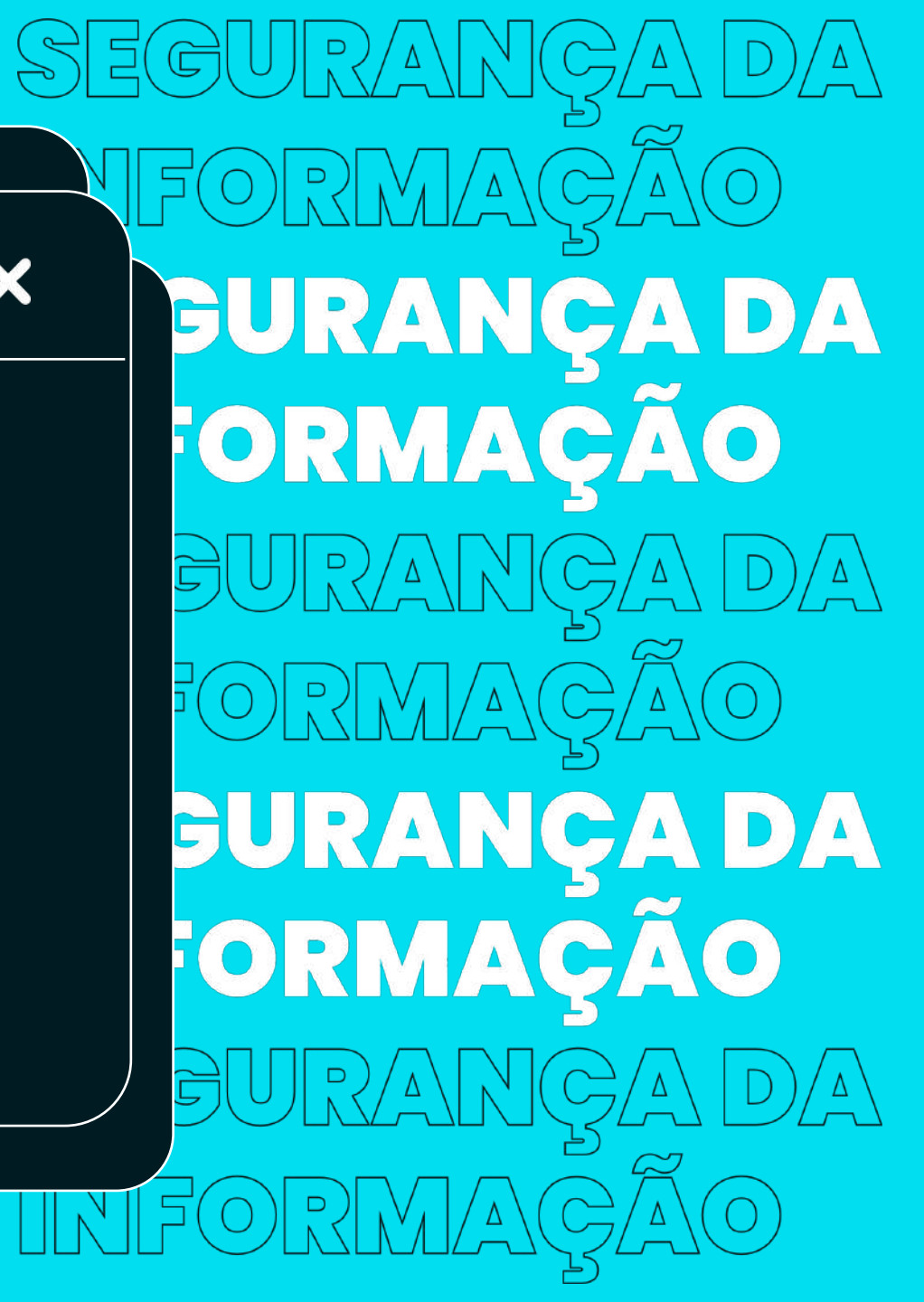
Guia técnico

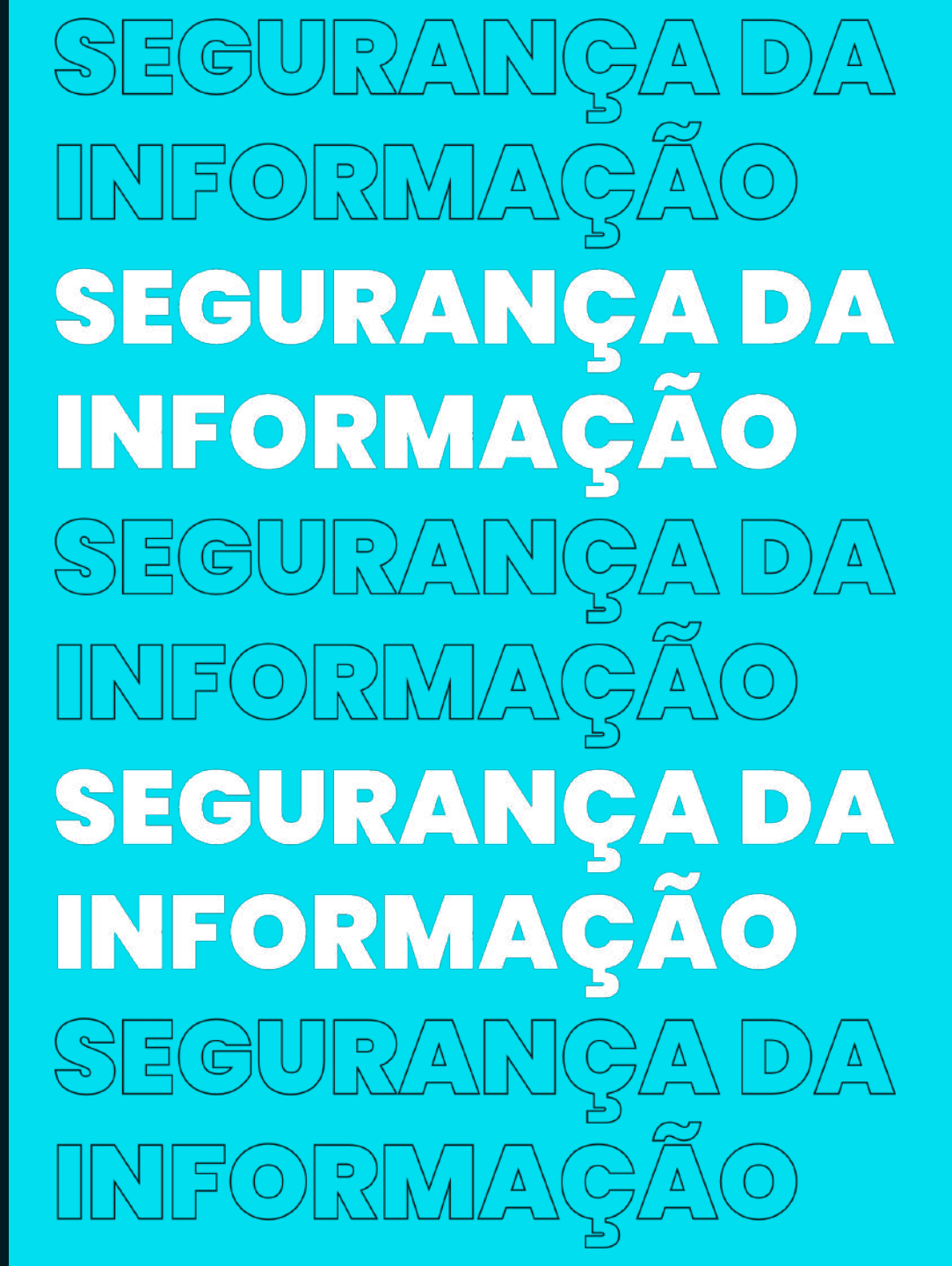
Segurança da Informação do **Sistema de Gestão OMIE - ERP**



Introdução

Este guia apresenta as medidas de segurança adotadas no Sistema de Gestão OMIE – ERP e esclarece os papéis e responsabilidades na proteção dos dados no modelo de responsabilidade compartilhada entre a OMIE e seus Clientes.

Vamos, juntos, manter nossas informações seguras e livres de ameaças!



Arquitetura Geral da Solução

O sistema de gestão (ERP) é comercializado na modalidade SaaS (Software as a Service), onde o cliente acessa o sistema por meio da internet, sem a necessidade de instalação local.

Toda a responsabilidade pela operação, atualização, segurança da aplicação e da infraestrutura é da OMIE e o Cliente é responsável pelo uso adequado, pelas configurações de segurança e controle de acessos.

A nossa solução é hospedada na nuvem pública da AWS, na região do Brasil distribuída em duas zonas, com arquitetura que isola os ambientes de desenvolvimento, homologação e produção. Os dados dos clientes são separados logicamente no ambiente de produção e não são utilizados nos demais ambientes.

O sistema disponibiliza APIs públicas que permitem integrações com aplicações externas e automações por parte do Cliente.

Responsabilidades OMIE

Medidas Técnicas de Segurança

A proteção da aplicação e do ambiente de processamento e armazenamento dos dados são responsabilidades da OMIE. Para isso, adotamos medidas técnicas e administrativas, a fim de garantir que nosso sistema esteja livre de ameaças e ataques cibernéticos.

A seguir, enumeramos algumas medidas de segurança adotadas por nós, sendo que não se deve limitar somente a elas.

Proteção dos **dados**

Criptografia em repouso

Os dados confidenciais são armazenados utilizando criptografia **AES-256** (Advanced Encryption Standard – padrão de criptografia avançado), que é um algoritmo aprovado para proteger dados eletrônicos. O tamanho da chave é de 256 bits para criptografar e descriptografar.

Criptografia em trânsito

Todos os trafegados entre o cliente e o sistema de gestão são protegidos por criptografia utilizando protocolo **TLS 1.3** (Transport Layer Security), a versão mais segura e moderna.

Segurança da **aplicação**

Nosso sistema de gestão foi desenvolvido de acordo com as melhores práticas de desenvolvimento seguro, de maneira a ser protegido das ameaças listadas no framework da ***OWASP*** (Open WorldWide Application Security Project, projeto aberto de segurança em aplicações web).

Nosso sistema é submetido semestralmente a um Pentest (teste de penetração), realizado por uma empresa especializada.

Além disso, adotamos um Ciclo de Desenvolvido Seguro(Secure SDLC)onde são realizados testes estáticos e dinâmicos (SAST e DAST) para identificação e correção de vulnerabilidades desde as fases iniciais até a execução.

Proteção da **aplicação**

Utilizamos WAF (Web Application Firewall – firewall de aplicativos web) para proteger nosso sistema contra ataques cibernéticos descritos no framework da OWASP.

Por meio do WAF, também mantemos o ambiente protegido contra ataques de negação de serviço – DDoS (Distributed Denial-of-Service).

Proteção das **APIs**

Para o uso de nossas APIs (Application Programming Interface), é necessário um par de chaves para cada cliente.

Nossas APIs também estão protegidas com a utilização de WAF.

Somado a isso, o Cliente deve manter as chaves em local seguro, com acesso restrito.

SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

Proteção da **infraestrutura**

Usamos diversas tecnologias para proteger o ambiente que suporta o nosso sistema (Omie ERP).

Os ativos desse ambiente são atualizados diariamente, a fim de manter a versão mais atualizada em atividade nesse processo.

Este ambiente é monitorado em tempo real por um serviço que atribui um Score a essa proteção, em que A é o nível mais seguro.

Acesso à infraestrutura

A sustentação e a administração da nossa infraestrutura de nuvem ocorrem de forma **100% remota e independente da rede corporativa**. O acesso à infraestrutura do Sistema de Gestão (ERP) por parte da nossa equipe interna é restrito, protegido obrigatoriamente com autenticação forte MFA (Multi-Factor Authentication, ou múltiplo fator de autenticação), e uso de conexões seguras via VPN (Virtual Private Network).

A política de senha segue o padrão de complexidade, e todos os acessos são registrados em trilha de auditoria.

Backup

Diariamente são realizadas cópias de segurança das imagens das máquinas que suportam nosso sistema Omie ERP.

Os logs das transações são copiados em tempo real, garantindo um tempo de recuperação com o mínimo de perdas.

A rotina de backup é um processo interno da Omie para garantir a segurança das informações do nosso sistema (Omie ERP) e não está disponível para os Clientes.

Resposta a **incidentes**

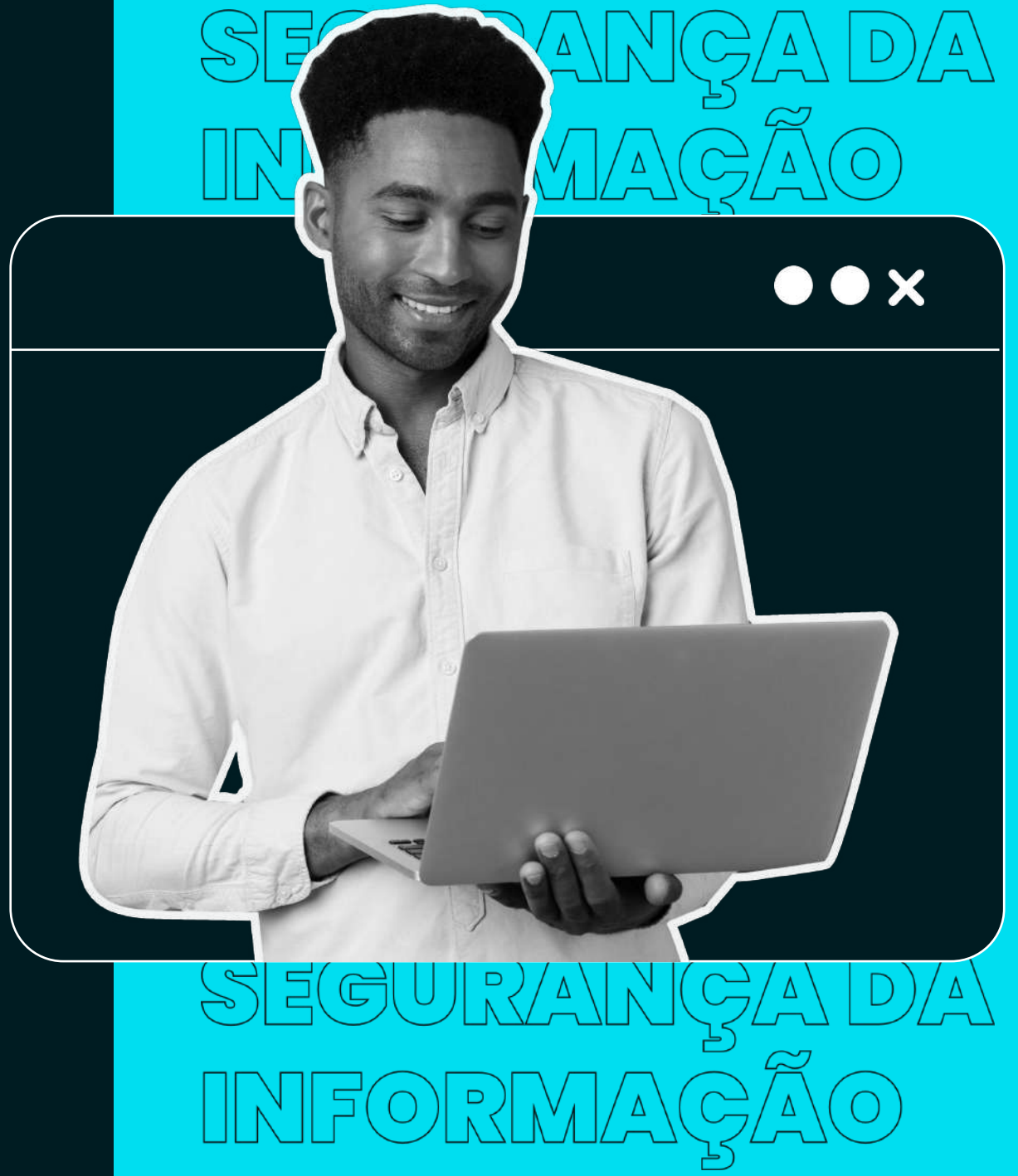
Embora a Omie tome medidas para proteger as informações, não somos responsáveis por atos de acessos não autorizados em nosso ambiente, nem por ataques e invasões criminosas. Para isso, mantemos um “Plano de Resposta”, de modo a rapidamente recuperar dados de um incidente de segurança da informação e privacidade.

Na ocorrência de um incidente que envolva dados dos clientes, eles serão comunicados no prazo adequado e exigido por lei.

Continuidade do negócio

A Omie mantém um “Plano de Continuidade do Negócio”, com o objetivo de manter as principais atividades do sistema (Omie ERP) disponíveis no caso de um incidente disruptivo.

Esse plano visa garantir a disponibilidade de acordo com o SLA (Service Level Agreement, ou acordo de nível de serviço) descrito no termo de uso do nosso sistema (Omie ERP).



Parceiros da **Omie.Store**

Todos os parceiros da Omie.Store são avaliados e monitorados durante toda a nossa parceria.

A Omie mantém uma Política de Segurança da Informação direcionada a estes parceiros.

Clique aqui para acessar nossa página de Segurança e Privacidade e conferir a política vigente.

Compartilhamento de **dados**

Para emissão das notas fiscais, é necessário o compartilhamento de dados com as prefeituras das cidades ou com a SEFAZ (Secretaria da Fazenda) de cada Unidade da Federação.

O compartilhamento é realizado de maneira segura, com criptografia.

Privacidade dos **dados**

Os dados pessoais são tratados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Aos usuários do nosso Sistema de Gestão (Omie ERP), oferecemos um e-book que esclarece a relação Omie (operador) ***X*** Cliente (controlador).

Também é possível acessar nossa Política de Privacidade.

Responsabilidades CLIENTE

Configurações de **acesso** e **restrição** de **segurança** do **Sistema OMIE ERP**

Para garantir a confidencialidade e a integridade dos dados e informações inseridos no sistema, é essencial que o Cliente, por meio do usuário ADMINISTRADOR, configure o Sistema OMIE ERP adequadamente.

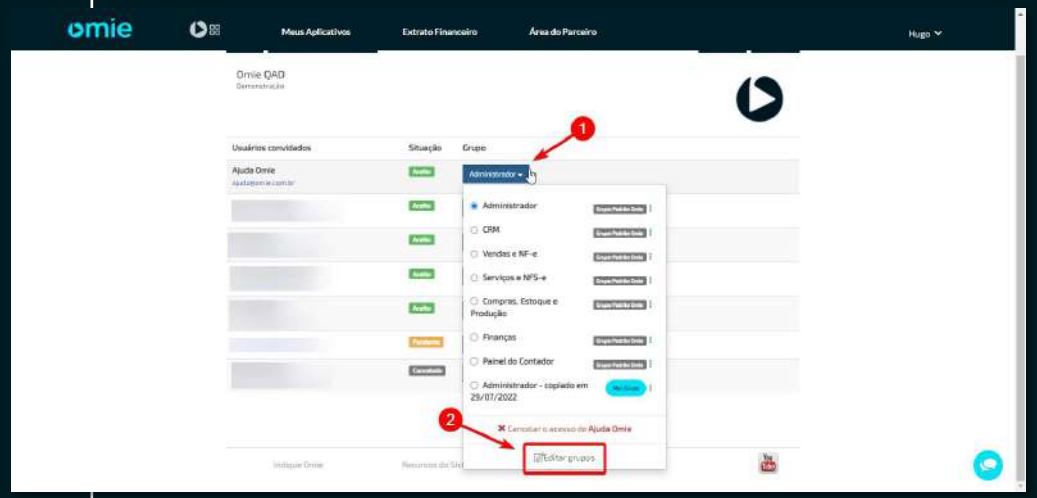
1. O primeiro passo é criar os usuários de acordo com as tarefas a serem executadas no sistema, considerando os princípios de "***mínimo privilégio***" (o acesso do usuário deve ser concedido em termos estritamente necessários para realizar suas funções) e "***segregação de função***" (as atividades conflitantes devem ser separadas entre diferentes usuários).
2. O segundo passo é realizar as configurações de segurança, ou seja, habilitar a autenticação de dois fatores e restringir acessos por IP e/ou por horário.
3. E o terceiro passo é monitorar as atividades realizadas pelos usuários por intermédio das opções de rastreabilidade do sistema.

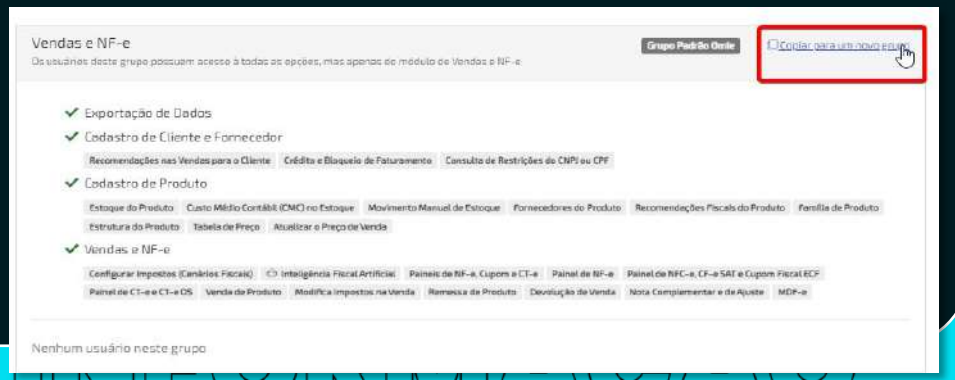
Criação de usuários **OMIE ERP**

Ao contratar nosso sistema, o Cliente (usuário) recebe um login administrador. Por meio dele, será possível criar novos usuários, bem como definir permissões de acesso.

O sistema tem grupos pré-definidos, mas o **Administrador** pode criar novos.

Clique aqui para conferir mais informações sobre criação de usuários e permissões de acesso.

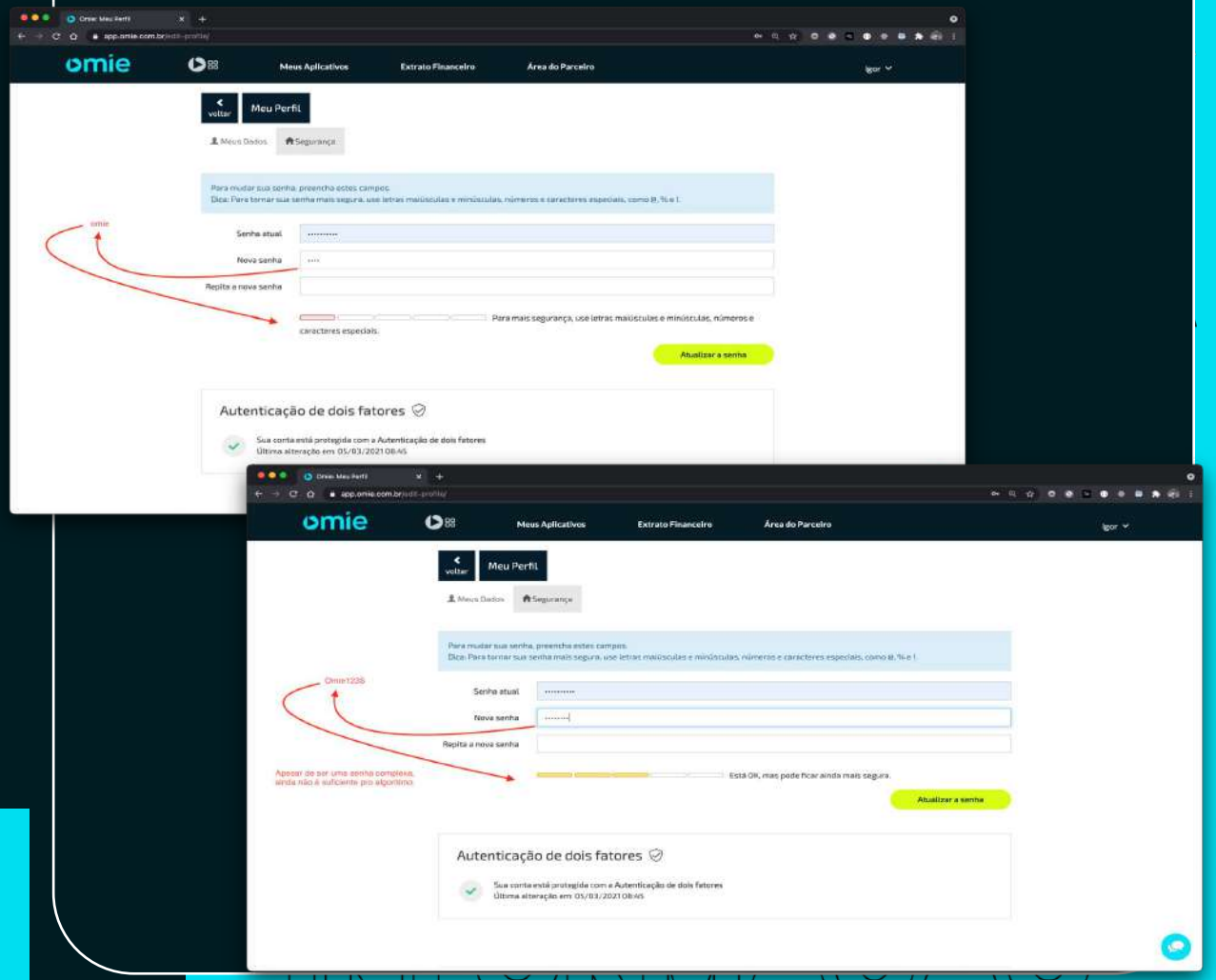




Nossa política de senha

Com o objetivo de garantir a **confidencialidade**, o Sistema OMIE ERP conta com uma política de senha que exige complexidade, ou seja, exige o uso de caracteres especiais, letras e números, bem como com um dicionários de palavras comuns, que não devem ser utilizadas para criar senhas.

Todas as senhas são armazenadas de modo criptografado.



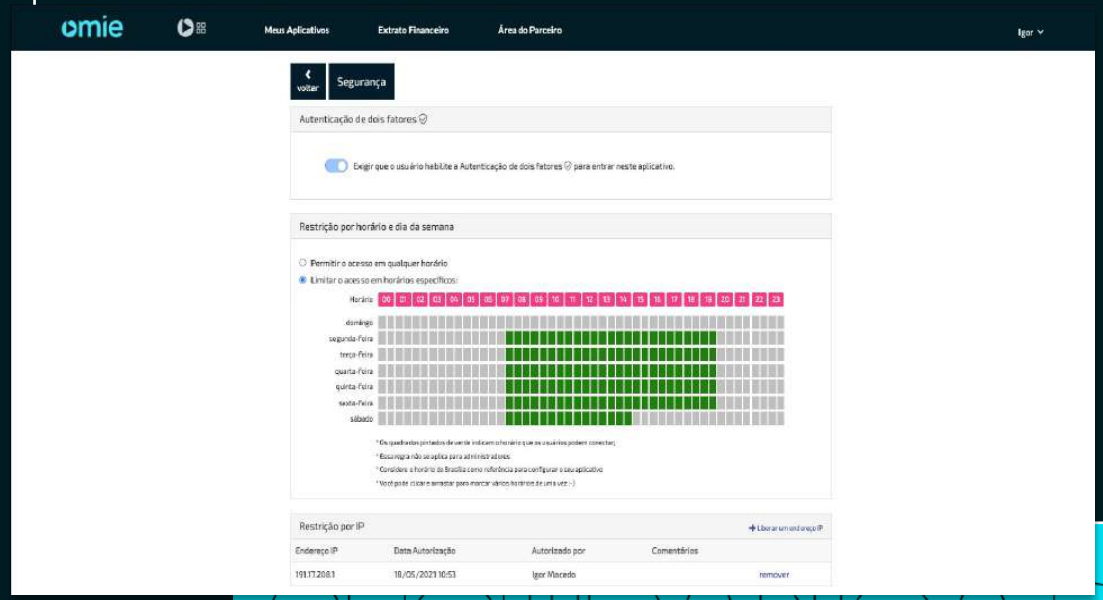
ATENÇÃO! Apesar de complexidade da senha, recomendamos fortemente a habilitação da autenticação de dois fatores!

Habilitação da autenticação de dois fatores

A autenticação de dois fatores é uma camada adicional de segurança para garantir a você o acesso único à sua própria conta, consistindo na identificação dos usuários pela combinação de dois componentes, que pode ser ou algo que somente o usuário sabe (senha) ou algo que apenas o usuário tem (token).

O sistema OMIE ERP garante o uso da autenticação de dois fatores, mas é necessário – e fortemente recomendado – habilitar essa funcionalidade.

O segundo fator de autenticação do sistema é um token exibido no aplicativo. Clique aqui para saber mais sobre a autenticação de dois fatores do sistema OMIE ERP.

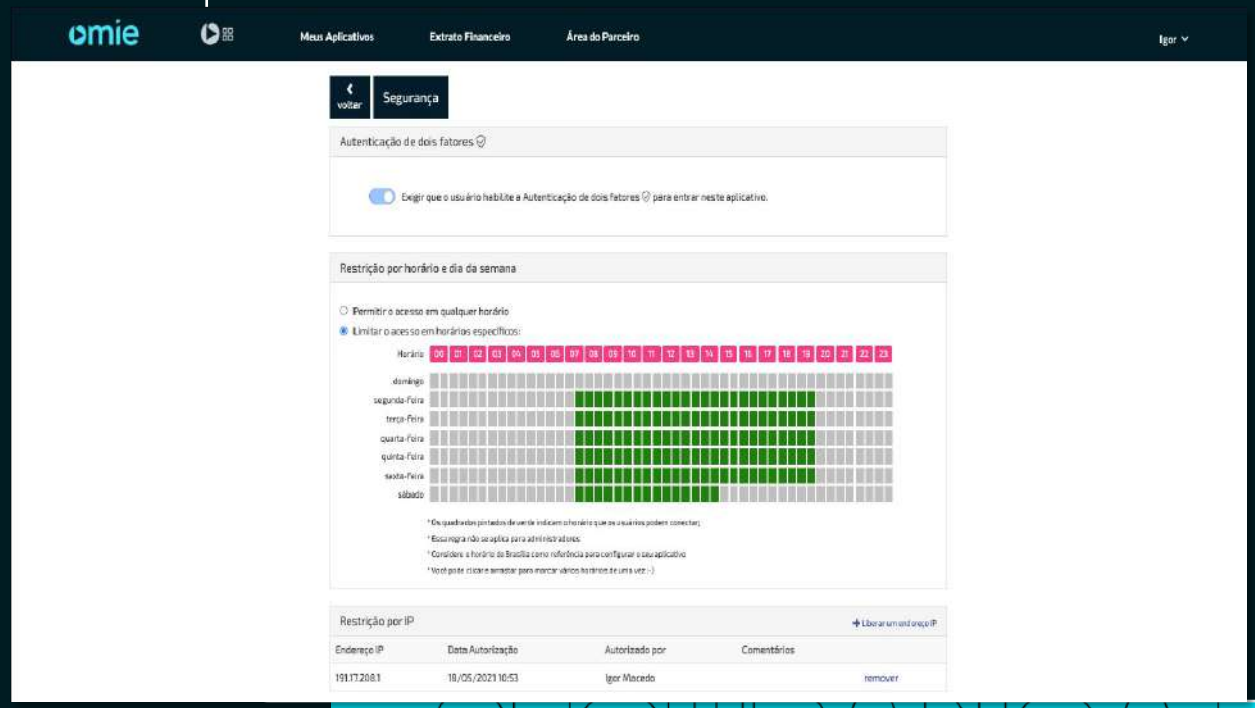


Restrição por **horário**, dia da **semana** e **IP**

Com o objetivo de melhorar o controle dos acessos ao sistema, é possível restringir acessos por horário e dia da semana, de acordo com as necessidades do seu negócio.

Além disso, é possível restringir o acesso pelo endereço IP, evitando acessos de locais “desconhecidos”.

Clique aqui para mais informações.



SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

Rastreabilidade

A rastreabilidade é um dos mais importantes itens para garantir a segurança das informações, pois é como você pode avaliar todos os passos de uma informação (quem acessou, quem alterou, horário e local etc.).

Verifique quais usuários estão conectados (online)

Usuários online (3) — Encerrar todas sessões online

Nome do Usuário	E-mail do Usuário	Endereço IP	Entrada		Duração
Igor Macedo	igor@omie.com.br	187.11.48.129	10/07/17 10:43	online	14 minutos
Igor Macedo	igor@omie.com.br	187.11.48.129	10/07/17 10:42	online	15 minutos
Rodrigo Angeline	rangeline@omie.com.br	187.11.48.129	10/07/17 10:30	online	27 minutos

Verifique os acessos realizados pelos usuários

Últimos 50 acessos

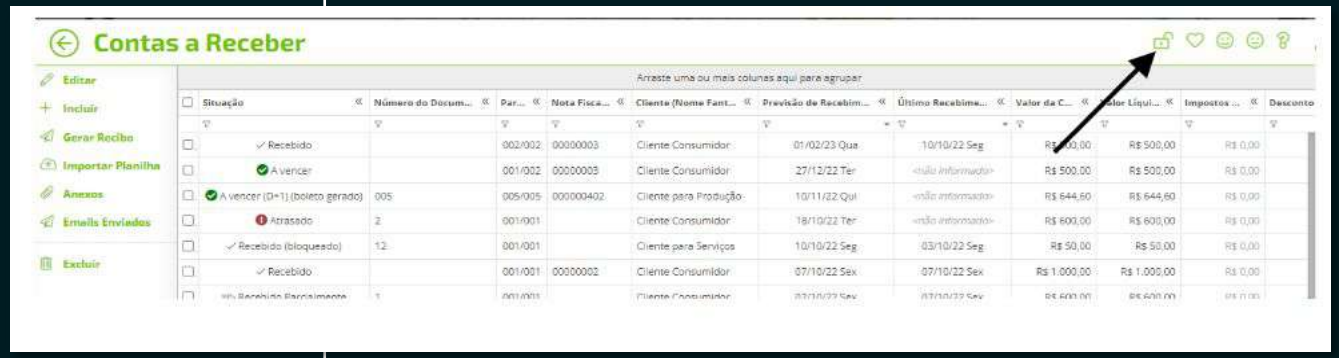
Nome do Usuário	E-mail do Us			
Rodrigo Angeline	rangeline@o			
Rafael Olmos	rafael@omie			
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:51	Bloqueado pela restrição de acesso por IP
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:50	Bloqueado pela restrição de acesso por IP
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:50	Bloqueado pela restrição de acesso por IP
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:50	Bloqueado pela restrição de acesso por IP
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:50	Bloqueado pela restrição de acesso por IP
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:50	Bloqueado pela restrição de acesso por IP
Rafael Olmos	rafael@omie.com.br	187.11.48.129	10/07/17 10:49	Bloqueado pela restrição de acesso por IP
Rodrigo Angeline	rangeline@omie.com.br	187.11.48.129	10/07/17 10:30	Conectado por 31 minutos
Igor Macedo	igor@omie.com.br	187.11.48.129	10/07/17 10:30	Conectado por 13 minutos
Rodrigo Angeline	rangeline@omie.com.br	187.11.48.129	07/07/17 08:35	Conectado por 3 horas

Rastreabilidade

Verifique quem tem acesso a uma determinada tela dos sistema.
Veja aqui mais informações.

Consulte o histórico de alterações realizadas.

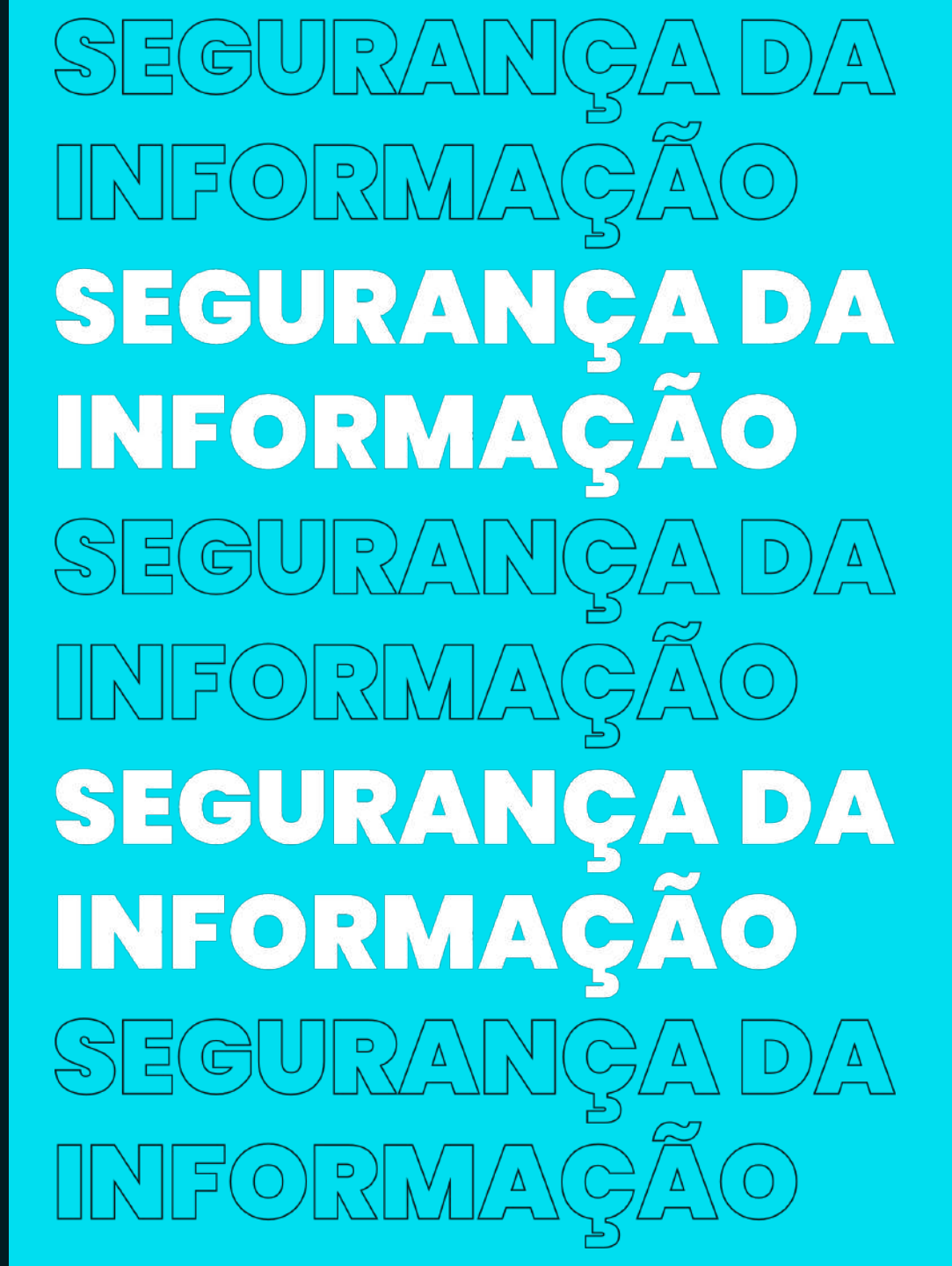
Veja aqui mais informações sobre consulta de histórico.



Além das consultas manuais de histórico, a Omie disponibiliza gratuitamente o **Consultor de Segurança** no próprio ERP. Esta ferramenta monitora continuamente o seu ambiente e gera um Score de Segurança, alertando o Administrador sobre usuários sem MFA habilitado e outras configurações críticas, permitindo que você atue preventivamente no monitoramento de acessos

Recomendações finais

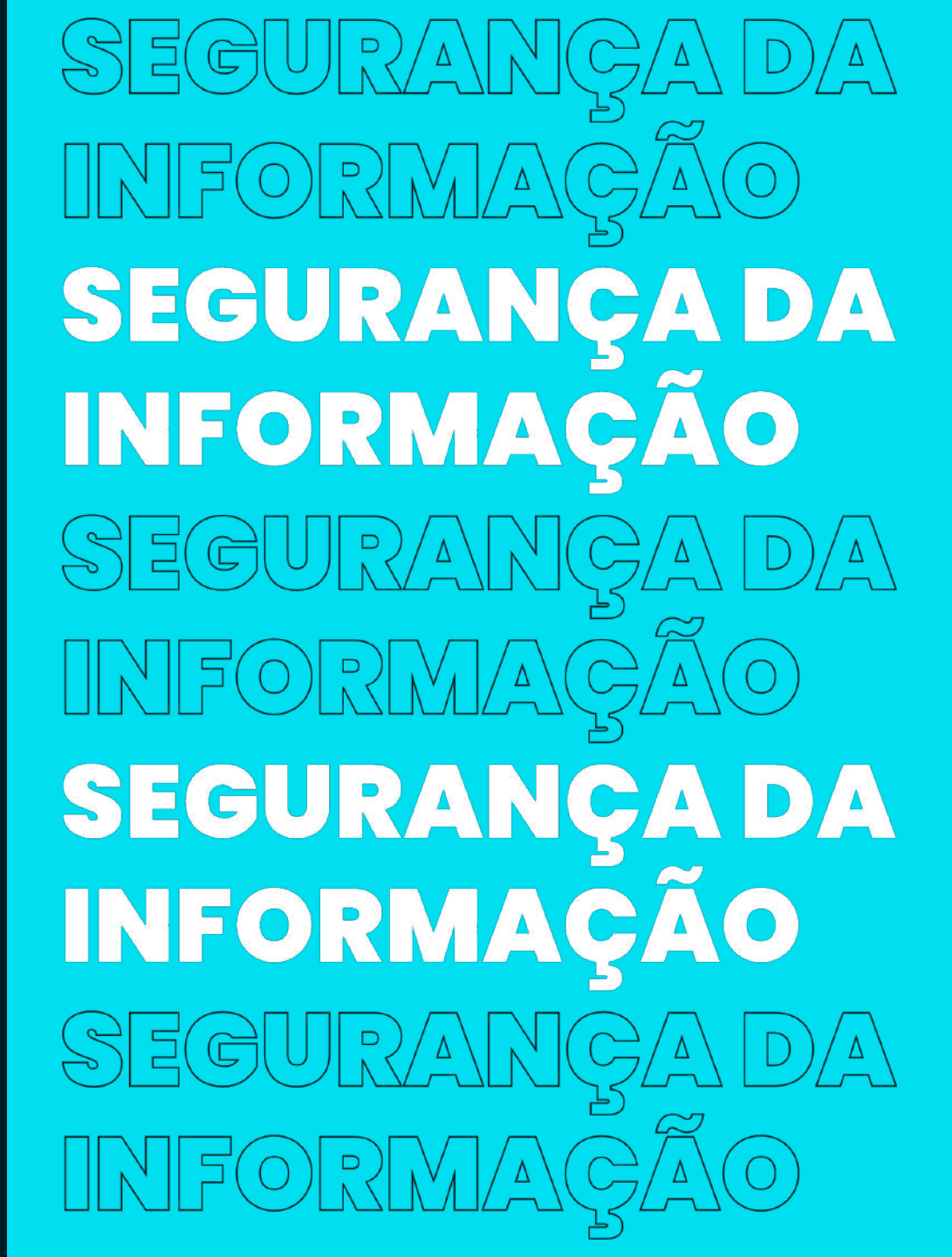
- Nunca acesse o Sistema OMIE ERP utilizando redes Wi-Fi públicas ou redes que possam comprometer a **confidencialidade**, a **integridade** e a **disponibilidade** de suas informações.
- Evite o compartilhamento de senha e usuários genéricos. Crie um usuário nominal para cada pessoa que for acessar o sistema.
- Habilite a autenticação de dois fatores.
- Altere a senha quando ocorrer qualquer suspeita de uso indevido da conta ou de divulgação inadequada.
- Cancele os acessos de um usuário quando ele se desligar da sua empresa.
- Não compartilhe dados pessoais nem dados confidenciais no Chat de Suporte ao sistema.
- O cadastro, o uso e o acesso das informações, entre outras operações com dados pessoais, deve ser realizado em conformidade com a LGPD.
- Utilize apenas os canais oficiais da Omie para solicitar contato, suporte e demais funcionalidades que oferecemos.



Contatos

Para assuntos de Segurança da Informação, utilize o e-mail ciso@omie.com.br

Para assuntos de privacidade, utilize o e-mail privacidade@omie.com.br



Suporte

Fale com a gente!

Clique aqui : nossa equipe de atendimento está sempre pronta para ajudar você.

Ajuda

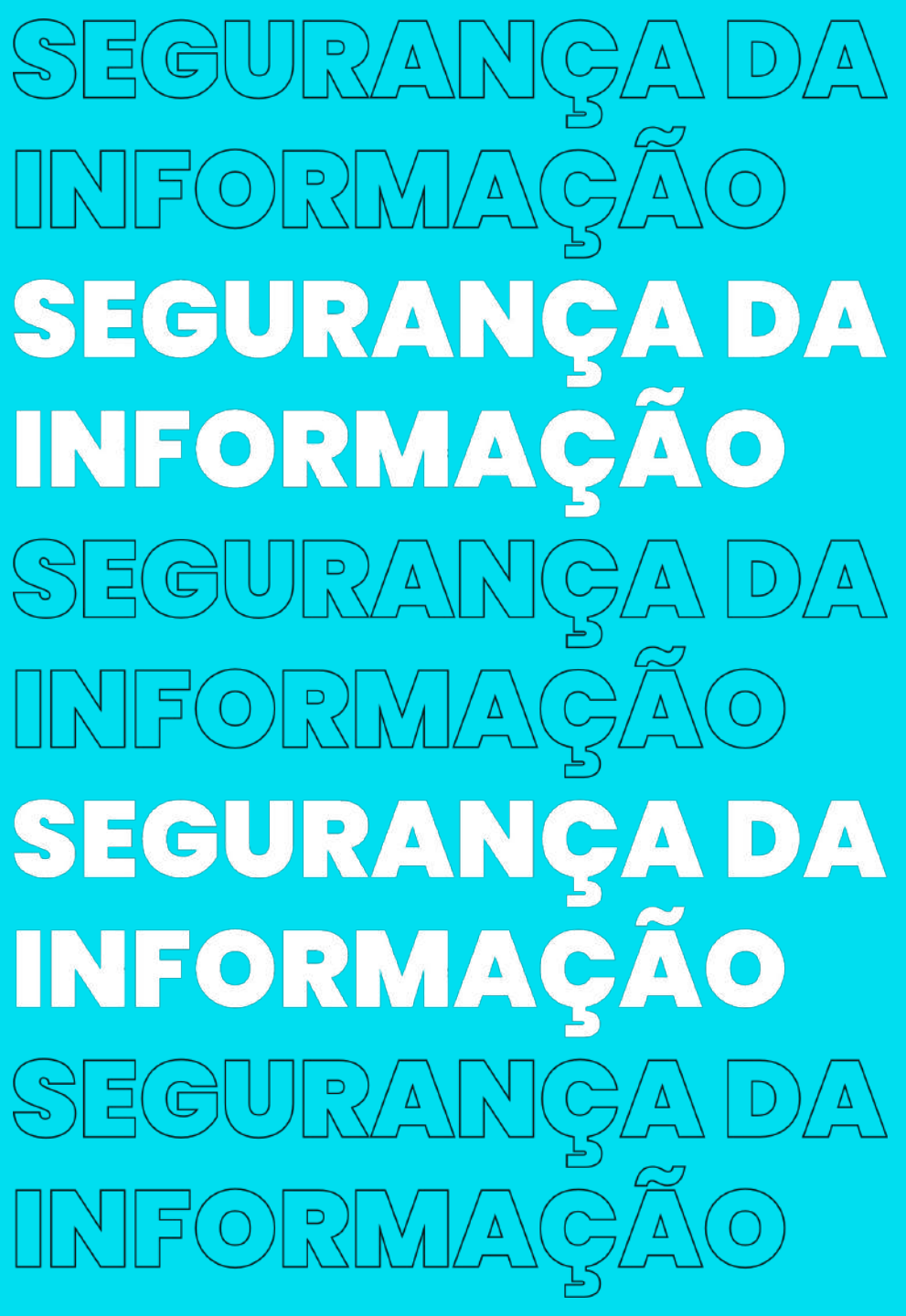
Encontre respostas para as dúvidas mais frequentes de nossos clientes.

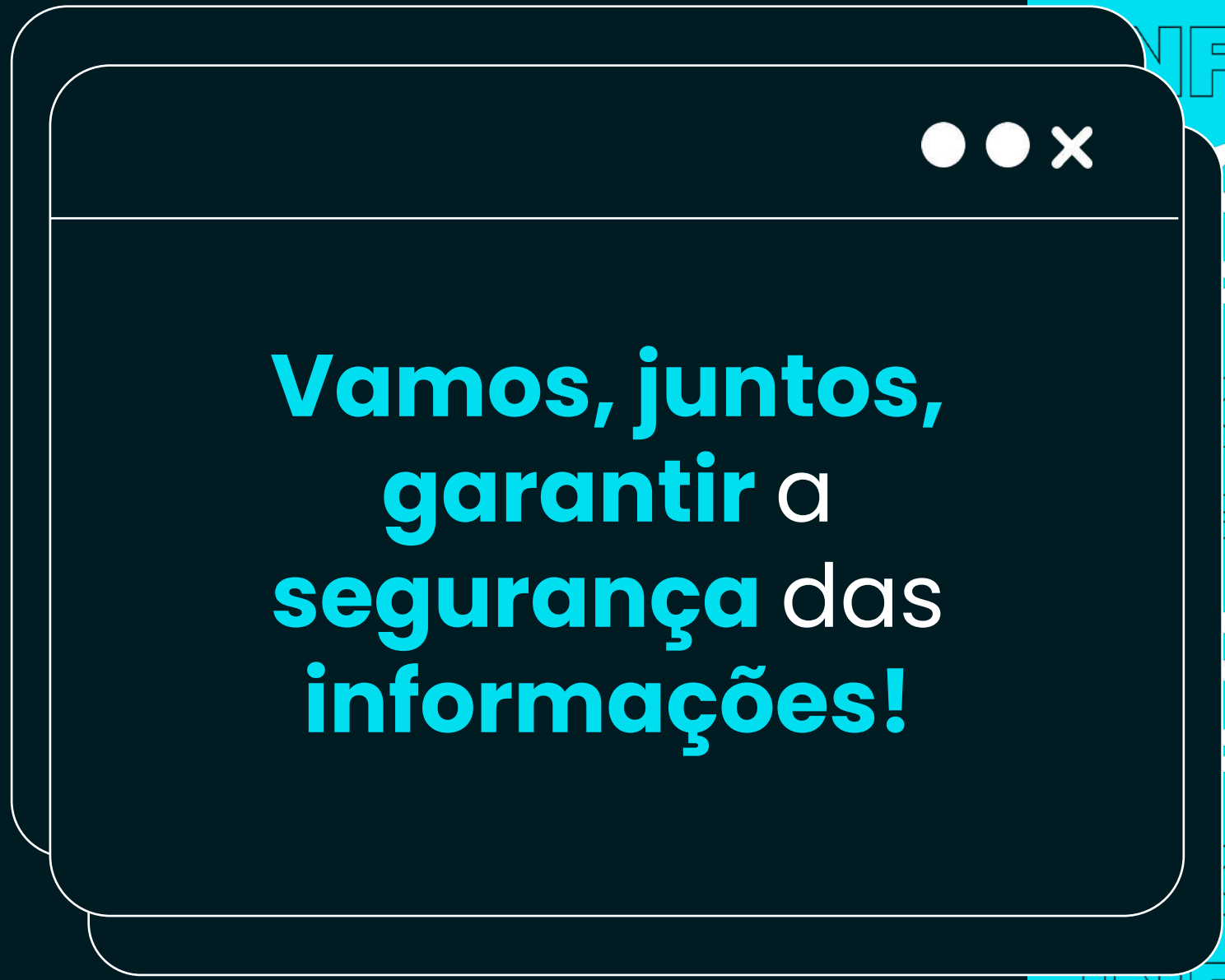
Chat

Receba atendimento personalizado, rápido e em tempo real.

0800 942 7592

Nossos atendentes estão preparados para tirar suas dúvidas.





SEGURANÇA DA INFORMAÇÃO