

Segurança em Aplicativos de Mensagens

Segurança da Informação



Informativos Gerais



Introdução

Segurança em Aplicativos de Mensagens

Na Rede Américas, devemos utilizar apenas ferramentas homologadas para a comunicação interna e externa entre colaboradores(as) e parceiros. Em determinadas situações, pode haver a necessidade de recorrer a aplicativos de mensagem instantânea para comunicação com clientes (WhatsApp, por exemplo). Para isso, é fundamental que esses aplicativos sejam previamente avaliados pela equipe de Segurança da Informação, a fim de garantir a proteção dos dados e o cumprimento das normas internas.

Este manual tem como objetivo orientar tanto o uso profissional quanto o pessoal, com exemplos práticos que visam manter a segurança, a privacidade e a responsabilidade legal em todas as formas de comunicação.

Ferramentas oficiais e uso de aplicativos de mensagem

Uso corporativo:

As ferramentas homologadas garantem a conformidade com as normas internas e a segurança dos dados. Quando a comunicação com pacientes, clientes ou parceiros exige o uso de aplicativos de mensagem, esses devem ser avaliados pela equipe de Segurança da Informação.

Uso pessoal:

Caso utilize esses aplicativos para fins pessoais, adote as boas práticas apresentadas neste manual, pois o mesmo rigor na utilização é necessário para garantir a segurança dos seus dados.

Compartilhamento de informações sensíveis

Tudo que for compartilhado com terceiros corre o risco de "vazar". Por isso, não compartilhe informações que contenham dados sensíveis, os quais podem causar prejuízo financeiro, problemas legais ou facilitar golpes de roubo de identidade.

Não compartilhe os seguintes itens:

- Cópia de laudos, exames, RG, CPF, certidões, atestados e declarações;
- Dados bancários, senhas, notas fiscais, recibos e imagens de cartões de crédito;
- Dados e documentos de terceiros: lembre-se de que, se essas informações forem vazadas, a responsabilidade recairá sobre quem as compartilhou;
- Imagens de terceiros sem o devido consentimento.

Utilize sempre os canais oficiais e seguros para o compartilhamento de informações e, em caso de dúvida, consulte a equipe de Segurança



Respeite as regras de cada aplicativo

Como exemplo, apresentamos algumas diretrizes dos Termos de Uso do WhatsApp. Segundo esses termos, o serviço não deve ser utilizado para:

- **Compartilhar informações falsas, incorretas ou enganosas (fake news);**
- **Enviar comunicados em massa ou mensagens automáticas (spam);**
- **Divulgar conteúdos que infrinjam os direitos de privacidade e propriedade intelectual (plágio).**

A violação dos termos de uso pode acarretar sanções legais e administrativas, incluindo o banimento da plataforma.

Quadro comparativo com exemplos práticos

Situação	O que fazer 	O que não fazer 
Documentos e informações pessoais	Compartilhe apenas notificações públicas ou informações que, se acessadas por terceiros, não causem prejuízo ou violem a privacidade.	Enviar laudos, exames, RG, CPF, certidões, atestados e declarações de terceiros.
Envio de arquivos	"Olá, seu exame já está disponível no nosso aplicativo."	"Olá, segue arquivo anexo com seu exame."
Dados bancários	Encaminhar os dados bancários do fornecedor por e-mail corporativo ou pelo sistema financeiro interno.	Enviar os dados bancários do fornecedor pelo grupo de WhatsApp.
Relatórios financeiros	"Acabei de enviar um e-mail com o relatório completo e os indicadores para sua análise."	"Este gráfico mostra que nossa receita cresceu 15% este mês, mas deve cair 5% no próximo."
Processos de seleção e remuneração	"Vou te ligar para conversarmos de forma mais detalhada sobre a proposta de remuneração do candidato."	"O candidato Carlos, do Banco XYZ, pediu 5 mil reais, menos do que nosso analista Antônio."
Relatórios confidenciais	"O relatório financeiro do mês já está disponível no nosso portal seguro. Confira seu e-mail para mais detalhes."	"Enviei o relatório financeiro do mês no grupo do WhatsApp."
Exames e laudos	"Olá, o laudo do exame do paciente João está disponível no sistema seguro de saúde. Por favor, acesse-o com sua senha."	"Olá, segue o laudo do exame do paciente João pelo WhatsApp."
Informações de pacientes	"Entre em contato pelo canal seguro para discutirmos os detalhes do caso da paciente Maria."	"Saiu o resultado do paciente Maria e ela está com câncer."
Prontuários	"Favor encaminhar o prontuário do paciente por meio do nosso sistema interno para garantir a segurança dos dados."	"Envie uma foto do prontuário do paciente para análise imediata aqui no WhatsApp."
Agendamento e confirmação de consultas	"Prezado paciente, sua consulta já foi agendada. Por favor, confirme a data e horário pelo nosso portal."	"Prezado paciente, o link para confirmar sua consulta é http://site.com/consulta/12345 ."

Riscos dos aplicativos de mensagem

Todo aplicativo de mensagens possui vulnerabilidades que podem ser exploradas por criminosos. Esteja atento aos seguintes riscos:

- **Clonagem de conta:**

Nunca forneça o código de autenticação do aplicativo. Se esse código for compartilhado, um criminoso poderá assumir o controle do seu perfil e acessar todos os seus contatos.

- **Mensagens falsas e links fraudulentos:**

Desconfie de mensagens que contenham links suspeitos, pois podem infectar seu dispositivo com vírus ou roubar seus dados pessoais.

- **Abertura de anexos maliciosos:**

Evite abrir anexos de fontes desconhecidas. Arquivos maliciosos podem comprometer seu dispositivo, possibilitando o acesso indevido a senhas, dados bancários e outros códigos de acesso.

Atenção na versão Web

Encerramento de sessão:

Ao utilizar a versão Web em computadores compartilhados, certifique-se de encerrar a sessão ao finalizar suas atividades para evitar o acesso não autorizado às suas mensagens.

Verificação por biometria:

Ative a verificação por biometria no seu celular, uma vez que o acesso à versão Web depende da autenticação com o aparelho.

Gerenciamento de dispositivos:

Verifique regularmente em quais dispositivos o aplicativo está ativo e desconecte aqueles que não estiverem em uso.

Boa conduta na comunicação

Para manter uma comunicação clara e profissional, observe as seguintes práticas:

Revisão dos textos:

Sempre revise seus textos antes de enviá-los para evitar erros ortográficos ou de concordância que possam comprometer sua imagem profissional.

Uso de gírias e abreviações:

Evite gírias e abreviações excessivas que podem não ser compreendidas por todos.

Uso de emojis:

Evite utilizar emojis, principalmente em conversas com pacientes e clientes, a fim de manter o tom formal e profissional.

Uso de caixa alta:

Evite escrever em CAIXA ALTA, a menos que seja para alertar ou destacar uma nomenclatura ou sigla, pois pode ser mal interpretado.

Horário de uso profissional:

Se o aplicativo for destinado para fins profissionais, utilize-o somente durante o horário comercial e siga as regras de classificação das informações.

Envio de áudios:

Evite enviar áudios longos. Confirme com o interlocutor se o envio desse formato é adequado para a comunicação pretendida.

Responsabilidade legal e controle das informações online

Responsabilidade legal:

Somos legalmente responsáveis por tudo o que compartilhamos. Respeite o direito de todos antes de expor imagens ou dados. Sempre solicite o consentimento antes de compartilhar informações de terceiros.

Controle das informações online:

Uma vez que um conteúdo é publicado na internet, você perde o controle sobre como e por quem ele será utilizado, podendo se espalhar rapidamente para um público desconhecido.

Envio seguro de imagens:

Quando necessário enviar imagens, opte por recursos como envio de visualização única ou mensagens temporárias, garantindo que os dados não permaneçam armazenados por muito tempo. Consulte o site do aplicativo para mais detalhes.

Conheça os Termos de Privacidade:

Aplicativos gratuitos possuem Termos de Aceite ou Políticas de Privacidade que detalham quais dados são coletados e como eles podem afetá-lo. Mantenha-se informado sobre essas políticas.

Considerações finais de imagens:

Manter uma comunicação segura e responsável é responsabilidade de todos, seja utilizando as ferramentas oficiais da empresa ou aplicativos de mensagens para uso pessoal, adote sempre as práticas recomendadas para proteger informações sensíveis e evitar riscos legais.

Este manual serve como referência para que cada pessoa compreenda a importância de uma comunicação consciente, alinhada com as diretrizes de segurança e as políticas internas.



Rede
Américas

paixão por cuidar