

Seus canais e sua jornada

Tudo o que gestores e colaboradores precisam para aproveitar o contrato com a Rastek: canais oficiais, prazos de atendimento e as sete práticas essenciais do dia a dia.

Canais oficiais de atendimento

CANAL PREFERENCIAL

app.tiflux.com.br

Abertura e acompanhamento de chamados

WHATSAPP

(51) 3398-2008

Dúvidas rápidas e urgências

TELEFONES

(51) 3398-2008 · (51) 3398-2110

Segunda a sexta, das 9h às 18h

E-MAIL

suporte@rasteksolucoes.com.br

Registro formal de solicitações

A jornada em 7 passos

1 Comece aqui

Canais oficiais e prazos de atendimento.

2 Senhas e MFA

Credenciais fortes e MFA nos sistemas.

3 Golpes digitais

Reconhecer phishing e fraudes antes do clique.

4 Home office

Rede, equipamento e ambiente seguros.

5 Uso de tecnologia

Softwares, arquivos, e-mail e uso seguro de IA.

6 Incidentes

O que fazer nos primeiros minutos.

7 Para gestores

Acessos, offboarding e cultura de segurança.

O que esperar do seu contrato

Atendimento com SLA

Prazos claros de início por prioridade, de 2h a 16h úteis, com histórico completo de cada chamado.

Operação preventiva

Monitoramento, atualizações e backup acompanhados de forma contínua, não apenas quando algo falha.

Segurança por padrão

Boas práticas de segurança, privacidade e conformidade aplicadas ao ambiente e às pessoas.

COMO USAR ESTE GUIA

Cada página a seguir corresponde a uma trilha da Central do Cliente. Distribua para as equipes, use em integrações de novos colaboradores e mantenha à mão nos primeiros 90 dias de contrato. Conteúdo completo e sempre atualizado em rastek.com.br/clientes.

Fale com a gestão

Reclamações, sugestões e elogios sobre o atendimento: operacional@rasteksolucoes.com.br — retorno em até 2 dias úteis. A Rastek nunca solicita a sua senha por e-mail, telefone ou WhatsApp.

Como acionar a Rastek

Saiba exatamente o que pedir, por qual canal e em quanto tempo o atendimento começa. Todo atendimento é registrado, garantindo histórico, continuidade e visibilidade para o gestor do contrato.

O que você pode solicitar

- Dúvidas de sistemas, e-mail e aplicativos
- Hardware: computador, notebook, periféricos
- Software homologado, atualizações e erros
- Rede e internet: lentidão, quedas, acesso remoto
- Impressão, digitalização e nuvem corporativa
- Segurança: suspeitas, alertas, acessos indevidos
- Backup e recuperação de arquivos

Como abrir um chamado

Escolha o canal e comece agora. Todos levam ao mesmo time — a diferença está na agilidade do registro.

RECOMENDADO

Sistema de chamados

Acompanhe o andamento, anexe prints e mantenha o histórico organizado.

app.tiflux.com.br

E-mail do suporte

Quando você não tem acesso ao sistema ou precisa encaminhar uma mensagem suspeita para análise.
suporte@rasteksolucoes.com.br

Telefone

Para quando não conseguir acessar e-mail e sistema.

(51) 3398-2008 · (51) 3398-2110

HORÁRIO E URGÊNCIAS

Atendimento de segunda a sexta, das 9h às 18h; chamados abertos fora desse período são tratados no início do próximo dia útil. Em situação crítica fora do horário, use o celular de atendimentos urgentes informado no contrato e registre o chamado em seguida.

Prazos de início de atendimento (SLA)

PRIORIDADE	QUANDO APLICAR	EXEMPLOS	INÍCIO
● P1 — Crítica	Empresa ou serviço crítico parado, ou incidente grave de segurança	Rede indisponível, servidor parado, ransomware	2h úteis
● P2 — Alta	Impacto relevante em vários usuários, setor ou processo	Departamento parado, serviço degradado	4h úteis
● P3 — Média	Impacto individual com alternativa possível	PC, Outlook, impressão, acesso, aplicação	8h úteis
● P4 — Baixa	Solicitação sem impacto imediato ou programável	Instalação, permissões, ajustes, orientações	16h úteis

ACELERE O SEU ATENDIMENTO

O prazo indica o tempo máximo para iniciar o atendimento; a solução depende da complexidade e de terceiros. Descreva o que aconteceu, copie a mensagem de erro e anexe um print. Suporte remoto autorizado por você em rastek.com.br/suporte-remoto.

Senhas e autenticação

A maioria dos incidentes começa em uma credencial: senha reutilizada, senha padrão nunca trocada, acesso compartilhado. Proteger credenciais depende de hábitos simples.

As regras essenciais

- Troque imediatamente qualquer senha padrão de primeiro acesso, inclusive as enviadas pela TI
- Use no mínimo 12 caracteres, misturando maiúsculas, minúsculas, números e símbolos
- Nunca reutilize a mesma senha em serviços diferentes — um vazamento não pode abrir várias portas
- Evite dados óbvios: datas, nomes de familiares, placa do carro, "123456" ou "empresa2024"
- Guarde senhas em um gerenciador confiável, nunca em planilhas, blocos de notas ou papéis
- Credenciais são individuais: não compartilhe a sua nem use a de um colega
- Ative a autenticação em dois fatores (MFA) em todos os sistemas que oferecem o recurso

MFA em linguagem simples

MFA é provar quem você é de duas formas: algo que você sabe (a senha) e algo que você tem (o celular com aplicativo autenticador ou biometria). Mesmo que descubram sua senha, o acesso não se completa. Prefira aplicativos autenticadores a códigos por SMS — o SMS é o método mais fácil de interceptar.

ATENÇÃO: FADIGA DE MFA

Nunca aprove uma notificação de acesso que você não solicitou. Golpistas disparam dezenas de pedidos em sequência esperando aprovação por cansaço. Negue todos e avise a Rastek imediatamente — é sinal de que sua senha já está em mãos erradas.

Passkeys: a evolução das senhas

Alguns serviços já permitem entrar sem senha, com uma chave vinculada ao dispositivo e liberada por biometria ou PIN. Como não existe senha digitável, não há o que ser adivinhado ou capturado por uma página falsa. Consulte a Rastek antes de adotar.

Suspeita de senha vazada? Faça isso agora

- Troque a senha do serviço afetado e de qualquer outro em que ela tenha sido reutilizada
- Avise a Rastek pelo sistema de chamados ou por telefone, informando a conta envolvida
- Verifique acessos e dispositivos desconhecidos conectados à conta
- Não use variações da senha antiga: crie uma senha nova e única

Sinais típicos: e-mails de redefinição que você não pediu, avisos de login de outra cidade, mensagens enviadas em seu nome. Verificar é rápido e não gera nenhuma penalidade.

Golpes digitais e engenharia social

Fraudes digitais não atacam sistemas: atacam a rotina das pessoas. Podem chegar por e-mail, WhatsApp, Microsoft Teams, SMS, ligação ou até por um áudio que imita a voz de alguém conhecido.

Os sinais de alerta

- Urgência artificial: “último aviso”, “conta será bloqueada hoje”
- Remetente levemente alterado — uma letra trocada no domínio muda tudo
- Links encurtados ou endereços diferentes do site oficial
- Anexos inesperados, sobretudo planilhas, ZIP e arquivos que pedem habilitar conteúdo
- Qualquer pedido de senha, código de verificação ou dados bancários
- Tom de segredo: “não comente com ninguém”, “resolva direto comigo”

Golpes que circulam hoje no Brasil

Boleto alterado

A cobrança chega parecida com a real, mas o código de barras ou o beneficiário foi trocado. Confira sempre o nome do beneficiário antes de pagar.

Falso diretor, TI ou RH

Por WhatsApp ou pelo Microsoft Teams, contas externas usam nome e foto de um gestor, do suporte de TI ou do RH e pedem transferência, código ou acesso remoto. Confirme por canal já conhecido.

Encomenda retida

SMS pede taxa pequena ou atualização de endereço em site falso, capturando dados de cartão.

Clone de imagem e voz com IA

Áudios, chamadas e vídeos imitam a voz ou o rosto de um diretor para autorizar pagamentos. Nunca aprove apenas por áudio ou vídeo.

REGRA DE OURO

Na dúvida, não clique. Pergunte à Rastek — verificar leva 2 minutos, um incidente pode custar dias.

Cliquei. E agora?

- Avise a Rastek imediatamente por telefone ou pelo sistema de chamados
- Se informou uma senha, troque-a agora e diga qual conta foi usada
- Não apague a mensagem: ela ajuda na análise e na proteção dos colegas
- Siga as orientações da equipe antes de desligar ou reiniciar o equipamento

Acontece com profissionais experientes, inclusive de TI. O que define o desfecho não é o clique, é a velocidade do aviso. Ninguém será punido por reportar.

Comunicação legítima da Rastek

Nossos contatos partem sempre de rastek.com.br, rasteksolucoes.com.br, do sistema app.tiflux.com.br e de e-mails @rasteksolucoes.com.br. A Rastek nunca solicita sua senha por e-mail, telefone ou WhatsApp.

Trabalho remoto e híbrido

Fora do escritório, você passa a ser também o responsável pelo ambiente. Quatro blocos simples cobrem praticamente todos os riscos do trabalho remoto.

1. Sua rede

- Senha forte e exclusiva no Wi-Fi de casa; troque a senha padrão do roteador
- Não use Wi-Fi público para trabalho sem VPN ou orientação da TI
- Fora de casa, prefira o roteamento de dados do próprio celular
- Evite compartilhar a rede de trabalho com dispositivos de visitantes

2. Seu equipamento

- Bloqueie a tela sempre que se afastar, mesmo por poucos minutos
- Mantenha sistema e aplicativos atualizados; separe uso pessoal do corporativo
- Não instale programas por conta própria: solicite instalação homologada
- Mantenha o antivírus ativo; nunca desative proteções para “resolver” um erro
- Salve arquivos nos repositórios oficiais para que o backup os alcance

3. Seu ambiente

- Posicione a tela fora do alcance de curiosos, inclusive em casa
- Evite reuniões confidenciais em locais públicos; use fone de ouvido
- Atenção ao compartilhar tela: documentos e notificações expõem dados
- Guarde anotações e impressões em local reservado; descarte com fragmentação

4. Em trânsito

- Nunca deixe notebook, tablet ou celular visível dentro do veículo
- Em cafés e coworkings, não deixe o equipamento sozinho
- Em viagens, transporte o equipamento na bagagem de mão
- Perda ou furto: avise a Rastek imediatamente para bloqueio dos acessos

REGRA DE OURO

Em casa, na rua ou no escritório, trate cada arquivo e cada tela como se estivessem sobre a mesa de uma sala de reunião com a porta aberta.

Dados pessoais também vão para casa

Planilhas de clientes, contratos, currículos e relatórios com nomes, CPFs ou dados de saúde são protegidos pela LGPD: o cuidado do escritório vale na sala de casa. Acesse apenas pelos sistemas oficiais e compartilhe somente com quem precisa da informação.

Uso responsável dos recursos

Equipamentos, sistemas e dados são ativos da empresa. Usá-los bem protege o seu trabalho, o dos colegas e a informação de quem confia no negócio.

Instalação de softwares: sempre pela TI

Quando alguém instala ferramentas por conta própria surge o shadow IT — tecnologia em uso sem conhecimento da empresa. O risco é duplo: o programa pode conter malware ou versão pirateada, e os dados que passam por ele ficam fora de qualquer controle de backup, acesso e conformidade.

- Precisa de uma ferramenta nova? Abra um chamado explicando o objetivo
- Não baixe instaladores de sites de download ou links patrocinados
- Não use versões “crackeadas” ou geradores de licença
- Extensões de navegador também são software: peça avaliação antes

Onde guardar arquivos

- Não armazene documentos de trabalho em pendrives ou HDs pessoais
- Não envie arquivos da empresa para e-mails ou drives particulares
- Não mantenha a única cópia de um documento na área de trabalho local
- Compartilhe pelo repositório oficial, apenas com quem precisa

E-mail corporativo

- Use-o para assuntos de trabalho; cadastros pessoais no e-mail particular
- Confira o destinatário antes de enviar — o preenchimento automático é a principal causa de vazamento acidental
- Ao enviar para vários contatos externos, use cópia oculta
- Não encaminhe correntes, anexos desconhecidos ou conteúdo não solicitado

Inteligência artificial no trabalho

A IA é bem-vinda, desde que homologada pela empresa, com contrato adequado e controle de retenção. A atenção está no que você digita: um prompt é um envio de dados, que pode ser armazenado, processado em outro país e, em plataformas gratuitas, usado para treinar modelos.

- Use apenas ferramentas aprovadas; em caso de dúvida, pergunte antes
- Nunca insira dados de clientes, dados pessoais, contratos ou credenciais
- Descreva o problema de forma genérica, sem nomes, CPFs ou trechos sigilosos
- Revise o resultado: a responsabilidade pela entrega continua sendo humana

REGRA DE OURO

Se a informação não poderia ser publicada, ela também não deve ser colada em um prompt de uma ferramenta de IA não aprovada.

Algo deu errado? Aja rápido

Incidentes acontecem em empresas de todos os tamanhos. O que diferencia um susto de um prejuízo é a rapidez do aviso — e é nisso que você pode ajudar.

O que é um incidente, na prática

- Cliquei em um link suspeito ou abri um anexo inesperado
- Perdi ou tiveram furtado notebook, celular ou pendrive de trabalho
- Tela pedindo resgate ou informando arquivos criptografados
- Arquivos sumiram, mudaram de nome ou não abrem mais
- Confirmação de login ou troca de senha que eu não fiz
- Um colega recebeu mensagem estranha enviada em meu nome
- Computador subitamente lento, com janelas abrindo sozinhas
- Qualquer comportamento fora do normal em acessos e arquivos

Por que os minutos importam

Em um ataque de ransomware, a criptografia se espalha pela rede em minutos. A diferença entre avisar agora e avisar no dia seguinte pode ser a diferença entre isolar um computador e restaurar dias inteiros de trabalho de toda a empresa. O mesmo vale para credenciais: bloquear uma conta comprometida no início impede o acesso a e-mails, sistemas financeiros e dados de clientes.

Os três NÃO

Não desligue o equipamento

Sem orientação, desligar pode apagar informações essenciais para entender o que aconteceu e agravar a perda de arquivos.

Não tente resolver sozinho

Programas de limpeza, exclusões e reinstalações por conta própria destroem evidências e atrasam a recuperação.

Não esconda o ocorrido

Nenhuma penalidade virá do aviso. O silêncio custa tempo — e tempo é exatamente o que protege a empresa.

A quem avisar e o que informar

- Urgências: ligue para (51) 3398-2008 ou (51) 3398-2110 e, fora do horário comercial, acione o celular de atendimentos urgentes constante no contrato
- Sistema de chamados: app.tiflux.com.br, com prioridade urgente
- E-mail: suporte@rasteksolucoes.com.br, útil para encaminhar a mensagem suspeita
- Avise também o gestor imediato da sua área
- Informe: o que aconteceu, quando, em qual equipamento e usuário
- Diga se informou senha, código ou dado de pagamento e se outras pessoas receberam a mesma mensagem

REGRA DE OURO

Avisar rápido é o comportamento que protege todos. Quem reporta um incidente está ajudando a empresa — não sendo julgado por ele.

Boas práticas de governança

Tecnologia bem gerida depende de decisões de gestão. Estas práticas custam pouco tempo e reduzem de forma significativa o risco operacional da sua empresa.

O papel do gestor na cultura de segurança

O time reproduz o comportamento da liderança. Quando o gestor bloqueia a tela ao sair da mesa, usa MFA sem reclamar e trata um alerta com seriedade, a equipe entende que aquilo faz parte do trabalho. O contrário também é verdadeiro: uma exceção aberta para a diretoria vira, em pouco tempo, exceção para todos.

Revisão periódica de acessos

- Priorize sistemas financeiros, folha, dados de clientes e contas administrativas
- Revogue permissões herdadas de funções anteriores
- Confirme que cada acesso é individual, sem contas compartilhadas
- Solicite à Rastek a relação de usuários e permissões dos ambientes gerenciados

OFFBOARDING: AVISE DE FORMA PROGRAMADA

Sempre que possível, comunique o desligamento de forma programada, com data e hora de bloqueio definidas com antecedência. Em desligamentos excepcionais, a comunicação deve ser imediata, no ato do desligamento, para bloqueio de acessos, e-mail, VPN, sistemas em nuvem e dispositivos. Contas ativas de ex-funcionários estão entre os riscos mais comuns em pequenas e médias empresas — e entre os mais simples de eliminar.

Admissões e desligamentos

- Admissão: informe cargo, área e sistemas com antecedência, com privilégio mínimo
- Recolha os equipamentos e registre a devolução
- Desligamento programado: avise com antecedência, com data, hora e destino de arquivos e e-mail
- Mudança de função: trate como novo acesso, revogando o que não é mais necessário
- Desligamento excepcional: comunique imediatamente, no ato, para bloqueio em tempo real

Controle de exceções

- Toda exceção deve ser registrada, com motivo claro
- Temporária, com data de revisão definida
- Aprovada por um responsável identificado
- Revisada no vencimento: renove formalmente ou encerre

Cultura de reporte e acompanhamento do contrato

Ambientes que punem quem erra não ficam mais seguros: ficam mais silenciosos. Deixe explícito que reportar é o comportamento esperado. Use app.tiflux.com.br para acompanhar volumes, recorrências, prazos e relatórios; assuntos de escopo, projetos e melhorias com a gestão de operações em operacional@rasteksolucoes.com.br. Recorrências no histórico são o melhor indicador de onde investir na próxima etapa.