadas para garantir a **proteção dos dados** pessoais de forma segura e em conformidade com a LGPD.

A adoção dessas práticas não é apenas uma recomendação, mas uma necessidade. De acordo com o Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte, a implementação dessas medidas é vista como "adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano". Isso denota o comprometimento da empresa com a segurança e a proteção dos dados, ajudando a evitar sanções e a manter a **conformidade com a legislação**.


4
CONHEÇA
AS MEDIDAS
PREVISTAS
NO MANUAL

Neste capítulo, apresentaremos as principais **medidas de cibersegurança** que você pode adotar para proteger a empresa contra os **riscos digitais**. Com o aumento das ameaças à segurança, é preciso agir de forma estratégica, implementando, primeiro, ações urgentes e avançando conforme as necessidades do negócio. As dicas a seguir ajudarão você a fortalecer a proteção de dados e os sistemas e informações, garantindo a continuidade das operações e a confiança dos clientes.

Cibersegurança é, antes de tudo, uma questão de **gestão de riscos**. Caso não consiga implementar todas as medidas de segurança de imediato, o ideal seria começar com as mais urgentes. Avalie as necessidades específicas da sua organização e implemente, primeiro, as ações mais importantes.

O manual da ANPD oferece diversas **medidas recomendadas** para agentes de tratamento, com foco em pequenos negócios. A seguir, destacamos algumas dessas ações que podem fortalecer a segurança do negócio e reduzir riscos.

4.1 ELABORAÇÃO E IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A primeira medida para a segurança do seu negócio é a **criação e a implementação de uma Política de Segurança da Informação**, que deve ser clara e acessível, com diretrizes específicas sobre como proteger dados e informações sensíveis.

Além disso, é fundamental que todos os **colaboradores sejam treinados** para compreender e seguir as regras estabelecidas, garantindo que a segurança da informação seja incorporada à rotina da companhia. As pessoas costumam ser o elo mais vulnerável na cadeia de cibersegurança: atualmente, 17% dos ataques a pequenos negócios têm origem em *phishing*, enquanto 88% dos incidentes são resultados de erros humanos ou uso inadequado de ativos digitais. Por isso, é imprescindível investir na criação de uma Política de Segurança da Informação clara e eficiente, além de treinar os colaboradores para segui-la corretamente. Isso reduzirá os riscos de falhas provocadas por comportamentos descuidados.

4.2 REALIZAÇÃO PERIÓDICA DE CÓPIAS DE SEGURANÇA

Outra prática importante é **fazer cópias de segurança** (*backups*) de forma **regular e sistemática**. Essas cópias devem ser armazenadas de maneira **segura e offline**, ou seja, em um ambiente físico ou lógico distinto do original, garantindo que os dados estejam protegidos, mesmo em caso de falhas no sistema principal ou incidentes cibernéticos. A **periodicidade** das cópias precisa ser definida conforme a importância e a frequência das atualizações dos dados.

Em caso de ataques que comprometam a disponibilidade dessas informações, como é o caso do *ransomware*, é vital a manutenção de *backups* seguros. Dispor de cópias de segurança em um ambiente separado e protegido garante que a empresa possa recuperar rapidamente os dados e retomar as operações, minimizando os prejuízos. Portanto, é fundamental implementar uma rotina de cópias de segurança para garantir a continuidade do negócio.

4.3 CONTROLES RIGOROSOS DE AUTENTICAÇÃO

A **autenticação de usuários** é basilar para garantir que apenas pessoas autorizadas tenham acesso a sistemas e informações da empresa. Para isso, é necessário gerar **senhas fortes**, que devem ter entre 10 e 12 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, a senha deve ser alterada no **primeiro acesso**, sendo a sua reutilização **proibida**.

Recomenda-se ainda a adoção da **Autenticação Multifator** (MFA), que adiciona uma camada extra de segurança, exigindo mais de um método de verificação para validar a identidade do usuário. O uso da MFA pode reduzir o risco de comprometimento de contas em até 99%.

4.4 CONTROLE DE ACESSO E CRIPTOGRAFIA DE DADOS

É importante também que a empresa implemente **controles de acesso rigorosos**, garantindo que cada usuário tenha somente as permissões necessárias para desempe-

nhar a própria função. Esse controle limita o acesso a informações sensíveis, minimizando riscos de vazamentos ou uso indevido. Além disso, é fundamental a **criptografia dos dados pessoais em repouso** (armazenados) para garantir que, mesmo em caso de acesso não autorizado, as informações não possam ser lidas ou usadas indevidamente.

4.5 GARANTIA DE COMUNICAÇÕES E REDES SEGURAS

Uma das principais medidas de segurança digital é garantir que todas as **comunicações e redes** da empresa estejam **seguras**. Isso inclui assegurar que os dados sejam transmitidos por canais **criptografados** (como o **HTTPS**), evitando que informações sensíveis sejam acessadas por terceiros não autorizados. É válido também implementar um ***firewall*** (ou Web Application Firewall) adequadamente configurado, protegendo os sistemas contra acessos externos indesejados. É preciso, ainda, eliminar a exposição desnecessária de dados ao público.

4.6 ATUALIZAÇÃO CONTÍNUA DE SISTEMAS E APLICATIVOS

Manter sistemas e aplicativos **sempre atualizados** também é uma **prática** de cibersegurança. As **atualizações** periódicas ajudam a corrigir falhas conhecidas, protegendo a empresa contra vulnerabilidades que possam ser exploradas por cibercriminosos. Além disso, é importante garantir que todas as atualizações sejam feitas de forma rápida e eficiente, sem afetar a continuidade das operações.

4.7 IMPLEMENTAÇÃO DE SOLUÇÕES 'ANTIMALWARE' E ANTIVÍRUS

A adoção e a **atualização constante de soluções *anti-malware*** ou **antivírus** é obrigatória para proteger os sistemas da empresa contra ameaças digitais. Essas ferramentas devem ser configuradas para realizar **varreduras periódicas**, identificando e removendo softwares maliciosos, antes que causem danos a dados ou sistemas. Lembre-se de manter essas soluções **atualizadas**.

E não se esqueça: o *malware* é uma das principais causas de incidentes em pequenos negócios, representando 18%

dos ataques. Portanto, garantir a proteção contínua desses sistemas é uma prioridade para evitar riscos.

4.8 REGISTRO E MONITORAMENTO DE ACESSOS E AÇÕES

A empresa também precisa implementar **sistemas de registro** (*logs*) apropriados para **monitorar acessos** e, quando possível, **ações realizadas** nos sistemas. Esses registros ajudam a detectar comportamentos suspeitos e facilitam a análise e a investigação de incidentes. Se possível, é recomendada a implementação do **Security Information and Event Management** (SIEM). Essa é uma solução que permite a **guarda** e o **monitoramento** contínuo desses *logs*, expandindo a capacidade de resposta a ameaças.

4.9 GARANTIAS AO CONTRATAR SERVIÇOS EM NUVEM

Quando a empresa contrata **serviços em nuvem**, é preciso garantir que o provedor ofereça **garantias de segurança** adequadas. Isso inclui a verificação de **Acordos de Nível de Serviço** (SLA) que garantam a **disponibilidade** e o **controle**

de acesso aos dados armazenados. Certifique-se também de que o provedor tenha políticas fortes de **segurança** e **autenticação**, atendendo aos requisitos necessários para proteger as informações do negócio.

4.10 PROTEÇÃO PARA DISPOSITIVOS MÓVEIS

Com o aumento do uso de **dispositivos móveis** no ambiente corporativo, adote controles específicos para proteger as informações armazenadas e transmitidas por esses aparelhos. Além disso, garanta que os **acessos a aplicativos e sistemas corporativos** sejam protegidos por **MFA** e, sempre que possível, separe os dispositivos pessoais dos usados no trabalho, o que minimiza ameaças de exposição de dados sensíveis. Também é importante adotar mecanismos que permitam o **bloqueio** e o **apagamento remoto** de dados em caso de perda ou roubo. Isso garante que informações críticas não caiam em mãos erradas. ■

QUER SABER MAIS?

Leia o **Guia da ANPD** e o **Checklist de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte**.


CONCLUSÃO

A cibersegurança é uma necessidade real e urgente para proteger a empresa contra as ameaças crescentes do ambiente online. Independentemente do tamanho do negócio, adotar medidas de segurança adequadas é elementar para proteger dados, garantir a continuidade das operações e reforçar a confiança dos clientes. As práticas recomendadas, apresentadas neste material, podem ser implementadas conforme a realidade de cada negócio, sempre com foco na gestão de riscos.

A ausência de estratégias de proteção pode levar a consequências graves, como o comprometimento da integridade dos dados e a perda de confiança no mercado. Isso não só impacta financeiramente a empresa como também prejudica a sua imagem perante clientes, fornecedores e parceiros. Portanto, além de tratar-se de uma questão de conformidade com normas legais, investir em segurança cibernética mostra-se uma estratégia básica para a sustentabilidade do negócio.

O processo de implementação pode parecer desafiador, mas não precisa ser feito de uma vez. Comece com as medidas mais urgentes e, gradualmente, adote as demais conforme as necessidades específicas. As ações descritas visam proporcionar uma base sólida de pro-

teção, mesmo para empresas que estejam começando a fortalecer as defesas cibernéticas.

Proteger a empresa contra riscos cibernéticos é uma decisão inteligente e necessária. Ao adotar as práticas certas, você tomará um passo importante para garantir a segurança e a continuidade do negócio, evitando surpresas desagradáveis e mantendo a confiança do seu público. ■

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo para agentes de tratamento de pequeno porte*. Disponível em: https://www.gov.br/anpd. Acesso em março de 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Checklist de medidas de segurança para agentes de tratamento de pequeno porte*. Disponível em: https://www.gov.br/anpd. Acesso em março de 2025.

BRASIL. Lei 13.709, de 14 de agosto de 2018. *Diário Oficial da União* (DOU): seção 1, Brasília, DF, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em março de 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). "Jurisprudência sobre responsabilidade proativa em segurança da informação". Disponível em: https://www.stj.jus.br. Acesso em março de 2025.

FICHA TÉCNICA

RONY VAINZOF

Consultor de Proteção de Dados da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP) e sócio do VLK Advogados

---

CAIO LIMA

Consultor de Proteção de Dados da FecomercioSP e sócio do VLK Advogados

---

JEAN SANTANA

Advogado do VLK Advogados

FECOMERCIOSP

PUBLICAÇÃO DA FEDERAÇÃO
DO COMÉRCIO DE BENS, SERVIÇOS
E TURISMO DO ESTADO DE SÃO PAULO