Manual prático para **autenticação de Wi-Fi corporativo**

Como estruturar:

Políticas de acesso

Segmentar usuários

Acesso seguro e rastreável do zero

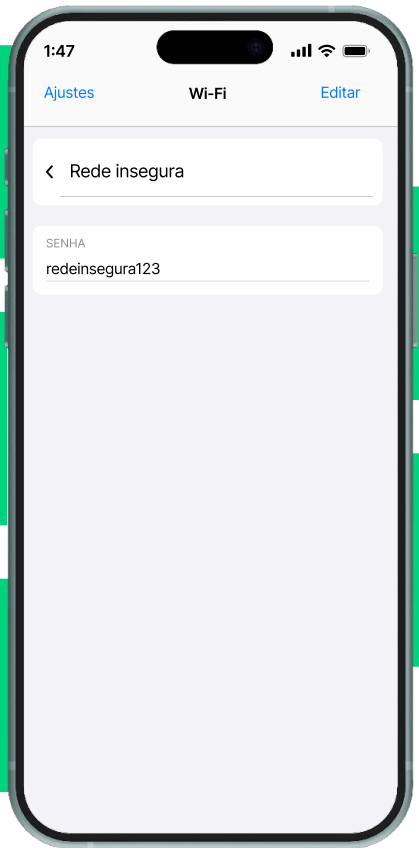
Do desenho estratégico à infraestrutura ideal: *passo a passo para* ***proteger sua rede Wi-Fi empresarial*** e estar em ***conformidade com a LGPD e Marco Civil da Internet***

Wi-Fi sem autenticação é porta aberta

Toda empresa hoje tem Wi-Fi, **mas poucas tratam a rede como infraestrutura crítica.**

O que acontece na prática é:

1. Colaboradores e visitantes usam a mesma senha;
2. A senha circula no WhatsApp;
3. Fornecedores conectam dispositivos pessoais sem controle;



4. Não há registro claro de quem acessou, quando e por quanto tempo;
5. Em caso de incidente, não tem como rastrear.

A rede Wi-Fi vira apenas conveniência quando deveria ser mais uma ferramenta de controle e segurança.

É aqui que entra a **autenticação estruturada.**

O que é autenticação em redes Wi-Fi?

Autenticação é o processo de:

1. Definir políticas de acesso e regras de uso;
2. Identificar quem está tentando acessar a rede;
3. Validar se essa pessoa pode acessar;
4. Registrar o acesso para fins de segurança e compliance.

Pense assim: se a sua rede fosse um prédio corporativo, o **WiFeed seria o segurança que controla quem entra.**

Ele **verifica identidade, libera o acesso correto e registra tudo.**

Sem autenticação estruturada, a empresa depende apenas de senha compartilhada, que não é nada seguro e pode se transformar em prejuízo milionário em caso de invasões digitais.

Por que isso é estratégico (e não apenas técnico)?

Porque o Wi-Fi está conectado a:

- Sistemas internos;
- Dados sensíveis;
- Servidores;
- Equipamentos IoT;

Sem autenticação, qualquer dispositivo entra na rede. Sem segmentação, qualquer dispositivo que entrou pode acessar tudo.

- Vazamento de dados;
- Movimento lateral dentro da rede;
- Acesso indevido à rede de colaboradores;
- Problemas jurídicos por falta de logs;
- Falta de rastreabilidade (Marco Civil + LGPD).

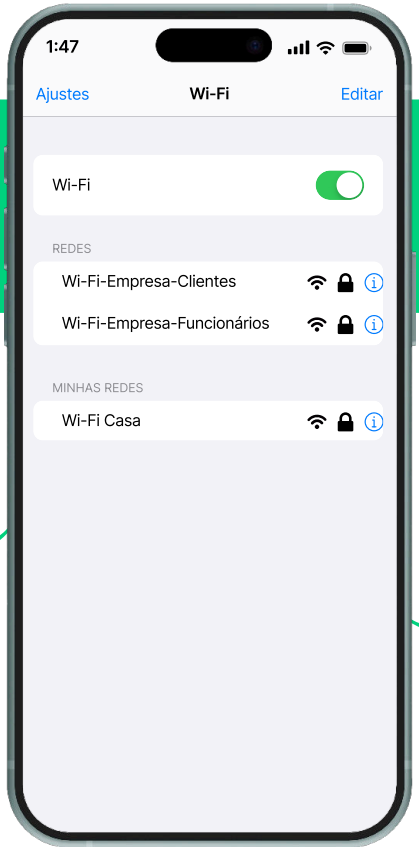
E o mais comum: **TI sobrecarregada** *resolvendo problemas simples que poderiam estar automatizados.*

Como as empresas normalmente fazem (e onde erram)

Modelo mais comum:

Uma rede interna;

Uma rede “visitante”;



Mesma senha para todos;

Nenhuma política de acesso.

Isso não é só desorganização, é um risco estrutural. *O problema não é ter uma rede simples, é não ter uma política.*

O passo a passo estratégico para estruturar políticas de acesso

Agora entramos na parte prática. Antes de falar de infraestrutura, ***você precisa decidir estrategicamente:***

1 Mapear perfis de usuários

Pergunta básica: **quem realmente usa sua rede?**

Exemplo:

- Diretoria;
- Colaboradores administrativos;
- Operação;
- Fornecedores;
- Visitantes;
- Dispositivos IoT;

Em uma escola:

- Alunos;
- Professores;
- Coordenação;
- Visitantes.

Em hospital:

- Médicos;
- Enfermagem;
- Administrativo;
- Pacientes.

Sem clareza de perfil, não existe política.

O passo a passo estratégico para estruturar políticas de acesso

2 Definir regras por perfil de usuário

Aqui você começa a **estruturar as políticas de acesso** e **regras de uso por perfil de usuário.**

	SSID	Método de autenticação	N° de devices	Horário de funcionamento	Tempo de conexão
Diretoria	.Empresa Wi-Fi	Active Directory	Ilimitado	24h	Ilimitado
Colaboradores	.Empresa Wi-Fi	Active Directory	Ilimitado	Almoço e break	Ilimitado
Parceiros	.Guest Wi-Fi	Aprovação de acesso	2	08h às 18h	8h
Guest	.Guest Wi-Fi	Formulário	1	08h às 18h	2h

Para cada perfil, definir:

A SSID

- Vai ser rede exclusiva?
- Ou múltiplos SSIDs mapeados para VLANs diferentes?

B Método de autenticação

- Active Directory
- Google Workspace
- Voucher
- Formulário
- Aprovação de Acesso
- gov.br
- MAC
- Login e senha
- e vários outros.

C Número de dispositivos permitidos

- 1?
- 2?
- Ilimitado

O passo a passo estratégico para estruturar políticas de acesso

D Controle por MAC Address (apenas dispositivos cadastrados)

- Apenas dispositivos previamente cadastrados podem conectar
- Útil para rede interna e BYOD.

E Horário de uso

- 24h?
- Apenas horário comercial?
- Apenas período letivo?

F Tempo de conexão

- 2h?
- 4h
- 8h?
- Quando necessário

G Nível de acesso (Definido no firewall ou gateway da infraestrutura)

- Acesso à rede interna?
- Apenas internet?
- Acesso a sistemas específicos?

3 Definir isolamento e segmentação
(Definido no firewall ou gateway da infraestrutura)

Aqui entra um conceito fundamental: **cada perfil deve estar em uma VLAN separada.**

Exemplo:

- VLAN 10 → Diretoria;
- VLAN 20 → Colaboradores;
- VLAN 30 → Visitantes;
- VLAN 40 → IoT.

Isso evita:

- Comunicação indevida entre redes;
- Acesso lateral;
- Risco interno ampliado.

Segmentação é o que **transforma Wi-Fi em infraestrutura segura.**

4 Garantir rastreabilidade e conformidade

Toda política precisa prever:

- Registro de logs;
- Registro de IP atribuído;
- Data e horário de acesso;
- Termo de uso aceito;
- Consentimento LGPD.

Sem isso, você não tem segurança jurídica.

E aqui o **WiFeed atua como camada de autenticação e registro, integrando com gateways, controladoras e APs homologados.**

O que você precisa na infraestrutura para isso funcionar

Até aqui, você já desenhou a parte mais importante: **a política de acesso.**

Agora vem a etapa que transforma esse desenho em realidade: **a infraestrutura de rede.**

Para que o WiFeed consiga aplicar autenticação, segmentação por perfil, regras de uso e registro de acessos, ***sua rede precisa atender a alguns requisitos básicos.***

1 O papel do gateway (firewall ou access point)

Em todos os cenários recomendados pelo WiFeed, existe um elemento central: **o gateway da rede.**

É ele quem:

- **Recebe o link da internet;**
- **Faz a separação de redes (VLANs);**
- **Aplica regras de roteamento e firewall;**
- **Integra com o WiFeed para autenticação e captive portal.**

Dependendo do ambiente, esse papel pode ser exercido por:

- **Fortigate (Firewall)**
- **Fortigate (FortiAP)**
- **AP com controladora**
- **MikroTik**

O que você precisa na infraestrutura para isso funcionar

2 O papel dos Access Points (APs)

Os APs não “decidem” quem entra ou não na rede. **Eles executam a política que você desenhou no core da rede com o WiFeed.**

Nos cenários recomendados:

- Os APs operam em modo bridge;
- Cada SSID está associado a uma VLAN específica;
- O AP apenas “transporta” o tráfego até o gateway ou controladora.

Na prática, isso significa:

- O AP não mistura redes;
- O perfil do usuário já nasce segmentado;
- A segurança não depende do Wi-Fi em si, mas da arquitetura da rede.

Controladoras homologadas:

FORTINET · CISCO · aruba · Ruckus WIRELESS · HUAWEI · AEROHIVE NETWORKS · UBIQUITI NETWORKS · tp-link · Extreme networks · Entre outras.

A regra é simples: **se o equipamento é homologado, ele funciona corretamente com o WiFeed.**

O que você precisa na infraestrutura para isso funcionar

3 Requisitos técnicos mínimos do ambiente

Independentemente do cenário escolhido, **alguns pontos são obrigatórios:**

- Suporte a VLANs por SSID;
- Gateway ou firewall com acesso à internet;
- Comunicação estável entre gateway/ controladora e APs;
- DHCP funcional para as redes de usuários;
- Link estável para que o fluxo de autenticação funcione.

Esses requisitos garantem:

- Isolamento entre redes internas e visitantes;
- Políticas de acesso;
- Funcionamento do captive portal e da autenticação;
- Registro de logs e rastreabilidade dos acessos.

Conectando com cenários recomendados

Esses cenários existem porque cobrem a grande maioria das realidades encontradas em empresas, do ambiente mais robusto ao mais simples.

1 Fortigate como firewall (Gateway da rede)

Esse é um dos **modelos mais comuns em médias e grandes empresas.**

Como funciona:

- O **Fortigate** atua como gateway principal da rede;
- O **WiFeed é configurado em uma interface (VLAN)** do Fortigate;
- Cada SSID corresponde a uma VLAN;
- Os APs operam em **modo bridge**, apenas repassando o tráfego.

Configurações do captive realizadas diretamente na interface (VLAN)

Link chegando no Gateway;

→

FortiGate entregando rede de gerência para o AP e uma VLAN para cada SSID.

Sendo uma VLAN com a autenticação do WiFeed e as demais conforme a necessidade da empresa;

→

AP recebe rede de gerência + VLAN para o SSID.

Cada SSID irá pegar o DHCP da VLAN tagueada.

2 Fortigate com FortiAP (gateway + controladora)

Aqui, o **Fortigate faz dois papéis ao mesmo tempo:** Gateway da rede e Controladora dos access points (FortiAP).

Como funciona:

O WiFeed é configurado no SSID dentro da interface Wireless do Fortigate;

Os APs recebem automaticamente as configurações;

Toda a gestão de Wi-Fi fica centralizada no Fortigate.

Configurações do captive realizadas diretamente na interface wireless (SSID)

Link chegando no Gateway;

FortiGate atuando como gateway e controladora dos APs. A autenticação do WiFeed é configurada no SSID desejado;

AP recebe todas as configurações do Fortigate e direciona o usuário para o captive.

3 AP com controladora dedicada

Esse é o **cenário típico de ambientes com: Cisco, Aruba, Ruckus, TP-Link Omada, Ubiquiti, etc.**

Como funciona:

O **WiFeed é configurado diretamente na controladora;**

O gateway entrega rede e VLANs para os APs;

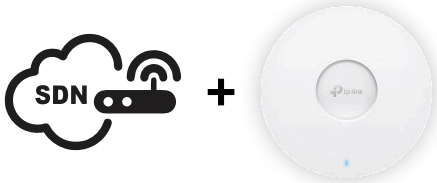
Os APs recebem as configurações pela controladora via internet ou rede interna;

Cada SSID usa sua VLAN específica.

Configurações do captive realizadas diretamente na controladora

Link chegando no Gateway;

Gateway entregando rede de gerência para o AP e uma VLAN para cada SSID;



AP recebe rede de gerência + VLAN para o SSID.

O AP se comunica via internet com a controladora, recebe as configurações e direciona o usuário para o captive.

Para o correto funcionamento:

O AP deve receber IP via DHCP e ter acesso à internet;

Criar uma **rede de gerência exclusiva para os APs;**

Usar VLANs separadas por SSID, isolando: rede interna, rede de visitantes e rede de autenticação.

4 MikroTik como gateway

Esse é o **cenário mais simples e prático.**

Como funciona:

O **MikroTik atua como gateway da rede;**

O **WiFeed é configurado em uma interface (VLAN)** no MikroTik;

Os APs operam em **modo bridge;**

Cada SSID está associado a uma VLAN.

Configurações do captive realizadas diretamente na interface (vlan)

Link chegando no MikroTik;

MikroTik entregando rede de gerência para o AP e uma VLAN para cada SSID.

Sendo uma VLAN com a autenticação do WiFeed configurada via script e as demais conforme a necessidade da empresa;

AP recebe rede de gerência + VLAN para o SSID.

Cada SSID irá pegar o DHCP da VLAN tagueada.

Qual cenário escolher?

A decisão depende de três fatores:

1. **O que você já tem hoje na rede;**
2. **O nível de controle e escala que precisa;**
3. **A maturidade da sua operação de TI**

A boa notícia: **o WiFeed se adapta à sua realidade**, desde que a *arquitetura respeite os princípios de segmentação, VLAN e controle de acesso.*

Além disso, **todos os cenários convergem para o mesmo resultado**: uma *rede Wi-Fi corporativa gerenciada pelos princípios de Zero Trust, com identidade verificada, acesso segmentado e rastreabilidade garantida.*

O papel do WiFeed nesse cenário

O WiFeed não substitui seu firewall, seus switches ou seus access points.

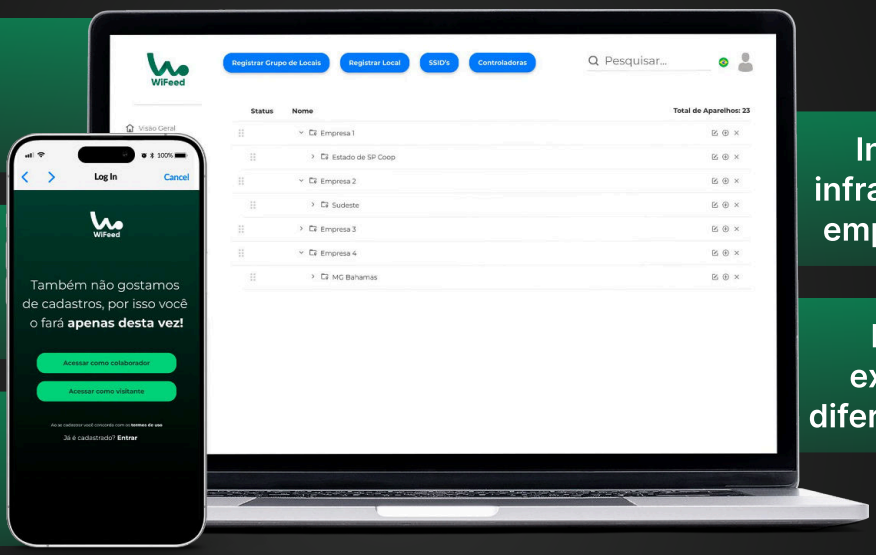
Ele faz algo diferente e essencial: organiza, centraliza e governa o acesso à sua rede Wi-Fi.

Na prática, isso significa:

Centralizar métodos de autenticação;

Garantir rastreabilidade de acessos;

Aplicar políticas de acesso por perfil de usuário;



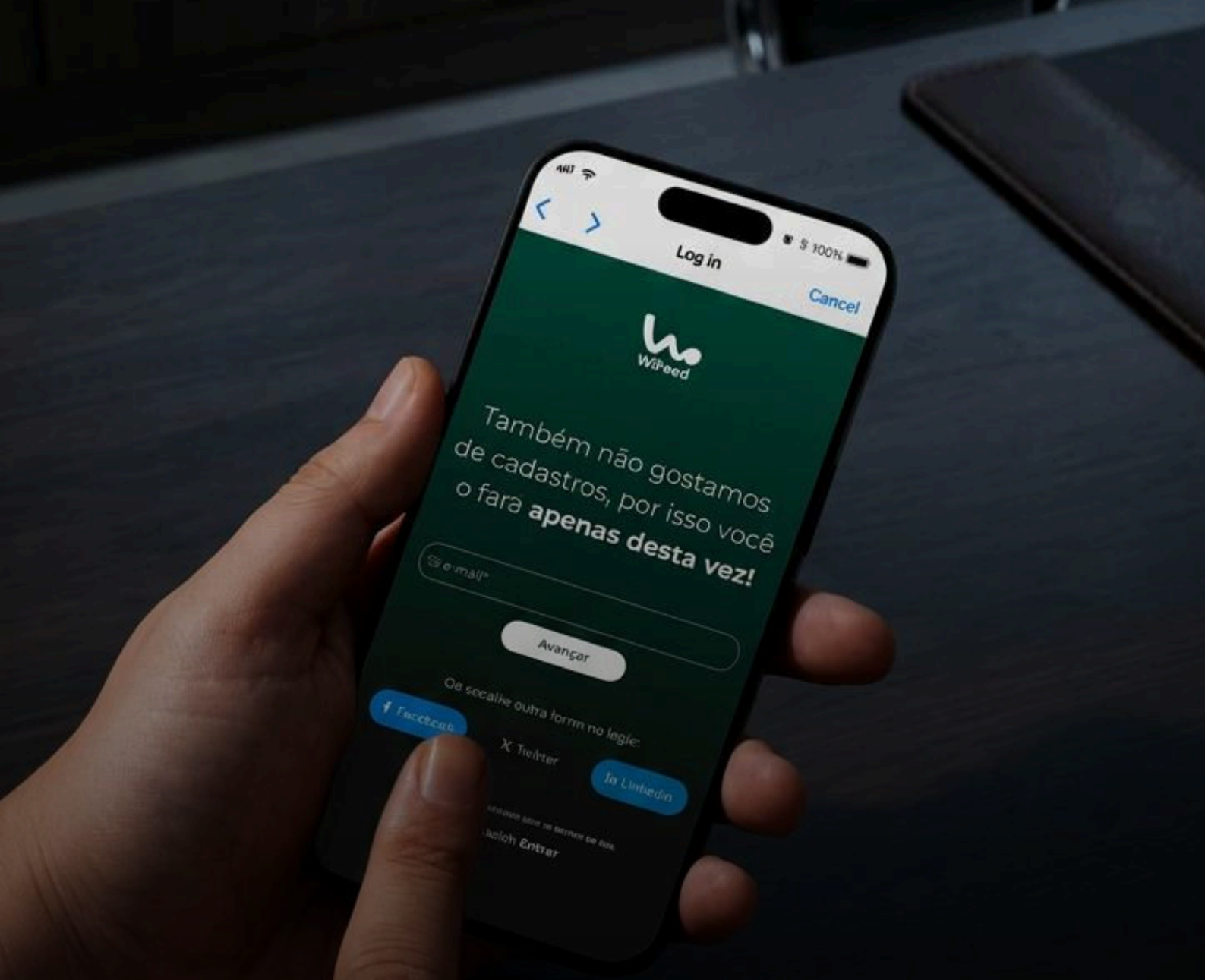
Integrar com a infraestrutura que a empresa já possui;

Padronizar a experiência em diferentes unidades.

O WiFeed atua como a **camada de controle de acesso** entre a conectividade e a segurança.

Clique no botão abaixo e confira na prática como o WiFeed eleva a segurança da sua rede Wi-Fi corporativa.

Assistir uma demonstração



Quando bem estruturado, o Wi-Fi vira:

Controle | **Previsibilidade** | **Segurança** | **Governança**

E é exatamente nesse ponto que a
tecnologia deixa de ser custo operacional
e passa a ser ativo estratégico do negócio.

wifeed.com.br @wifeedbr WiFeed