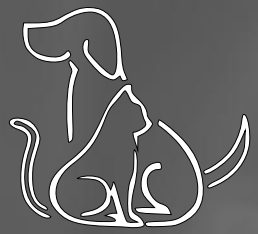
Boas Práticas de Acesso Seguro

ONG CÃOMER



Bem-vindo à nossa cartilha de segurança!

Nesta cartilha, você encontrará orientações essenciais para proteger nossas informações e assegurar que todos nós – colaboradores e voluntários – trabalhemos em um ambiente digital seguro.

Segurança de Senhas e Acesso

Crie Senhas Fortes

- Use senhas longas (pelo menos 12 caracteres) e misture letras maiúsculas, minúsculas, números e símbolos.
- Evite usar informações pessoais, como aniversários ou nomes, nas senhas.

Não Compartilhe Suas Senhas

- Nunca compartilhe sua senha com colegas, amigos ou familiares. Use um gerenciador de senhas se precisar lembrar várias.

Autenticação de Dois Fatores (2FA)

- Habilite o 2FA nas plataformas da ONG para uma camada extra de segurança. Isso ajuda a proteger seu acesso mesmo se sua senha for comprometida.

Uso de Redes Wi-Fi de Forma Segura

Conecte-se Somente a Redes Seguras

- Use sempre a rede segura e protegida da ONG. Redes públicas (como cafés ou redes abertas) são alvos fáceis para ataques.
- Para comunicações entre filiais, utilize a VPN da ONG, que oferece uma conexão segura e criptografada.

Proteção de Dados Sensíveis

Manuseio e Armazenamento de Dados

- Dados de adotantes, doadores e animais devem ser armazenados em plataformas seguras e de forma criptografada.
- Nunca salve informações sensíveis em dispositivos pessoais.

Faça Backups Regulares

- Realize backups dos dados críticos semanalmente ou automaticamente, para garantir que as informações estejam sempre protegidas.

Segurança Física nas Filiais

Acesso Restrito a Áreas Sensíveis

- A entrada nas áreas administrativas deve ser restrita a colaboradores autorizados.
- Não permita que visitantes tenham acesso a computadores ou áreas onde dados confidenciais estão armazenados.

Câmeras de Segurança e Alarmes

- Certifique-se de que câmeras e alarmes estejam funcionando adequadamente e revisados periodicamente para proteger nossos espaços.

Prevenção e Resposta a Incidentes de Segurança

Esteja Atento a Tentativas de Phishing

- Não clique em links suspeitos e não abra anexos desconhecidos, especialmente em e-mails de remetentes desconhecidos.
- Sempre verifique o endereço de e-mail do remetente e comunique qualquer e-mail suspeito ao setor de TI.

Plano de Resposta a Incidentes

- Saiba como proceder em caso de violação de dados ou incidente de segurança. Informe-se sobre o plano de ação e quem deve ser contactado em emergências.

Atualização e Manutenção de Softwares

Mantenha Seus Sistemas Atualizados

- Certifique-se de que todos os sistemas e softwares da ONG estejam com as atualizações mais recentes, pois elas corrigem falhas de segurança conhecidas.
- Evite usar softwares piratas ou de fontes desconhecidas, pois eles podem conter malwares.

Use Antivírus e Firewall

- Sempre utilize um antivírus confiável e mantenha o firewall ativado para proteger os sistemas contra ameaças externas.

Educação e Treinamento

Participe dos Treinamentos de Segurança

- Todos os colaboradores e voluntários devem participar de treinamentos regulares para entender a importância de seguir essas boas práticas e aprender a agir em casos de incidente.

Pergunte Sempre que Estiver em Dúvida

- Em caso de dúvidas sobre segurança digital ou manuseio de dados, entre em contato com o responsável pela segurança da ONG. Melhor perguntar do que arriscar!

Conformidade com a LGPD
(Lei Geral de Proteção de Dados)

Proteger Dados Pessoais é Fundamental

- Manuseie os dados pessoais dos adotantes e voluntários com cuidado, garantindo o cumprimento da LGPD. Lembre-se de que esses dados devem ser coletados e usados com propósito claro e informado.

Conclusão

Seguir essas boas práticas ajudará a proteger nossa ONG, nossos adotantes e os animais. Contamos com a sua colaboração para manter um ambiente seguro para todos!

Esta cartilha pode ser distribuída em formato digital (PDF) ou impresso, e é recomendável revisá-la periodicamente para acompanhar mudanças em políticas de segurança ou tecnologias.