

E-BOOK

OS 6 MAIORES DESAFIOS DE REDE NAS PMES E COMO SOLUCIONÁ-LOS DE FORMA EFICIENTE

RESUMO:

Este e-book foi desenvolvido para servir como um guia estratégico para pequenas e médias empresas, auxiliando o entendimento de como as novas tendências e tecnologias em redes podem ser aplicadas de forma prática e eficaz, apoiando a transformação digital de seus negócios. Vamos explorar desde os fundamentos de arquiteturas como SD-WAN e MPLS até os desafios de segurança e a crescente adoção de dispositivos IoT. Além disso, abordaremos como criar uma rede escalável, capaz de acompanhar o crescimento dos negócios, e como garantir que a segurança de dados seja uma prioridade constante. Seja para melhorar a conectividade interna ou preparar sua infraestrutura para o futuro.

A importância de uma rede resiliente e segura para o crescimento operacional das pmes

Em um cenário global onde a digitalização e a transformação tecnológica se tornaram temas centrais na estratégia empresarial, as pequenas e médias empresas (PMEs) enfrentam desafios únicos no que diz respeito à gestão e proteção de suas redes de dados, para manter suas operações eficientes, seguras e escaláveis, enquanto lidam com a pressão das mudanças digitais cada vez mais aceleradas.

De acordo com a pesquisa da FGV Projetos em parceria com a Agência Brasileira de Desenvolvimento Industrial (ABDI) revelou que dois terços das micro e pequenas empresas (66%) estão em estágios iniciais de maturidade digital. O estudo destaca que, para 38% das empresas, o maior entrave para a transformação digital é a falta de recursos financeiros, por esse fato, acabam enfrentando dificuldades relacionadas à infraestrutura de TI e conectividade essenciais para adoção de novas tecnologias e aplicar inovação. Esse descompasso entre necessidade e capacidade de implementação cria um ambiente propício para problemas que vão desde interrupções no serviço até vulnerabilidades críticas de segurança.

(Fonte: <https://www.abranet.org.br/publicacoes/noticias/3839>)



Fonte: <https://designbundles.net/liligraphie/2778649-ai-robot-and-human-hands-touching-artificial-intel>

A rede de uma empresa é o alicerce sobre o qual a infraestrutura tecnológica é construída, desempenhando um papel fundamental na conectividade interna e na interação com clientes, parceiros e fornecedores. De acordo com dados recentes, as pequenas e médias empresas (PMEs) enfrentaram quase 200 milhões de ciberataques em 2023, evidenciando a importância de uma rede robusta e confiável para suas operações diárias. Para essas empresas, falhas de conectividade ou problemas de segurança podem resultar em prejuízos financeiros diretos e danos à reputação, afetando tanto a produtividade quanto o crescimento sustentável.

(Fonte: <https://minutodaseguranca.blog.br/pmes-foram-alvo-de-quase-200-milhoes-de-ciberataques-em-2023>)

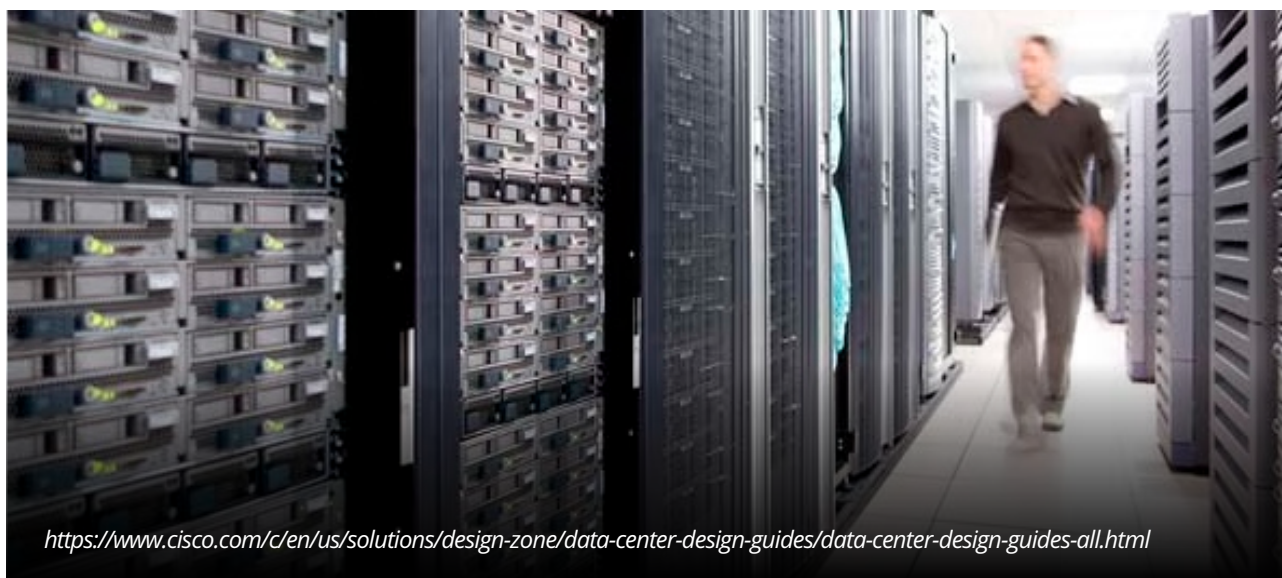
As redes definidas por software (SDN), arquiteturas de nuvem híbrida e soluções de segurança integrada como o Secure Access Service Edge (SASE) estão entre as inovações que podem transformar a operação das PMEs, reduzindo custos operacionais e aumentando a eficiência. Dessa forma, a prioridade se torna clara: é essencial investir em uma infraestrutura de rede moderna e flexível, que permita a integração com novas soluções de tecnologia, ao mesmo tempo que garanta segurança robusta.

Por fim, para líderes de TI, a segurança da rede se destaca como uma das maiores preocupações, onde as PMEs são especialmente vulneráveis a ataques cibernéticos, muitas vezes por falta de recursos tecnológicos e expertise para implementar soluções de cibersegurança de ponta. Além disso, a crescente demanda por acesso remoto e a expansão do trabalho híbrido aceleraram ainda mais a necessidade de soluções que não apenas protejam os dados da empresa, mas também garantem conectividade de alta performance, independentemente da localização de seus colaboradores. A adoção de soluções como SD-WAN, VPNs seguras e firewalls de última geração estão se tornando uma realidade não apenas para grandes corporações, mas também para PMEs que buscam competitividade em seu segmento de atuação, acompanhando um mundo cada vez mais digital.

Desafio 1: Conectividade Intermitente – Causas e soluções simples de infraestrutura

A conectividade intermitente é um dos problemas mais comuns enfrentados pelas pequenas e médias empresas (PMEs) no Brasil, impactando diretamente a produtividade e a eficiência dos negócios. Essa falha pode gerar atrasos no atendimento ao cliente, dificuldades no uso de sistemas em nuvem e até perdas em transações online. Alguns fatores, como infraestrutura inadequada geralmente estão na raiz do problema, mas podem ser resolvidos com ajustes relativamente simples e de baixo custo.

Figura 1 - Conectividade de redes



Entre as principais causas de conectividade intermitente estão:

- Redes mal configuradas;
- Uso de equipamentos obsoletos;
- Falta de redundância e Monitoramento no acesso à internet.

Muitos roteadores e switches utilizados pelas PMEs não são dimensionados para suportar o volume de tráfego que uma empresa em crescimento exige. Além disso, o crescimento da quantidade de dispositivos conectados, como notebooks, smartphones e dispositivos IoT, sobrecarrega ainda mais a infraestrutura existente. É comum que empresas menores invistam pouco em auditorias de rede e diagnósticos técnicos, o que faz com que problemas pequenos, como interferências de sinal Wi-Fi ou cabos mal conectados, resultem em interrupções constantes.

Para resolver esse problema, algumas soluções simples podem ser implementadas. O primeiro passo é realizar uma análise detalhada da rede, identificando gargalos de desempenho. Ferramentas de monitoramento de tráfego, como Zabbix ou PRTG, podem ajudar a identificar onde ocorrem os principais pontos de falha, porém, soluções que envolvem serviços profissionais qualificados somadas a ferramentas de análise e diagnóstico de rede, tornam-se extremamente eficazes para identificar gargalos e problemas, além de indicar as melhores ações e investimentos para aumentar a qualidade da rede, como a solução [Hackone Network Quality](#).

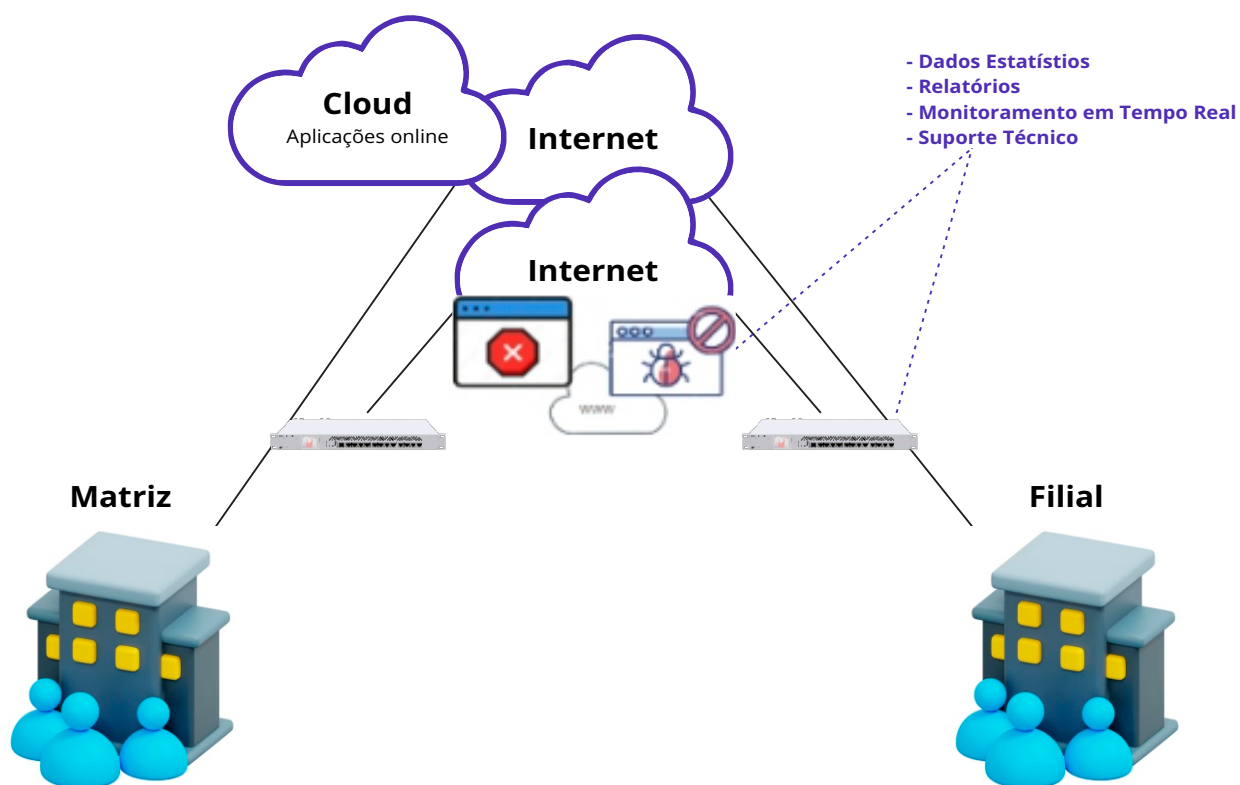
Outra solução eficaz é a adoção de uma infraestrutura de rede mais moderna e escalável, como a implementação de switches gerenciáveis e roteadores com suporte a redes de alta velocidade, como Wi-Fi 6. Além disso, a configuração de uma solução de redundância de links, como a utilização de duas operadoras de internet (dual WAN) somadas a soluções inteligentes de tratamento destes links como SD-WAN, pode garantir que, caso um serviço caia ou tenha perda de qualidade, outro assuma imediatamente, minimizando o tempo de inatividade. Essas ações preventivas não só garantem uma rede mais estável, como também proporcionam à empresa a base necessária para crescer de forma sustentável e segura no ambiente digital.

Desafio 2: Falta de Segurança na Rede – Soluções de firewall, VPN, e monitoramento de tráfego.

A falta de segurança na rede é um dos desafios mais críticos enfrentados pelas pequenas e médias empresas. Com o aumento dos ataques cibernéticos, as PMEs se tornam alvos fáceis, muitas vezes devido à ausência de sistemas de defesa robustos. Para evitar essas ameaças e proteger dados valiosos, é essencial que as PMEs invistam em soluções como firewalls, VPNs e monitoramento de tráfego.

Os firewalls realizam a primeira linha de defesa contra invasões e ameaças externas. Um firewall atua como uma barreira entre a rede interna e o mundo externo, filtrando o tráfego de dados e bloqueando acessos não autorizados. No entanto, muitas PMEs ainda utilizam firewalls simples, que oferecem pouca proteção contra ataques avançados, como tentativas de phishing, ransomware e ataques distribuídos de negação de serviço (DDoS), ou ainda utilizam equipamentos de roteamento de internet básico achando que estão protegidos com serviços de firewall. A solução ideal é implementar firewalls de última geração (Next-Generation Firewalls, ou NGFWs), que não só analisam pacotes de dados, mas também monitoram o comportamento do tráfego em tempo real, identificando anomalias e bloqueando automaticamente atividades suspeitas.

Figura 2 - Solução de proteção de perímetro utilizando firewall e soluções da Fortinet como serviços - SureNet



Fonte: <https://hackone.com.br/consultoria-ficha-tecnica-sure-net>

Outro ponto crítico para fortalecer a segurança da rede é a adoção de redes privadas virtuais (VPNs). Com o aumento do trabalho remoto e da mobilidade, a necessidade de acessar a rede corporativa de locais externos se tornou uma realidade. As VPNs garantem que os dados trafegam por um túnel criptografado, protegendo informações sensíveis contra interceptações. O uso de VPNs deve ser complementado com uma autenticação multifator (MFA), que oferece uma camada adicional de segurança ao exigir que os usuários confirmem sua identidade através de vários métodos, como senha e autenticação por aplicativo.

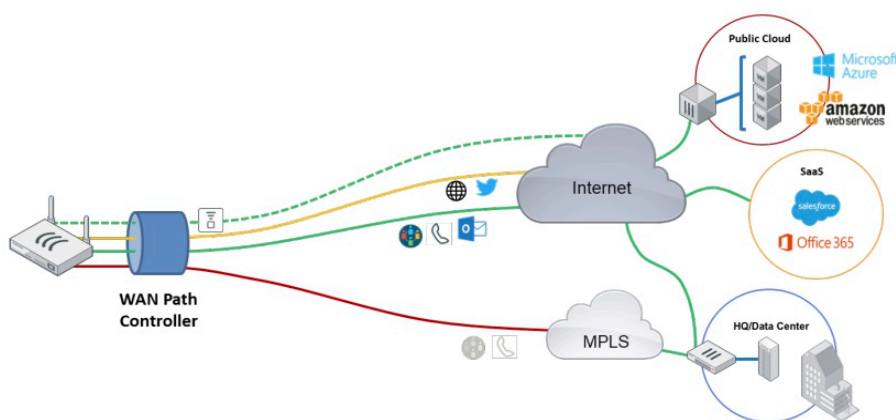
Por fim, o monitoramento constante do tráfego de rede é crucial para identificar e mitigar ameaças antes que elas causem danos. Ferramentas como o SolarWinds ou o Zabbix oferecem visibilidade completa sobre o comportamento da rede, permitindo que os administradores de TI detectem atividades incomuns, como picos inesperados de tráfego ou tentativas de acesso em horários anormais. Além disso, esses sistemas podem ser configurados para alertar automaticamente a equipe de TI quando uma ameaça é detectada, permitindo uma resposta rápida. Investir nessas soluções não só protege a operação da empresa, mas também garante que a rede permaneça segura e eficiente, mesmo diante de novos desafios.

A combinação de firewalls robustos, VPNs seguras e um monitoramento eficaz cria uma barreira de proteção sólida, essencial para qualquer PME que queira proteger seus ativos digitais e manter a confiança de seus clientes.

Desafio 3: Baixa Performance de Rede – Como otimizar o desempenho com SD-WAN e balanceamento de carga.

A baixa performance de rede é um problema que impacta diretamente a produtividade e a experiência dos usuários em PMEs, resultando em atrasos operacionais e frustração de colaboradores e clientes. À medida que as PMEs adotam mais aplicações em nuvem, ferramentas colaborativas e serviços digitais, a demanda sobre a rede aumenta, e quando essa não é capaz de suportar tais exigências, os tempos de resposta se alongam, a comunicação interna é prejudicada e a eficiência da empresa diminui. Para enfrentar esse desafio, tecnologias como SD-WAN e o balanceamento de carga se apresentam como soluções eficazes para otimizar o desempenho da rede e garantir uma operação contínua.

Figura 3 - Solução SD-WAN da Fortinet



Fonte: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf

A SD-WAN (Software-Defined Wide Area Network) transforma a maneira como as redes são gerenciadas, oferecendo maior flexibilidade e controle sobre o tráfego de dados. Diferente das redes WAN tradicionais, que dependem de links físicos e roteamentos fixos, a SD-WAN utiliza uma abordagem inteligente, priorizando o tráfego conforme a necessidade e otimizando o uso dos recursos disponíveis. Com essa tecnologia, uma PME pode utilizar simultaneamente diferentes tipos de conexões, como MPLS, 4G/5G e banda larga, garantindo uma rede mais resiliente e de alta performance. Além disso, a SD-WAN permite a criação de políticas de priorização, onde o tráfego mais crítico, como o de aplicativos financeiros ou de comunicação, recebe prioridade sobre o tráfego menos essencial, como downloads de arquivos.

O balanceamento de carga é outra estratégia eficaz para melhorar o desempenho da rede. Ele distribui o tráfego de forma equilibrada entre múltiplos servidores ou links de internet, evitando sobrecargas e garantindo que os recursos sejam utilizados de maneira eficiente. Em muitas PMEs, é comum que um único link de internet seja responsável por todo o tráfego, o que aumenta as chances de congestionamento e falhas. Implementar o balanceamento de carga permite que diferentes caminhos sejam usados de forma dinâmica, distribuindo o tráfego e maximizando a velocidade de acesso. Uma solução prática e acessível é configurar o balanceamento entre diferentes provedores de internet, combinando links de banda larga e 4G/5G, por exemplo. Isso melhora a performance e garante a continuidade do serviço em caso de falha em um dos links.

Essas tecnologias se complementam, criando uma rede mais ágil e responsiva, capaz de lidar com as crescentes demandas das PMEs sem comprometer a qualidade do serviço. Ao investir em soluções como SD-WAN e balanceamento de carga, as PMEs não apenas solucionam problemas de performance, mas também criam uma base sólida para crescer e inovar, adaptando-se rapidamente às exigências de um mercado digital cada vez mais competitivo.

Desafio 4: Problemas com Wi-Fi Corporativo – Melhores práticas para garantir cobertura e estabilidade.

O Wi-Fi corporativo é um dos pilares da operação moderna em pequenas e médias empresas (PMEs), mas também é fonte frequente de frustração devido a problemas de cobertura e instabilidade. Um estudo da Cisco revelou que 53% das PMEs enfrentam dificuldades com a performance e confiabilidade de suas redes sem fio, resultando em interrupções no trabalho e perda de produtividade. Com o aumento do número de dispositivos conectados, como smartphones, notebooks e IoT, garantir uma rede Wi-Fi robusta, estável e com cobertura adequada tornou-se um desafio crescente para muitas empresas. Contudo, existem práticas eficazes que podem ser adotadas para melhorar a performance e garantir que o Wi-Fi atenda às demandas corporativas.

Um dos principais problemas que as PMEs enfrentam é a falta de cobertura adequada, principalmente em espaços maiores ou com várias divisões físicas. Para resolver essa questão, a primeira etapa é o planejamento adequado da rede Wi-Fi. Um erro comum é depender de um único roteador para cobrir toda a área, o que não é suficiente para ambientes de escritórios amplos ou com muitos obstáculos, como paredes e móveis. A solução mais indicada é a implementação de access points (APs) adicionais, estrategicamente distribuídos pelo ambiente para garantir cobertura uniforme. Ferramentas de análise de cobertura de Wi-Fi, como o Ekahau ou NetSpot, podem ser utilizadas para mapear áreas de sombra ou pontos com sinal fraco, facilitando o planejamento e a disposição dos APs de maneira eficiente.

Também é possível realizar um estudo prévio de como ficaria a cobertura de sinal wireless de um determinado ambiente mesmo antes de comprar os equipamentos e instalá-los, garantindo maior precisão no investimento, determinando o melhor modelo de Access Point (AP), as quantidades necessárias e posicionamento, pode-se aplicar esse trabalho também para redes existentes, sugerir o remanejamento ou aquisição de novos pontos de acesso para corrigir áreas de sombra, tal prática é chamada de Wireless Site Survey Preditivo (WSSP), que é realizado utilizando ferramentas especializadas e serviços profissionais de especialistas wireless para executar tal análise preditiva e elaboração do relatório.

A Hackone oferece o serviço de Wireless Site Survey para até 50 Access Point de forma gratuita através do link: [Adicionar o link do Wireless Site Survey Preditivo \(WSSP\)](#)

Figura 4 - Exemplo de Wireless Site Survey utilizando o Ekahau



Fonte: <https://www.ekahau.com/blog/introducing-survey-2-0-and-pro-10-4/>

Além da cobertura, a estabilidade do sinal Wi-Fi é outro ponto crítico. A interferência de outros dispositivos, como telefones sem fio, micro-ondas e até redes Wi-Fi vizinhas, pode causar quedas de conexão e flutuações de velocidade. Uma solução simples para mitigar esse problema é a escolha adequada dos canais de frequência. Em áreas congestionadas, o uso de canais sobrepostos pode degradar significativamente a performance da rede. A utilização de equipamentos que suportem a banda de 5 GHz, além da tradicional 2.4 GHz, pode reduzir a interferência e proporcionar maior velocidade e estabilidade, já que a banda de 5 GHz oferece mais canais e é menos propensa a interferências externas.

Outra boa prática é o uso de redes Wi-Fi gerenciadas. Para PMEs, a implementação de soluções de gerenciamento centralizado, como o UniFi da Ubiquiti ou o Aruba Instant On, pode simplificar a administração e monitoramento da rede. Essas plataformas permitem gerenciar vários APs de forma unificada, ajustar automaticamente os canais de frequência, priorizar o tráfego de dados e até detectar e mitigar interferências em tempo real. Além disso, é fundamental garantir que o firmware dos dispositivos Wi-Fi esteja sempre atualizado, pois as atualizações geralmente trazem melhorias de performance e segurança.

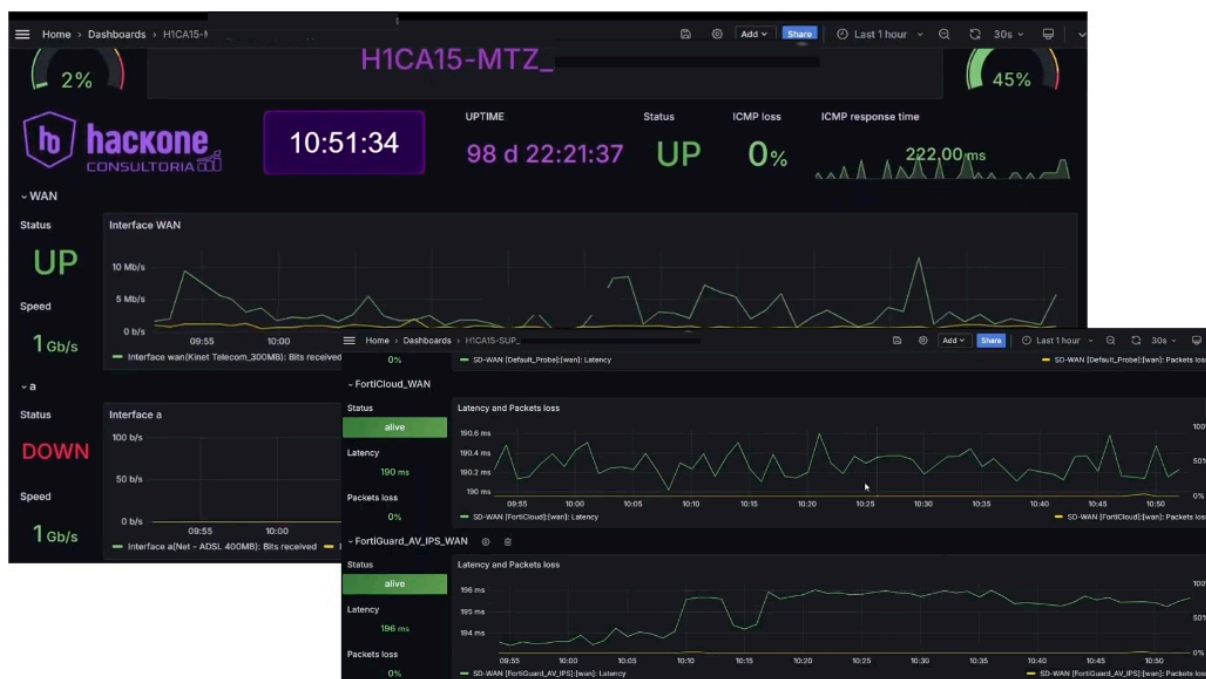
Adotar essas melhores práticas não só resolve problemas imediatos de cobertura e instabilidade, mas também prepara a empresa para futuras demandas, garantindo que a rede Wi-Fi seja escalável e capaz de suportar o crescimento da organização. Com uma rede sem fio bem projetada e gerenciada, as PMEs podem operar com mais eficiência e oferecer uma melhor experiência de conectividade a seus colaboradores e clientes.

Desafio 5: Falta de Gestão e Monitoramento de Ativos – Como implementar uma solução de gestão de dispositivos e redes.

A falta de gestão e monitoramento de ativos é um desafio crítico enfrentado por muitas pequenas e médias empresas (PMEs), resultando em ineficiências operacionais, maior risco de segurança e dificuldades em manter a continuidade dos negócios. Sem um sistema estruturado de gestão de ativos de TI, é comum ocorrerem falhas inesperadas e a incapacidade de identificar problemas antes que se tornem críticos. A implementação de uma solução de gestão de dispositivos e redes melhora a visibilidade sobre os recursos em uso, permitindo um melhor planejamento e alocação de recursos, o que resulta em uma operação mais eficiente.

A primeira etapa para implementar uma solução de gestão de ativos é realizar um inventário detalhado de todos os dispositivos e equipamentos de rede existentes, incluindo não apenas servidores e roteadores, mas também impressoras, dispositivos móveis e equipamentos IoT. Softwares especializados podem ser utilizados para automatizar essa tarefa, identificando e catalogando os dispositivos na rede de forma rápida e eficaz. Isso ajuda as empresas a saber exatamente o que possuem, facilitando a identificação de equipamentos obsoletos que precisam de atualização ou substituição. Além disso, um inventário bem estruturado facilita o planejamento financeiro, permitindo que as PMEs façam investimentos mais estratégicos e inteligentes.

Figura 5 - Sistema de Monitoramento da Hackone (Centro de Operações - COP)



Fonte: Hackone

Após o inventário, é fundamental implementar uma solução de monitoramento contínuo para acompanhar o desempenho e a saúde dos ativos de rede. Ferramentas de monitoramento possibilitam verificar a performance em tempo real, detectar falhas e receber alertas automáticos sobre problemas potenciais. Isso não apenas previne falhas, mas também permite uma resposta mais ágil a incidentes. Por exemplo, se um servidor apresentar lentidão, a equipe de TI pode ser notificada imediatamente, permitindo ações corretivas antes que o problema afete os usuários finais. O monitoramento contínuo também gera dados históricos, que podem ser analisados para identificar tendências e otimizar a operação da rede.

Outro aspecto importante da gestão de ativos é a segurança. Dispositivos não monitorados podem se tornar alvos fáceis para ataques cibernéticos, especialmente se estiverem desatualizados ou mal configurados. Para mitigar esse risco, é essencial implementar políticas de segurança de rede, incluindo a atualização regular de firmware e software, além de auditorias periódicas de segurança. Adicionalmente, o uso de soluções de gestão de identidade e acesso (IAM) ajuda a controlar quem tem acesso a determinados dispositivos e dados, reduzindo o risco de acessos não autorizados.

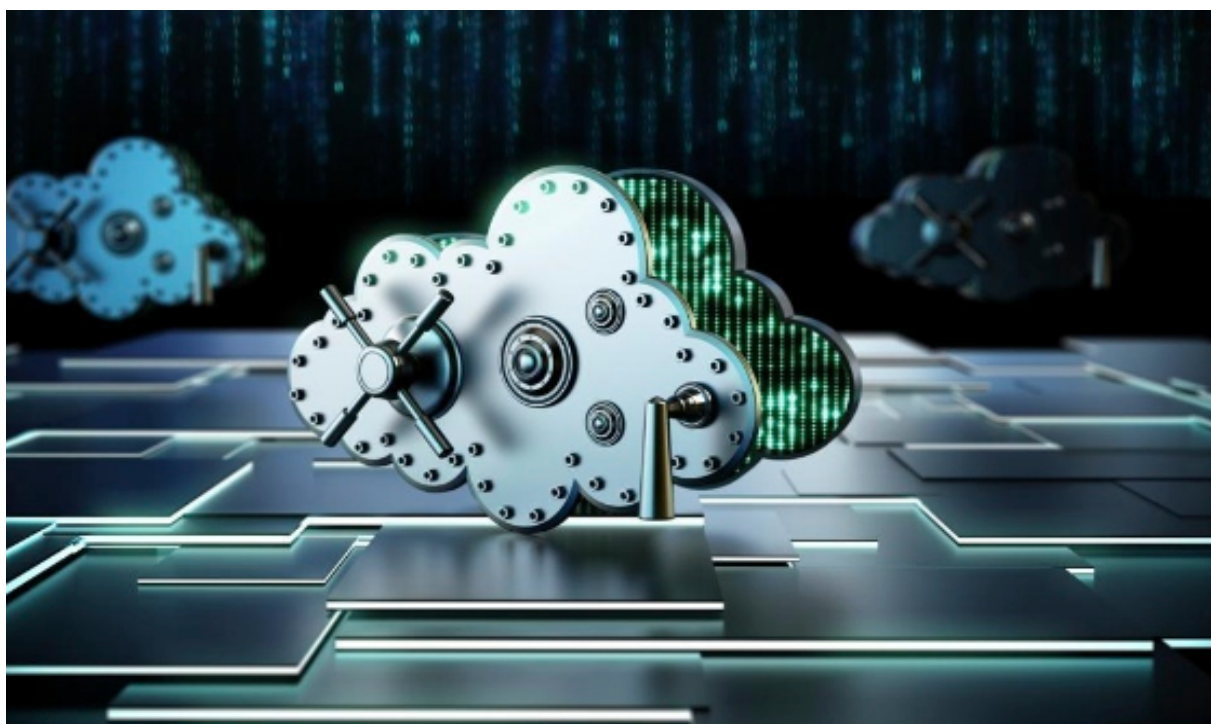
A implementação de uma solução eficaz de gestão e monitoramento de ativos pode transformar a operação de uma PME, trazendo maior eficiência, segurança e capacidade de resposta a incidentes. Ao investir em tecnologia e processos para gerenciar seus dispositivos de rede, as PMEs não só melhoram sua operação atual, como também se preparam para os desafios futuros, assegurando um crescimento sustentável e protegido no ambiente digital.

Desafio 6: Dificuldade em Escalar a Rede – Soluções de expansão com cloud e virtualização.

Em um ambiente de negócios em constante evolução, a dificuldade de escalar a rede é um dos principais desafios enfrentados pelas pequenas e médias empresas (PMEs). À medida que as demandas de mercado aumentam e novos serviços digitais são introduzidos, é essencial que a infraestrutura de TI acompanhe esse crescimento sem comprometer o desempenho e a segurança. A incapacidade de expandir as redes de forma adequada pode resultar em perda de oportunidades de negócios e aumento nos custos operacionais. Nesse contexto, a adoção de soluções em nuvem e virtualização surge como uma estratégia eficaz para superar essas barreiras e permitir uma expansão flexível e sustentável.

A computação em nuvem oferece uma alternativa poderosa para as PMEs que buscam escalar suas operações. Ao migrar serviços e aplicações para a nuvem, as empresas eliminam a necessidade de manter uma infraestrutura física robusta, reduzindo custos com hardware e manutenção. A nuvem permite que as PMEs ajustem rapidamente seus recursos de acordo com as necessidades do negócio, como aumentar a capacidade de armazenamento ou escalar aplicações para atender a picos de demanda. Provedores de serviços em nuvem oferecem modelos de pagamento por uso, permitindo que as empresas paguem apenas pelo que utilizam, tornando essa solução financeiramente acessível e eficiente.

Figura 6 - Computação em Nuvem



Fonte: Blog Hackone - <https://blog.hackone.com.br/2024/07/31/introducao-a-computacao-em-nuvem-transformando-o-futuro-da-tecnologia/>

A virtualização também desempenha um papel crucial no crescimento eficiente das PMEs. Com essa tecnologia, várias máquinas virtuais (VMs) podem ser executadas em um único servidor físico, otimizando o uso de recursos e permitindo uma gestão mais eficaz da infraestrutura de TI. Isso não só reduz os custos operacionais, como também melhora a flexibilidade. As empresas podem provisionar novas VMs rapidamente para suportar novos serviços ou aplicações, sem precisar adquirir hardware adicional. Além disso, a virtualização facilita a criação de ambientes de teste e desenvolvimento, permitindo inovações contínuas sem afetar as operações principais.

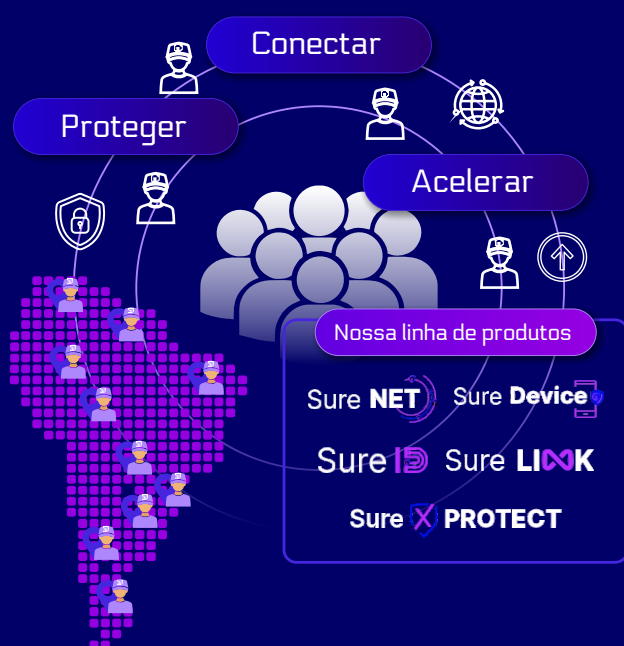
Outro grande benefício da adoção de soluções em nuvem e virtualização é a facilidade de implementação de políticas de segurança e backup. Provedores de nuvem geralmente oferecem soluções integradas de segurança, como criptografia de dados e autenticação multifator, garantindo a proteção das informações da empresa. Os backups automáticos na nuvem garantem que dados críticos sejam preservados e recuperáveis em caso de incidentes, proporcionando maior segurança e tranquilidade. Com isso, as equipes de TI podem se concentrar em estratégias de crescimento, sem a preocupação constante com a manutenção da infraestrutura.

A implementação de soluções em nuvem e virtualização permite que as PMEs escalem suas operações de maneira eficiente, tornando-se mais ágeis e resilientes em um mercado dinâmico. Ao ajustar rapidamente seus recursos e serviços, as empresas estão melhor posicionadas para aproveitar oportunidades de mercado e atender às demandas de seus clientes. Investir nessas tecnologias garante um crescimento sustentável e seguro, fortalecendo a presença das PMEs em um mercado cada vez mais competitivo.

Garanta uma Análise na Sua Rede Gratuitamente

Ao longo deste e-book, exploramos os seis maiores problemas que as pequenas e médias empresas (PMEs) enfrentam em suas redes e apresentamos soluções práticas para cada um deles. Desde a falta de segurança e a baixa performance até a dificuldade em escalar a infraestrutura, é evidente que uma rede eficiente e bem gerida é crucial para o crescimento e a sustentabilidade das operações de uma PME. No entanto, a implementação dessas soluções requer uma análise profunda e um entendimento claro das necessidades específicas de cada empresa.

Se a sua empresa está lutando com questões de conectividade, segurança ou gestão de ativos, nós da Hackone Consultoria temos uma proposta que pode transformar a sua realidade. Oferecemos uma análise completa da sua rede, que não só identificará as vulnerabilidades e os gargalos existentes, mas também proporcionará um plano de ação claro e objetivo, de uma maneira personalizada, para proteger futuros investimentos e otimizar a sua infraestrutura.



**Hackone
Network Quality**

8/10

Excelente



Network security: **9/10**



Network resilience: **10/10**



Network disaster recovery: **10/10**



Network growth: **9/10**



Network support team: **10/10**



Lucas Palma
CEO Hackone



Nossa equipe de **especialistas e consultores em TI da Hackone** realizará uma avaliação detalhada, examinando cada aspecto da sua rede, desde a configuração de dispositivos até sua performance e segurança. A transformação digital está ao seu alcance, e investir em uma infraestrutura de TI sólida é o primeiro passo para alcançar um crescimento sustentável e se destacar no mercado. Não deixe que problemas de rede continuem atrapalhando o seu negócio.

Acesso o link: <https://hackone.com.br/consultoria>