OAB SANTA CATARINA | Subseção Chapecó

Cartilha

Segurança da Informação e Mitigação de Riscos

Sumário

Apresentação das Presidentes.

É com grande honra que apresentamos esta cartilha sobre Segurança da Informação e Mitigação de Riscos.
Em um mundo onde a tecnologia evolui a passos largos e a informação se tornou um dos nossos ativos mais valiosos, é imperativo que tenhamos um guia claro e acessível para proteger nossos dados e, consequentemente, nossa privacidade e integridade.

A Lei de Acesso à Informação (Lei nº 12.527) e a Lei Geral de Proteção de Dados (Lei nº 13.709), são pilares fundamentais para garantir a transparência e a segurança no manejo das informações pessoais. Elas nos proporcionam as ferramentas necessárias para proteger nossos dados contra usos indevidos e acessos não autorizados.

Na OAB Chapecó por meio da Comissão de Direito Digital, temos o compromisso de promover a boa administração da justiça e de ampliar continuamente o espaço de discussão sobre temas cruciais, como a mitigação de riscos e a segurança da informação.
Esta cartilha é um reflexo deste compromisso, oferecendo orientações práticas e de fácil entendimento para fortalecer nossas defesas contra ameaças digitais.

Nossa gratidão à Subseção de Chapecó, especialmente à Comissão de Direito Digital por meio dos membros participantes da criação deste material.

Estendemos nossos agradecimentos também aos parceiros, incluindo a empresa RPF Comunicação, cujo apoio foi fundamental para a concretização deste projeto.

Estamos confiantes de que, juntos, criaremos um ambiente digital mais seguro e protegido para todos.

A segurança da informação é uma responsabilidade compartilhada, e cada passo em direção à conscientização e adoção de boas práticas é um avanço significativo para toda a sociedade.

Cordialmente,

Dra. Maria Tereza Zandavalli Lima
Presidente da OAB Chapecó
OAB/SC 22.673

Dra. Sabrine Sulzbach Haetinger
Presidente Comissão de Direito Digital OAB Chapecó
OAB/SC 46.379

OAB SANTA CATARINA | Subseção Chapecó

Agradecimentos

Gostaríamos de expressar nossa mais sincera gratidão:

• À Presidente da OAB Chapecó, Maria Tereza Zandavalli Lima, pelo apoio contínuo e liderança exemplar.

• Aos membros da Comissão de Direito Digital da Subseção de Chapecó, que, sob a liderança da Dra. Sabrine Sulzbach Haetinger, demonstraram um trabalho exemplar e dedicação incansável na elaboração desta cartilha.

• Aos colaboradores e parceiros que participaram deste projeto, fornecendo insights valiosos e ajudando a disseminar a importância da segurança da informação.

• À empresa RPF Comunicação, cujo apoio foi essencial para a realização deste projeto.

Reconhecemos o valor de cada um de vocês na concretização desta cartilha e reiteramos nosso compromisso com a promoção da segurança da informação em todos os níveis.

OAB SANTA CATARINA | Subseção Chapecó

Apresentação da Presidente da Comissão de Direito Digital

É com grande satisfação e sentido de dever que a Comissão de Direito Digital da Subseção de Chapecó apresenta esta cartilha sobre Segurança da Informação e Mitigação de Riscos. Vivemos em uma era de constante evolução tecnológica, onde a proteção dos nossos dados pessoais e empresariais se torna uma prioridade vital. Este material foi cuidadosamente elaborado para esclarecer conceitos fundamentais e fornecer estratégias práticas que garantam a segurança da informação em nossas vidas diárias.

Em consonância com as palavras da Presidente Maria Tereza, destacamos a relevância das legislações como a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados. Estas leis não apenas protegem nossos dados, mas também promovem uma cultura de transparência e responsabilidade.

Nosso compromisso com a segurança digital é contínuo. A adoção de boas práticas é fundamental para garantir um ambiente seguro para todos. Esperamos que esta cartilha seja uma ferramenta valiosa para advogados, empresários, lojistas e cidadãos preocupados com a proteção de suas informações.

Atenciosamente,
Dra. Sabrine Sulzbach Haetinger
Presidente da Comissão de Direito Digital da OAB/SC - Subseção de Chapecó
OAB/SC 46.379

Introdução à Cartilha

A segurança da informação diz respeito à proteção dos dados contra acesso não autorizado, uso indevido, alteração ou destruição.

Isso é importante porque nossos dados pessoais e informações confidenciais estão cada vez mais presentes em nossas vidas digitais.

Protegê-los significa garantir nossa privacidade, evitar fraudes e preservar a integridade das informações que compartilhamos online e offline.

Objetivos da Cartilha

Bem-vindo à nossa cartilha sobre Política de Segurança da Informação e Mitigação de Riscos.

O objetivo deste guia é fornecer orientações práticas para proteger suas informações e reduzir riscos associados a cibercrimes.

Com a crescente digitalização e o uso intensivo de tecnologias no dia a dia, é crucial adotar medidas de segurança para garantir a proteção de dados pessoais e profissionais.

Esta cartilha foi desenvolvida para advogados e sociedade em geral, com dicas simples e eficazes para manter suas informações seguras.

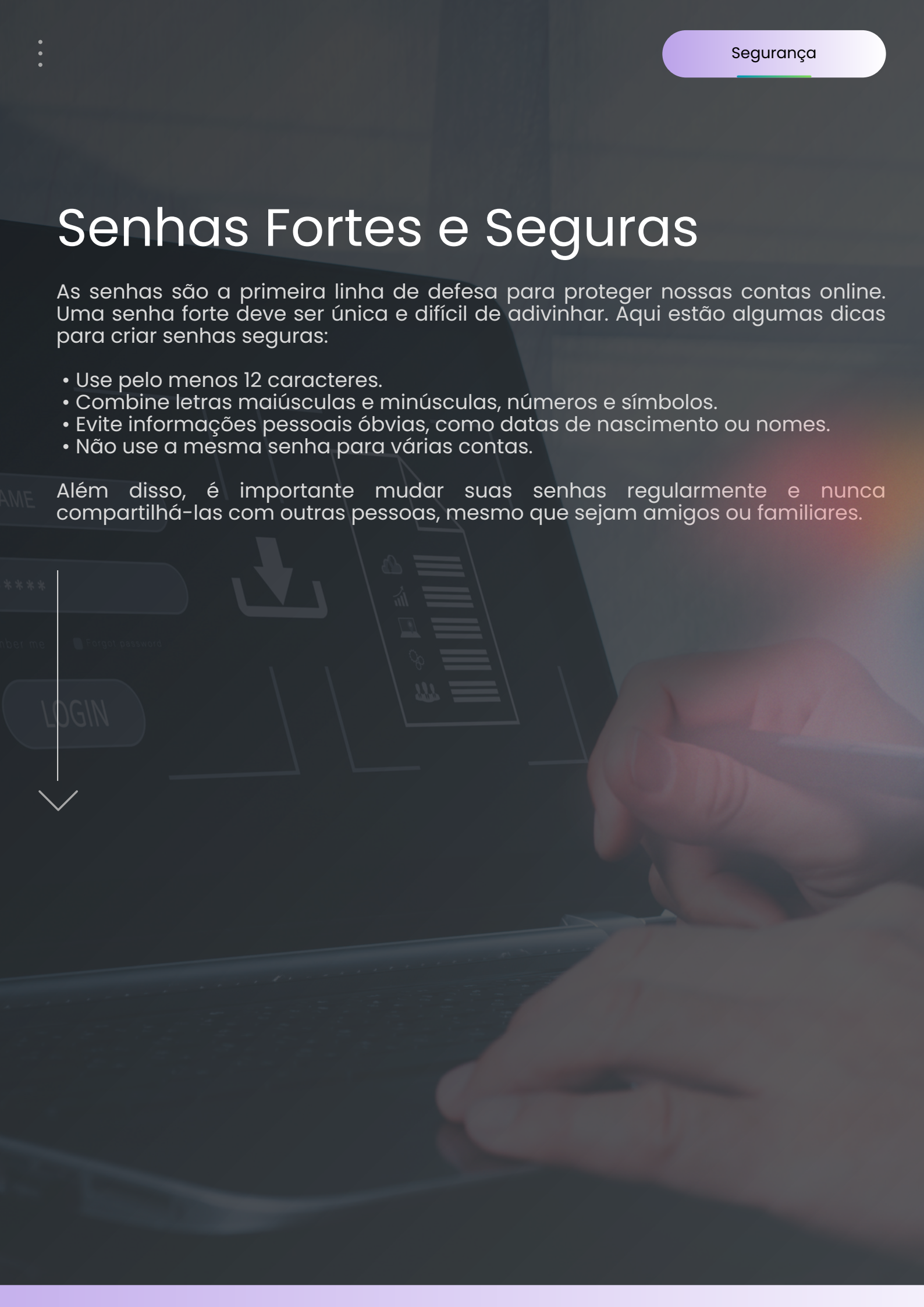
Boa leitura!

Senhas Fortes e Seguras

As senhas são a primeira linha de defesa para proteger nossas contas online. Uma senha forte deve ser única e difícil de adivinhar. Aqui estão algumas dicas para criar senhas seguras:

- Use pelo menos 12 caracteres.
- Combine letras maiúsculas e minúsculas, números e símbolos.
- Evite informações pessoais óbvias, como datas de nascimento ou nomes.
- Não use a mesma senha para várias contas.

Além disso, é importante mudar suas senhas regularmente e nunca compartilhá-las com outras pessoas, mesmo que sejam amigos ou familiares.



Uso Consciente do E-mail

O e-mail é uma ferramenta essencial na comunicação, mas também é um alvo frequente de cibercriminosos.

Ataques como [1]phishing e disseminação de [2]malware exploram a vulnerabilidade do e-mail para obter dados pessoais e causar danos.

É fundamental adotar medidas de segurança para proteger suas informações.
Para se proteger:

- Verifique o endereço de e-mail do remetente.
- Não clique em links suspeitos ou baixe anexos de remetentes desconhecidos.
- Fique atento a erros gramaticais ou de ortografia que podem indicar um e-mail de phishing.
- Desconfie de solicitações urgentes de informações pessoais.
- Adicione uma camada extra de segurança às suas contas de e-mail com o uso de autenticação multifator [3](MFA).
- Em ambiente de trabalho, se você receber um e-mail suspeito, exclua-o imediatamente ou encaminhe-o para sua equipe de segurança de TI para avaliação.

[1] Phishing é um tipo de ataque cibernético que utiliza a engenharia social para enganar usuários e induzir as vítimas a fornecer dados pessoais, como senhas, números de cartão de crédito ou informações de login.

[2] Malware é um termo genérico para qualquer tipo de software malicioso, projetado para causar danos ou explorar dispositivos, serviços ou redes.

[3] A autenticação multifator (MFA) é um sistema de segurança que exige mais do que apenas uma senha para confirmar a identidade do usuário para acessar uma conta online.

Atualizações de Software

Manter seu software atualizado é essencial para proteger seu dispositivo contra vulnerabilidades conhecidas. Isso inclui sistemas operacionais, navegadores da web, programas de segurança e aplicativos. As atualizações frequentemente corrigem falhas de segurança que os hackers podem explorar para acessar seus dados. Para verificar e instalar atualizações:

- Configure seu dispositivo para atualizar automaticamente, se possível.
- Verifique regularmente se há atualizações disponíveis nos menus de configurações do seu sistema ou aplicativo.
- Não ignore atualizações, mesmo que pareçam pequenas. Cada uma delas pode melhorar a segurança do seu dispositivo.

Uso Responsável de Dispositivos Móveis

Nossos smartphones e tablets armazenam muitas informações pessoais e podem ser alvos de roubo ou ataques cibernéticos. Para proteger seus dispositivos:

• Use um código de acesso forte ou biometria (como impressão digital ou reconhecimento facial).

• Evite conectar-se a redes Wi-Fi públicas não seguras, onde suas informações podem ser interceptadas por hackers.

• Instale aplicativos apenas de fontes confiáveis, como lojas de aplicativos oficiais.

• Se perder seu dispositivo, utilize serviços de rastreamento ou bloqueio remoto oferecidos pelos sistemas operacionais para proteger seus dados.

Backup de Dados

Fazer backup regularmente de seus dados é crucial para garantir que você possa recuperá-los em caso de perda, roubo ou corrupção de arquivos. Existem várias maneiras de fazer isso de forma segura:

- Use serviços de backup na nuvem que ofereçam criptografia forte.
- Faça backups físicos em unidades externas e mantenha-as em um local seguro.
- Teste regularmente a restauração de seus backups para garantir que eles estejam funcionando corretamente.

Ao fazer backups regularmente, você pode minimizar o impacto de perdas de dados inesperadas.

Redes Sociais e Informações Pessoais

Nas redes sociais, devemos ter cuidado com as informações que compartilhamos, pois elas podem ser usadas por pessoas mal-intencionadas. Aqui estão algumas dicas para proteger suas informações pessoais:

• Revise e ajuste as configurações de privacidade para controlar quem pode ver suas postagens e informações pessoais.

• Evite compartilhar detalhes sensíveis, como números de telefone, endereços ou informações financeiras.

• Pense antes de publicar: uma vez na internet, é difícil remover informações pessoais.

Ao proteger suas informações nas redes sociais, você reduz o risco de roubo de identidade e outros problemas de segurança.

Denúncia de Incidentes

Se você suspeitar de um incidente de segurança, como acesso não autorizado à sua conta ou perda de dados, é importante agir rapidamente. Aqui estão os passos que você pode seguir:

• Informe imediatamente seu supervisor ou equipe de TI, se estiver no ambiente de trabalho.

• Registre todos os detalhes relevantes do incidente, como horário, método de ataque percebido e quaisquer ações tomadas.

• Se necessário, altere suas senhas imediatamente para proteger suas contas.

Reportar incidentes de segurança ajuda a proteger não apenas suas informações, mas também as de outros usuários e a fortalecer a segurança geral da organização.

Conclusão

O objetivo desta cartilha é fornecer informações e orientações práticas para ajudar a proteger seus dados e informações pessoais.

A segurança da informação é uma responsabilidade contínua e compartilhada. Esperamos que este material tenha sido útil e que você possa aplicar as boas práticas aqui apresentadas em seu dia a dia.

A Comissão de Direito Digital da Subseção de Chapecó está sempre à disposição de todos.

Para mais informações ou dúvidas, entre em contato conosco através do e-mail: **oabchapeco@desbrava.com.br**

Muito obrigado.

Comissão Organizadora da Cartilha

COMISSÃO DE DIREITO DIGITAL OAB Chapecó

Dra. Sabrine Sulzbach Haetinger OAB/ 46.379
Dr. Vinicius Almada Mozetič - OAB/ 34.373
Dr. Andrei Bueno Sander OAB/ 15.381
Dra. Viviane Negri- OAB/ 47.349
Dra. Patricia Fortuna - OAB/ 46.909
Dra. Bernardo Ibagy Pacheco - OAB/SC 14.932
Dra. Juliana de Almeida Barbosa - OAB/SP 329.085 - OAB/SC 68.157
Dra. Elenice Bueno - OAB/28.461

OAB SANTA CATARINA | Subseção Chapecó

Desenvolvido por RPF Comunicação