# Boas Práticas de Segurança

## NexChat e a Segurança da Informação

Como empresa de tecnologia, estamos sempre preocupados em implementar mecanismos de segurança para nossos clientes. Por isso, investimos pesado em segurança da informação, aplicando medidas de segurança recomendadas no mercado. Além disso, contamos com o apoio de consultorias de segurança com o intuito de refinar o software.
Da mesma maneira, nos preocupamos com o treinamento e gestão das pessoas, mantendo contato com técnicas dedicadas a orientar as melhores práticas relacionadas à segurança. Entendemos ser de extrema importância o foco na proteção dos dados e contamos com ferramentas que auxiliam na mitigação e investigação de possíveis falhas.

Ainda nos atentamos à proteção dos dados pessoais e a privacidade, adequando o software para atender os requisitos da Lei Geral de Proteção de Dados (LGPD).

## Trabalhe com segurança!

Algumas dicas que você pode utilizar no seu sistema para aumentar a segurança.

### Configure as redes permitidas

Limitar quem pode acessar seu sistema é fundamental para aumentar sua segurança. Com essa configuração, você restringe o acesso ao sistema apenas para faixas de IPs locais ou faixas conhecidas pelo seu administrador de rede. Isso evita acessos de pessoas não autorizadas, mesmo em posse das credenciais de acesso.

Para saber como configurar as redes permitidas, clique aqui.

### Configure as permissões dos usuários

O Opa! Suite possui um sistema de permissões altamente configurável, permitindo que cada grupo de usuários tenha acessos limitados de acordo com a necessidade do administrador. Utilize isso a seu favor, configurando as permissões ao mínimo necessário (princípio do menor privilégio), seguindo as boas práticas de segurança.

Para saber como configurar as permissões de usuários, clique aqui.

## Configure e verifique seus backups

Uma das configurações mais importantes do sistema é o backup. Ele é gerado internamente no próprio servidor e pode ser enviado para um local protegido externamente, seja na nuvem ou dentro da sua própria estrutura. Crie uma rotina para verificação dos backups com frequência, pois eles podem salvar a sua empresa.

Para saber como configurar o backup do sistema, clique aqui.

## Cuide da senha do seu servidor

A senha root do servidor é um dado muito importante e sigiloso. Ao alterar a senha do seu servidor, utilize uma senha segura, com vários caracteres. Consulte a nossa equipe técnica ao fazer alterações no servidor.

## Não instale aplicações de terceiros em seu servidor

Não recomendamos que sejam instalados aplicativos de terceiros no mesmo servidor onde seu Opa! Suite está instalado. Aplicativos de terceiros podem comprometer a segurança dos dados, abrindo portas ou vulnerabilidades em seu servidor.

Na dúvida, consulte nossa equipe técnica.

## Mantenha seu servidor seguro

A proteção física do seu servidor também é muito importante. Restringir o acesso, manter longe de instalações hidráulicas, com climatização e fonte de energia redundante, são boas formas de cuidar da sua estrutura. Isso pode evitar problemas de indisponibilidade do seu sistema.

## Cuide dos acessos do seu sistema

Uma boa gestão de acessos é essencial para que seu sistema permaneça seguro.

Podemos considerar segura, uma senha que tenha no mínimo 8 dígitos contendo: letras maiúsculas, letras minúsculas, números e caracteres especiais.

Sair apertando todas as teclas segurando a tecla Shift alternadamente pode te ajudar a criar uma senha bem complexa.

Confira o material que produzimos para mais detalhes sobre como fazer a gestão das suas senhas.

## Manuseio de credenciais de acesso

Abaixo temos algumas dicas que vão te ajudar no momento de criar uma senha forte e mostrar como armazená-la de forma segura.

- Não utilize meio físicos, como sua agenda, para anotar suas senhas, até porquê, qualquer pessoa que pegá-la terá acesso a tudo que está escrito.

> Jamais escreva sua senha em um post-it e cole no seu monitor!

- Faça o máximo de esforço para utilizar uma credencial exclusiva para cada sistema. Assim, se alguém por acaso descobrir sua senha, não terá acesso em todas as suas contas!
- Atualize as suas senhas de tempos em tempos;
- Utilize a autenticação em dois fatores sempre que estiver disponível. Com ela, conseguiremos garantir que, mesmo se alguém tiver a nossa senha, não vai conseguir acessar nossa conta pois será necessário inserir um código único gerado por um aplicativo (como o Google Authenticator) ou enviado para o nosso e-mail;

## Adicione camadas de segurança em sua rede

Proteger sua rede é essencial para a segurança da sua empresa. Muitas tentativas de ataques cibernéticos são feitas diariamente em equipamentos mal configurados ou sem proteção. A utilização de firewall de entrada e saída, por exemplo, aumenta a segurança de seus ativos de rede.

## Informe atividades suspeitas

> Ao sofrer algum incidente ou se deparar com uma situação atípica, informe imediatamente ao responsável e ao gestor de segurança da sua empresa. Você também pode entrar em contato com nosso suporte através da plataforma de atendimento.

> Para melhorar a experiência e visualização, esta Wiki também está disponível em PDF!