

TRILHA DE APRENDIZAGEM

LGPD

Fundamentos e boas
práticas de Proteção
de Dados Pessoais

CARTILHA DE BOAS PRÁTICAS

SEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS



Ficha Técnica

TRIBUNAL DE CONTAS DO ESTADO DE MINAS GERAIS

PRESIDENTE

Conselheiro Gilberto Pinto Monteiro Diniz

VICE-PRESIDENTE

Conselheiro Durval Ângelo Andrade

CORREGEDOR

Conselheiro Wanderley Geraldo de Ávila

OUVIDOR

Conselheiro Cláudio Couto Terrão

CONSELHEIROS

Agostinho Célio Andrade Patrus

José Alves Viana

Mauri José Torres Duarte

CONSELHEIROS SUBSTITUTOS

Licurgo Joseph Mourão de Oliveira

Hamilton Antônio Coelho

Adonias Fernandes Monteiro

Telmo de Moura Passareli

ESCOLA DE CONTAS E CAPACITAÇÃO PROFESSOR PEDRO ALEIXO

DIRETORA

Naila Garcia Mourthé

COORDENADORA DE PÓS-GRADUAÇÃO

Luciana Moraes Raso Sardinha Pinto

COORDENADORA DE CAPACITAÇÃO

Renê Lopes Lage

COORDENADORA DE BIBLIOTECA

E GESTÃO DA INFORMAÇÃO

Ana Carolina Ferreira

SECRETÁRIA ACADÊMICA

Soraya Nogueira Zordan

NÚCLEO DE EDUCAÇÃO A DISTÂNCIA

DESIGNER EDUCACIONAL

Débora Cristina Cordeiro Campos Leal

Juliane Maria de Lima Borges

DESIGNER GRÁFICO

Tamires Rodrigues de Araújo

PRODUTOR AUDIOVISUAL

Christiano Rodrigues Perdigão

REVISORES

Dionne Emília Simões do Lago Gonçalves

Jésus Araújo Vieira

WEB DESIGNER

Gabriel Augusto Duarte

CONTEUDISTA

Luiza Amâncio Ferreira Duarte



Sumário

[Apresentação | 04](#)

[Cuidado com senhas | 05](#)

[Proteja seus dados e realize backup – Impeça que as ameaças cheguem | 09](#)

[Fique atento ao seu banco via Internet | 10](#)

[Códigos maliciosos | 12](#)

[Comércio eletrônico | 13](#)

[Cuidados com computadores | 15](#)

[Cuidados com celular | 18](#)

[Proteja sua privacidade | 19](#)

[Proteção de Dados, como se prevenir? | 20](#)

[Dê limite a suas redes de acesso | 21](#)

[Torne suas redes sociais mais seguras | 22](#)

[Cuidados no trabalho remoto | 26](#)

[Vazamento de dados | 27](#)

[Referências | 29](#)



Esta é uma cartilha interativa. Utilize os ícones para navegar.



Retornar ao Sumário



Saiba Mais!



Voltar



Fechar



Avançar



Apresentação



Bem-vindo à Dicas de Segurança e Proteção de Dados.

É pensando na segurança da informação e na proteção de dados pessoais que o Tribunal de Contas do Estado de Minas Gerais (TCEMG) implementa um conjunto de controles para salvaguardar e garantir a confidencialidades dos dados tratados nesta Casa.

Este material foi elaborado para contribuir com a Trilha de Aprendizagem: LGPD Descomplicada - Fundamentos e Boas Práticas de Proteção de Dados Pessoais e foi desenvolvido a partir dos **Fascículos com temas específicos de Segurança da Informação** do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), e das **Cartilhas do Usuário sobre Segurança da Informação e Recomendações para o Uso Consciente da Internet**, ambas disponibilizadas pelo TCEMG para orientar seus colaboradores nos cuidados à proteção de dados.

Seguindo as orientações deste material, do Núcleo de Proteção de Dados e da Diretoria de Tecnologia de Informação do Tribunal ou da instituição em que você atua, a tendência é aumentar a segurança e a proteção dos dados em suas práticas, mantendo suas atividades mais seguras, além de aumentar seus conhecimentos em Segurança e Proteção de Dados.

Então, se ligue nas dicas e boa leitura!





Cuidados com senhas



Escolha senhas fortes e diferentes para várias contas, isso dificulta o acesso de terceiros.

- Uma senha forte deve ter, pelo menos, oito caracteres (letras, números e símbolos), e não se esqueça de criar uma senha fácil de lembrar e que não dificulte sua digitação.
- Evite seu nome, sobrenome de filhos, pets, placas de veículos, telefones, datas ou qualquer outro dado que pode ser facilmente localizado em redes sociais e que o identifique.



- Utilize um poema ou uma música que goste, que seja fácil de memorizar e extraia a primeira, a segunda ou a última letra de cada palavra; caso a senha exija caracteres especiais e números, você pode completar a sequência. **Ex.:** “Tudo vale a pena quando a alma não é pequena.” Fernando Pessoa – senha: **TePuAnP**
- Não armazene senhas no seu navegador (*browser*).



- Não marque a opção “**salvar o número de cartão de crédito em compras futuras**”.



A troca de senha com frequência é uma medida de segurança; fique atento à periodicidade definida pela sua instituição.



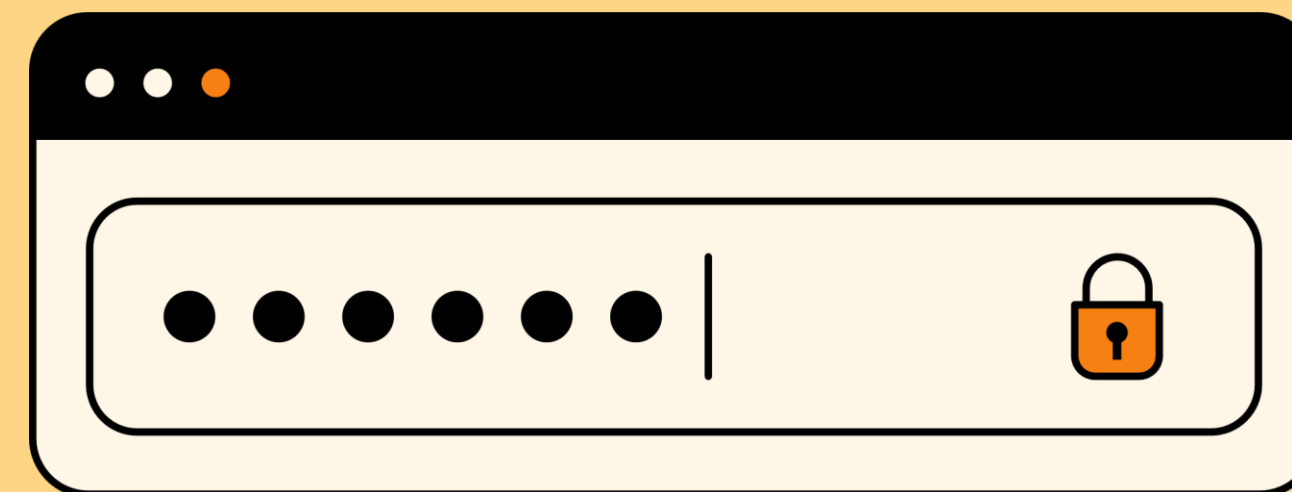
- Utilize autenticação com segunda etapa sempre com aplicativos autenticadores, como *Google Authenticator* ou *Microsoft Authenticator*. Autenticação via SMS apresenta riscos.



- Não divulgue seus hábitos no trabalho e rotinas familiares, como localização.
- Se necessário armazenar senha, utilize um cofre criptografado.



Não instale softwares suspeitos, inclusive plug-ins que alterem ou tragam ação a um software.



- Defina senhas diferentes para contas e aplicações distintas. Pode mesclar uma parte da senha igual com partes diferentes para cada tipo de conta, facilitando a memorização. Como exemplo, a técnica utilizada anteriormente; a parte igual da senha pode ser o código gerado com um poema ou música que goste.





- Utilize autenticação em aplicativos Authenticator Autenticação v

- Não divulgue senhas com familiares, com
- Se necessário, use senhas criptografadas.

- Evite salvar senhas de contas importantes na web e não permita o login automático de contas importantes.
- Não compartilhe senhas e códigos de verificação.
- Cadastre um e-mail de recuperação para sua senha.
- Evite o envio e/ou compartilhamento de recursos protegidos por leis de propriedade intelectual.
- Bloqueie telas de dispositivos antes de sair de perto deles.
- No *smartphone*, não utilize pontos e desenhos muito simples e configure para o rastro ficar invisível.

Não
inclus
tra





- Escolha dicas de segurança vagas e claras, isso dificulta a descoberta e o ajudará a lembrar.
- Fique sempre atento aos avisos e alertas de acesso à sua conta.
- Leia as informações de onde está indicando o último acesso e, caso verifique algo suspeito, acesse seu e-mail diretamente sem clicar em *links*.
- Evite digitar sua senha em computador de terceiros. Caso precise digitar, fique atento se a conexão é segura, se há alguém ou câmera observando-o no local.
- Cadastre *e-mail* e números de telefone alternativos; mantenha-os sempre atualizados caso precise receber códigos de verificação.



Não
inclus
tra





Proteja seus dados e realize *backup*— Impeça que as ameaças cheguem



- Faça mais de um *backup* de seus arquivos e não os armazene no mesmo local.
- Mantenha suas informações em mídias ou partições criptografadas. Dessa forma, se um equipamento for perdido ou roubado em uma viagem, ou enviado para manutenção, seus arquivos estarão protegidos.



Evite armazenar fotos e dados que exponham a privacidade.

- Ao utilizar criptografia, tenha certeza de salvar em local seguro a chave criptográfica, pois se esquecer a senha de acesso ou perder a chave, você não terá mais acesso aos seus dados.
- Não copie dados desnecessários, faça *backup* do que for necessário e elimine o restante.
- As mídias devem ser guardadas em local seguro e a restauração do backup deve ser simulada periodicamente.
- Antes de realizar a transferência dos arquivos, verifique se possui espaço disponível.
- Realize um backup manual, isso garante uma cópia atualizada.
- Mantenha um *backup off-line* para recuperação em casos em que sistemas podem ser completamente comprometidos.





Fique atento ao seu banco via *Internet*



- O número do seu telefone é um identificador para o app do seu banco. Quando trocar o número de telefone ou de chip, confirme a alteração com sua instituição financeira e não se esqueça de habilitar o backup do celular assim que trocar de aparelho; ele restaura seus dados no atual.
- Utilize mais de uma opção para realizar seu backup. Habilite para realizar de forma automática e sincronize com outro equipamento.



- Não salve senhas em blocos de notas, contatos ou navegador, não envie senhas por mensagens ou e-mail e não tire fotos.



- Faça busca em seu celular com a palavra senha. Você vai se surpreender.



- Fique atento ao acessar sua loja de aplicativos. Existem aplicativos muito similares aos oficiais; certifique-se de que o nome do fabricante e do desenvolvedor estejam corretos.



Atenção a páginas e perfis falsos!
Cheque no site da instituição os
canais oficiais.





- Instituições financeiras não entram em contato com pessoas pedindo senhas, códigos de verificação, *tokens*, códigos QR, dados de cartão ou outras informações. Para evitar golpes, encerre a comunicação e, em caso de dúvida, entre em contato com os canais oficiais.
- Para pagamentos não presenciais, utilize cartões virtuais, reduza o limite do cartão, se possível, e, periodicamente realize a troca para evitar fraudes.
- Em caso de pagamento por aproximação, limite junto ao seu banco os valores de pagamentos e sempre confira antes os dados no visor da máquina de cartão e depois que emitir o recibo.



Atenção ao bluetooth, pois costuma vir ativo de fábrica.



- Compartilhe dados apenas com instituições autorizadas.
- Não divulgue suas informações pessoais ou financeiras, principalmente em redes sociais.
- Crie um *e-mail* exclusivo para cadastro em instituições financeiras e não o deixe logado em aplicativos ou navegador de celular.
- Ative a localização remota do aparelho e anote o IMEI do celular em local seguro.
- Verifique periodicamente o extrato bancário dos seus cartões de crédito físicos e virtuais.

Códigos maliciosos



Mantenha seu antivírus atualizado; ative a atualização automática.

- Não clique em todos os links que recebe por *e-mail*, redes sociais, SMS ou aplicativos de mensagens.



- Desconfie sempre de arquivos anexos, cheque o arquivo com antivírus e, se estiver em dúvida, não abra.



- Verifique o remetente do *e-mail* e também os padrões de arquivos; a exemplo de um processo judicial, há padrões de números e das varas correspondentes.
- Não compartilhe notícias que podem ser falsas, correntes e outras mensagens que possam conter códigos maliciosos.





Comércio eletrônico

***
Verifique e valide no *site* da Receita Federal os dados cadastrais da empresa.

- Digite o endereço da loja diretamente do navegador da web, não utilize sites de buscas. Não entre em sites com links editados com bitly ou QR code, pois o endereço real do apontamento pode ser diferente do desejado.
- Pesquise na Internet se a loja possui reclamações; a opinião de clientes é importante.



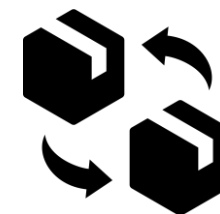
- Verifique as políticas da loja, como:



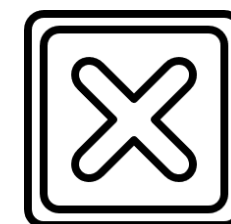
política de privacidade



garantia



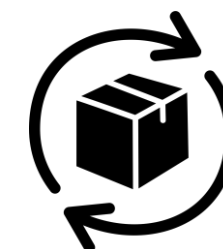
troca



cancelamento



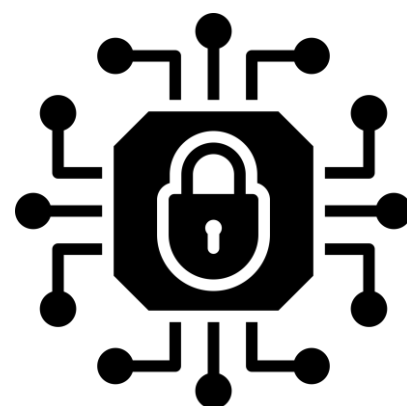
arrependimento



devolução



- Sempre desconfie de produtos muito baratos; faça pesquisas sobre o produto para ver outros valores.
- Quando enviar dados pessoais por *e-mail*, certifique-se de criptografar a mensagem; essa opção você configura ao compor a mensagem.



- Guarde as informações da compra, qualquer documento é válido.



- O endereço do site seguro sempre inicia com **https://** e, devido ao “**certificado digital *Secure Sockets Layer (SSL)***” (falaremos mais dele nesta cartilha), o desenho do cadeado é mostrado na barra de endereço. *Sites* com tal desenho possuem certificado em uso e informações da conexão.



- Se o seu produto não for entregue em casa ou em outro local, marque a entrega em lugar público.



Só libere o código de rastreamento enviado pelos Correios para o entregador quando o produto estiver em suas mãos.





Cuidados com Computadores

- Atualize os programas com as versões mais recentes.
- Se optar por utilizar um programa proprietário no seu computador particular, mas não possa adquirir a licença, procure por alternativas gratuitas ou mais baratas, e que possuam funcionalidades semelhantes às desejadas.
- Cuidado quando instalar aplicativos desenvolvidos por terceiros, verifique as permissões e cuidados antes de permitir que acessem seus dados pessoais.



- Instale um *firewall* pessoal, ele cria uma barreira de defesa, bloqueando o tráfego de dados indesejados.
- Quando utilizar seu computador em locais públicos, mantenha-o bloqueado com travas para evitar que seja aberto ou furtado.
- Configure seu computador para solicitar senha na tela inicial e utilize criptografia de disco; caso haja algum risco, isso dificulta o acesso a seus dados.
- Quando utilizar computadores de terceiros, utilize a navegação anônima e não efetue transações bancárias ou comerciais.





Cuidados com Computadores

- Atualize os programas com frequência.
- Se optar por utilizar um programa em um computador particular, mas não em um público, procure por alternativas seguras, baratas, e que possuam funções de segurança às desejadas.
- Cuidado quando instalar aplicativos de terceiros, verifique as permissões antes de permitir que acessem seus dados.
- Não utilize opções como **“Lembre-se de mim”** e **“continuar conectado”**. Não permita que suas senhas sejam memorizadas no navegador web.
- Limpe os dados pessoais salvos no navegador e certifique-se de que saiu (*logout*) de todas as suas contas conectadas.
- Mantenha seu computador sincronizado com a data e a hora conforme o **Protocolo de Tempo para Redes** (NTP) <https://www.ntp.br/>
- Instale um firewall pessoal, ele cria uma barreira de segurança contra o tráfego de dados indesejados.
- Não utilize computadores em locais públicos, especialmente aqueles sem travas para evitar que outros tenham acesso a seus dados.
- Quando utilizar computadores de terceiros, utilize a opção de acesso limitado para solicitar senha na tela de bloqueio; caso haja acesso a seus dados, não efetue transações.





Cuidados com Computadores

- Atualize os programas com frequência.
- Se optar por utilizar um programa em seu computador particular, mas não em um computador corporativo, procure por alternativas baratas, e que possam funcionar em computadores antigos.
- Cuidado quando instalar aplicativos de terceiros, verifique as permissões antes de permitir que acessem seus dados.
- Quando compartilhar arquivos de seu computador, estabeleça senhas e permissões e compartilhe pelo tempo mínimo necessário.
- **Cuidado ao enviar seu computador para manutenção!** Assegure-se de que a empresa possui boas referências e não permita a instalação de programas não originais. Se possível, faça o *backup* de seus dados antes.

• Instale um firewall pessoal, ele cria uma barreira de tráfego de dados indesejados.



• Não use seu computador em locais públicos, e sempre bloqueie com travas para evitar que

• Não deixe seu computador sem senha por muito tempo, ou para solicitar senha na inicialização do disco; caso haja acesso a seus dados.

• Quando usar computadores de terceiros, utilize a internet com cautela, não efetue transações





Cuidados com celular



Reduza limites de transferências bancárias: DOC, PIX e TED.

- Desabilite funções em tela bloqueada, como: mensagens e acessos rápidos (atalhos) a configurações.
- Configure a opção de fixar a tela em uma aplicação; no *Android* é chamado “**Fixação de Tela**” e, no iOS, “**Acesso Guiado**”.
- Instale um *app* que filtra ligações indesejadas e spam, como o “**Telefone do Google**” para *Android* ou *iOS*.



- Proteja seu chip SIM com uma senha, altere o PIN padrão e não se esqueça de anotar o IMEI em local seguro. IMEI é o código identificador do aparelho de celular que bloqueia o aparelho em caso de roubo (**digitando *#06# diretamente no aparelho**). A operadora de celular pode desativar o *chip* SIM e bloquear o IMEI.
- Ative a localização remota do aparelho para apagar informações remotamente, com o recurso chamado “**Encontre Meu Dispositivo**” no Android e “**Buscar iPhone**” no iOS.
- Ative e acesse o serviço de localização remota do seu aparelho e apague remotamente todos os dados do dispositivo em caso de roubo: serviço <https://android.com/find/> para *Android* e <https://icloud.com/find/> para *iOS*.



Proteja sua Privacidade



- Fique atento a imagens anexadas ao *e-mail*, configure seu programa leitor de e-mails para não abrir imagens que não estejam na própria mensagem; se a imagem for acessada, pode confirmar que o *e-mail* foi lido.
- Seja cuidadoso, quando aceitar cookies de um site, configure-os para que sejam apagados assim que o navegador fechar e, também, configure para que os cookies de terceiros não sejam aceitos.
- Esteja atento quando divulgar informações em sua página web ou em redes sociais, pois podem ser usadas em golpes de engenharia social para obter informações sobre você.



- Não disponibilize seus dados pessoais, mesmo que pareça o menos importante; sempre pare e questione: qual finalidade terá este compartilhamento, e, se tiver a menor desconfiança, investigue.
- Quando enviar seu currículo, seja por meio físico ou pela web, limite a quantidade de informações e só forneça seus dados se tiver a segurança da empresa. Se possível, cadastre-se no Currículo Lattes e compartilhe o *link*.
- Atente-se a ligações telefônicas e *e-mails* que solicitam suas informações, pois podem-se passar por alguma empresa, familiar ou amigo. Essa prática é conhecida como engenharia social, nela, os criminosos virtuais induzem usuários desavisados a enviar dados confidenciais, comprometendo seus dispositivos e informações.
- Verifique os “**termos e condições de uso**” dos sistemas e *app*, eles costumam informar o que são feitos com os dados coletados.



Proteção de Dados, como se prevenir?



Seja muito cuidadoso com equipamentos de terceiros.

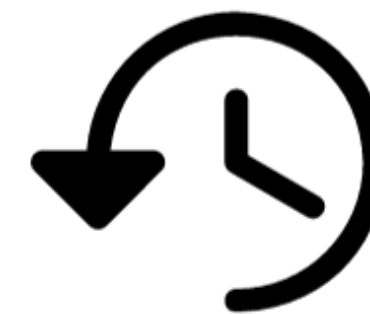
- Quando se desfizer de equipamentos e mídias, elimine seus dados com programa destruidor de arquivos ou de sanitização de dados (apagar dados), tornando impossível sua recuperação.



- Quando aceitar contatos em suas redes sociais, analise o perfil do solicitante.



- Limpe frequentemente o histórico de navegação.



- Informe-se sobre a **Lei Geral de Proteção de Dados Pessoais**, ela lhe dá o direito de saber como seus dados são tratados, quais são coletados e porque eles são compartilhados, ou seja, qual sua finalidade.



- As organizações públicas e privadas têm a obrigação de fornecer informações claras para que você compreenda termos de consentimento e bases legais que apoiam o tratamento de seus dados.



Dê limite a suas redes de acesso



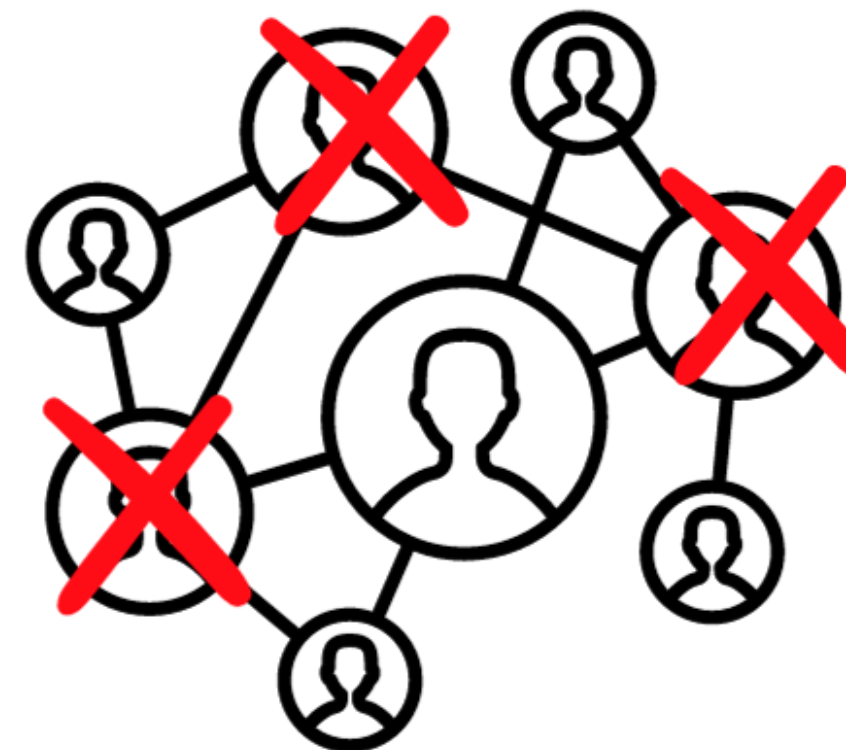
Desligue o equipamento de rede quando não estiver utilizando.

- Ative as interfaces de *Wi-Fi* e *bluetooth* apenas quando for utilizá-las, desative a função de compartilhamento e nunca se conecte a redes *Wi-Fi* públicas.



- Evite usar, nas características do dispositivo, dados que o identifiquem.

- Limite o compartilhamento e o controle de quem pode ver suas informações no perfil das suas redes sociais, como exemplo: **número de telefone, local onde reside e outros dados.**



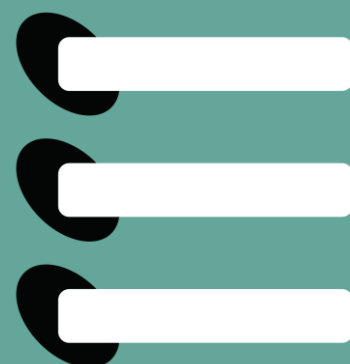
Evite usar, nas características do dispositivo, dados que o identifiquem.



Torne suas redes sociais mais seguras



- Bloqueie contatos e perfis que tiverem incomodando ou que desconheça.
- Avise seus contatos caso detecte contas falsas passando-se por você.
- Crie listas personalizadas de contatos para selecionar quem pode ver suas informações pessoais e de postagens, isso minimiza sua exposição.



- Configure suas redes sociais para que possa analisar postagens em que você for marcado.
- Respeite a privacidade de terceiros, algumas pessoas não se sentem à vontade por ter sua privacidade exposta.
- Peça autorização antes de postar imagens em que outras pessoas apareçam e muito cuidado com a exposição de menores.
- Cuide de sua imagem profissional:





Torne suas redes sociais mais seguras

- Ao postar suas informações, analise-as antes.
- Separe seus contatos em redes ou listas específicas.
- Respeite as políticas da sua empresa ou escola, incluindo o uso de redes sociais e compartilhamento de informações.



Torne suas redes sociais mais seguras

- Cuidado quando curtir ou compartilhar apoio a determinados conteúdos, pois esse posicionamento diz muito sobre você. Caso o conteúdo seja indevido (violência, discriminação, calúnia e difamação) pode gerar consequências, inclusive judiciais.
- Não repasse informações profissionais, principalmente em redes sociais.



Torne suas redes sociais mais seguras

- Configure suas redes sociais para que possa analisar postagens em que você for marcado.
- Respeite a privacidade de terceiros, algumas pessoas não se sentem à vontade por ter sua privacidade exposta.
- Peça autorização antes de postar imagens em que outras pessoas apareçam e muito cuidado com a exposição de menores.

Cuidados no trabalho remoto



Nunca compartilhe credenciais de acesso.

- Procure saber suas responsabilidades e consulte a política da instituição.
- Não tente burlar mecanismos de segurança para facilitar acessos.
- Cuidado ao instalar aplicativos. Se o computador é institucional, o setor responsável pela tecnologia bloqueia a ação. Caso seja equipamento particular, deve aplicar uma política de **BYOD** com assinatura de termo de responsabilização.



- Não permita que familiares utilizem o computador.
- Não imprima, copie ou transfira documentos institucionais para trabalhar remotamente, isso pode levar a vazamentos e ter implicações legais, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD).
- Evite fazer chamadas de vídeos/áudio em locais públicos.
- Desligue dispositivos ativados por voz antes das reuniões.
- Se por algum motivo você clicou em algum *link* de e-mail e depois descobriu ou desconfiou que é *phishing*, avise a equipe de Segurança da Informação imediatamente.
- E, se receber algum e-mail suspeito, antes de clicar avise a equipe de Segurança da Informação, ela irá ajudá-lo.



Vazamento de dados



- Caso receba alguma notificação de vazamentos de seus dados, altere imediatamente suas senhas e procure saber quais foram esses dados, isso o ajudará a saber quais medidas devem ser tomadas. Registre um boletim de ocorrência e contate as instituições envolvidas (controlador e operadores de dados) e, se sua solicitação não for atendida ou não souber qual instituição está envolvida, denuncie no site da **Autoridade Nacional de Proteção de Dados** (ANPD - <https://www.gov.br/anpd/>)



- Se confirmar que sua conta foi invadida ou criaram um perfil falso em seu nome, informe a seus contatos para que não caiam em golpes. Denuncie o perfil falso e recupere o acesso à plataforma.



- Não compre lista de dados; essa prática incentiva vazamentos inclusive dos seus dados.





Atenção!



- Certifique-se que os ambientes digitais que você acessa e que seus dados são coletados possuem o **certificado digital Secure Sockets Layer (SSL)**. Olhe na barra de endereço do seu navegador se o *site* começa com **HTTPS** (versão mais segura) ao invés de HTTP, pois ele está protegido com o **certificado SSL**, documento eletrônico que serve como identidade virtual que confere a validade jurídica e aspectos de segurança nas transações digitais.
- Muito cuidado com as conversas de corredor, elevador e outros ambientes públicos. O conteúdo pode ser ouvido e repassado, trazendo prejuízos.
- Aquelas pessoas que identificarem que estão com acesso a sistemas, aplicativos e informações que não lhe dizem respeito, devem comunicar à área superior para solicitar a interrupção do acesso.
- **Lembre-se:** acesso à várias informações, traz muita responsabilidade. Tenha acesso somente ao que é necessário.





REFERÊNCIAS

- BRASIL. Fascículos: **Cartilhas de Segurança para Internet. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)**. Disponível em: <https://cartilha.cert.br/fasciculos/#autenticacao>. Acesso em: 8 de ago. 2023.
- TCEMG. **Cartilha. Recomendações para uso mais consciente e seguro da internet**. Diretoria de Tecnologia da Informação. Dezembro de 2016. Acesso em: 17 de ago. 2023.
- TCEMG. **Cartilha do Usuário. Segurança da informação**. Diretoria de Tecnologia da Informação. Janeiro de 2016. Acesso em: 15 de ago. 2023.

**Avenida Raja Gabaglia, nº 1.305
Luxemburgo Belo Horizonte - MG
Edifício Anexo 1º Andar.
(31) 3348-2698**

Imagens e ícones disponibilizadas por Canva.

Siga-nos nas redes sociais:

