

# Trabalho Remoto



Produção:

**cert.br nic.br cgi.br**

# ***TRABALHO SEGURO EM QUALQUER LUGAR***

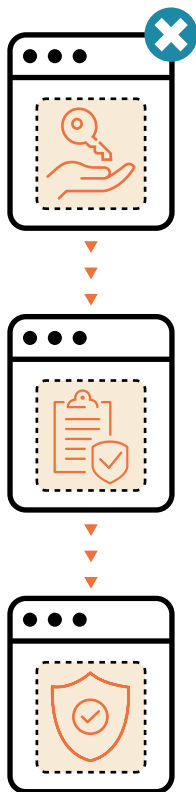
**U** aumento do trabalho remoto atraiu a atenção dos atacantes para o ambiente do usuário, com o objetivo de ganhar acesso a redes e sistemas corporativos. Uma conta invadida ou um computador infectado podem ser a porta de entrada para ataques contra a empresa onde você trabalha, causando prejuízos a todos, inclusive a você.

Veja aqui dicas de como trabalhar remotamente de forma segura.

# RESPEITE AS REGRAS DA EMPRESA

**R**espeitar as regras da empresa, especialmente quanto ao uso de recursos corporativos, requisitos de proteção de dados e procedimentos de segurança para trabalho remoto, evita incidentes e prejuízos. Lembre-se que o prejuízo também pode ser seu.

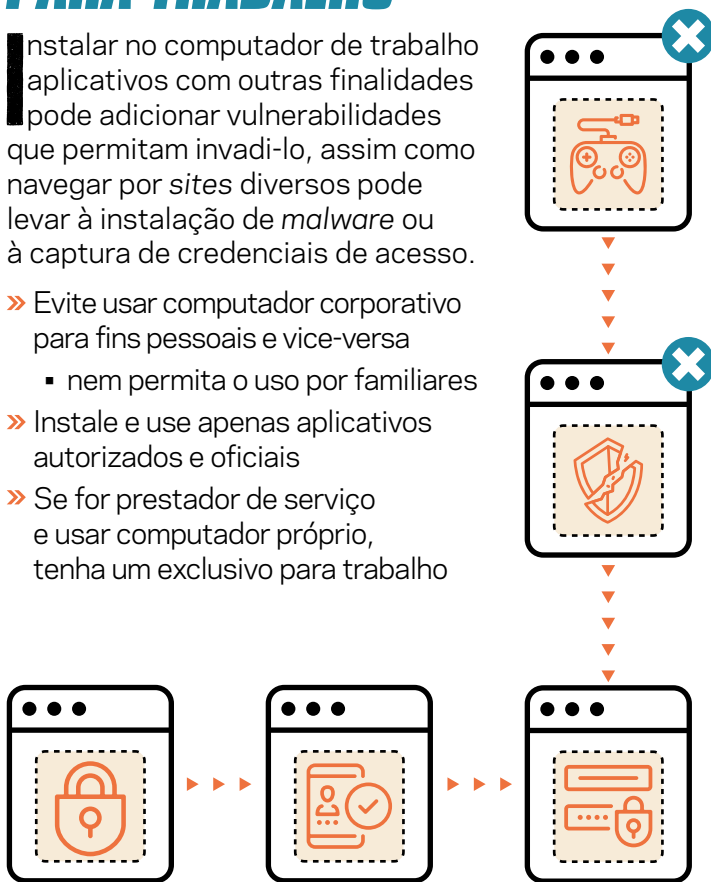
- » Busque saber o que é esperado e as responsabilidades associadas
  - se não houver uma política definida, consulte seu superior
- » Não tente burlar mecanismos de segurança para facilitar acessos
  - se algum controle for muito rígido, dificultando ou impedindo sua atividade, converse com seu superior
  - nunca compartilhe credenciais de acesso



# USE O COMPUTADOR DE TRABALHO SOMENTE PARA TRABALHO

Instalar no computador de trabalho aplicativos com outras finalidades pode adicionar vulnerabilidades que permitam invadi-lo, assim como navegar por sites diversos pode levar à instalação de *malware* ou à captura de credenciais de acesso.

- » Evite usar computador corporativo para fins pessoais e vice-versa
  - nem permita o uso por familiares
- » Instale e use apenas aplicativos autorizados e oficiais
- » Se for prestador de serviço e usar computador próprio, tenha um exclusivo para trabalho





## ***MANTENHA SISTEMAS E APLICATIVOS ATUALIZADOS***

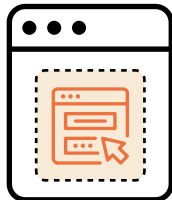
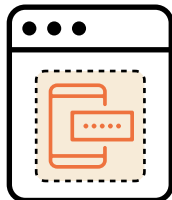
**S**istemas e aplicativos podem ter vulnerabilidades passíveis de serem exploradas para invadir o dispositivo e, a partir dele, acessar redes e sistemas aos quais se conecta. Aplicar atualizações evita que seus dispositivos sejam comprometidos e usados como parte de ataques.

- » Instale atualizações regularmente
  - ative a atualização automática, sempre que possível

# USE AUTENTICAÇÃO FORTE

**A** autenticação é o que protege o acesso às contas, mas usar apenas senhas pode não ser suficiente pois elas podem ser adivinhadas, obtidas em vazamentos de dados e capturadas por meio de *phishing* ou *malware*.

- » Use senhas fortes, difíceis de adivinhar
- » Não repita senhas
  - uma senha vazada pode levar à invasão de outras contas
- » Use verificação em duas etapas, sempre que possível
  - contas muito visadas, como VPN, *webmail* e serviços em nuvem não devem ficar sem!
  - se sua organização ainda não usa, sugira!

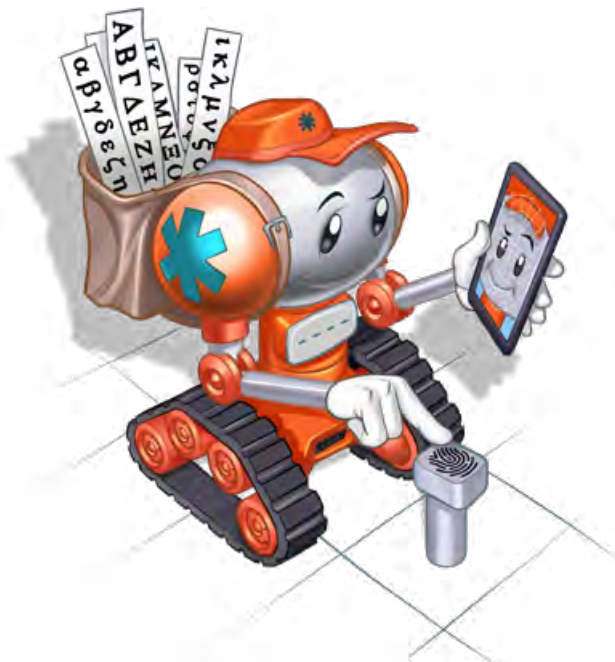


Veja mais dicas no fascículo "Autenticação".

# GUARDE AS SENHAS DE FORMA SEGURA

**E**m seu trabalho você pode ter inúmeras senhas que, se descobertas por um atacante, poderão ser usadas para invadir redes e sistemas corporativos.

- » Adote um método de gerenciamento. Você pode:
  - usar aplicativos gerenciadores de senhas
  - gravá-las em um arquivo criptografado
- » Não salve senhas no navegador



# UTILIZE MECANISMOS DE PROTEÇÃO NO COMPUTADOR



**F**erramentas como antivírus e *firewall* pessoal são mecanismos importantes para proteger seus computadores contra *malware* e ataques vindos da Internet, ao passo que a criptografia de disco protege contra acesso indevido aos dados em caso de perda ou furto.

- » Instale um antivírus (*antimalware*) e mantenha-o atualizado
- » Assegure-se de ter um *firewall* pessoal instalado e ativo
- » Ative a criptografia de disco



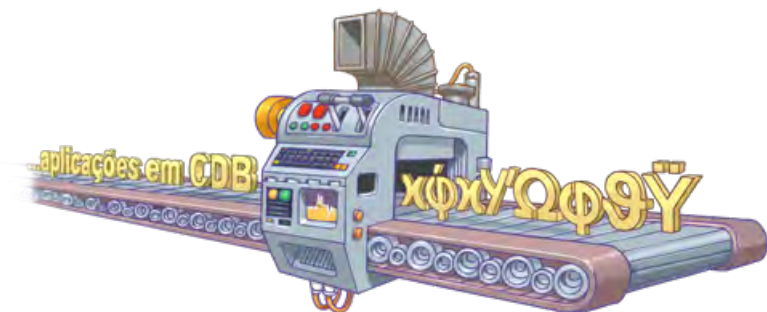
Veja mais dicas no fascículo "Computadores".



# USE CONEXÃO SEGURA PARA ACESSAR OS SISTEMAS CORPORATIVOS

**S**ua conexão remota aos sistemas corporativos pode ser interceptada para obter informações confidenciais, como credenciais de acesso e dados de clientes. A criptografia protege as informações enquanto trafegam pela rede e garante o acesso ao destino correto.

- » Utilize a VPN da empresa
- » Use conexão segura para acessar sistemas conectados diretamente à Internet (ex: https para *webmail*)





## ***TRATE DADOS SENSÍVEIS COM CUIDADOS EXTRAS***

**C**opiar e transportar dados de sistemas internos para trabalhar remotamente, em especial aqueles relacionados a dados pessoais, pode levar a vazamentos e ter implicações legais, inclusive com multa, conforme a Lei Geral de Proteção de Dados (LGPD).

- » Use apenas mecanismos aprovados pela empresa para transferência de informações
  - não use, sem autorização, serviços de compartilhamento em nuvem, dispositivos ou e-mails pessoais
- » Ative criptografia em mídias externas, para evitar acesso indevido em caso de perda ou furto
- » Copie apenas os dados estritamente necessários
  - apague-os assim que terminar o uso

# USE CANAIS DE COMUNICAÇÃO OFICIAIS PARA ASSUNTOS DE TRABALHO

Usar contas pessoais de e-mails e aplicativos de mensagens para tratar de assuntos corporativos pode levar a vazamentos de informações estratégicas e causar perda de competitividade ou de reputação.

- » Use apenas aplicativos autorizados e contas corporativas para assuntos de trabalho



# DESCONFIE DE LINKS E ANEXOS EM E-MAILS

**E**-mails com *links* ou anexos maliciosos são bastante usados por atacantes para obter informações de *login* ou instalar *malware*. Podem usar temas que despertam a curiosidade ou serem direcionados para convencer os usuários.

- » Não clique em *links* ou abra arquivos anexos se:
  - não tiver relação direta com seu trabalho
  - contiver ameaças ou ofertas vantajosas demais
  - fugir dos procedimentos usuais da empresa
- » Na dúvida, busque confirmar a veracidade
  - contate o autor via outro canal de comunicação, se for conhecido
  - peça ajuda da área de segurança da empresa





## FAÇA BACKUPS

**O**s dados armazenados em seu computador podem ser perdidos por falhas de *hardware* ou de sistema, por perda ou furto do aparelho ou pela ação de *malware*, como *ransomware*. Ter cópias permite recuperá-los, reduzindo os transtornos.

- » Faça cópias periódicas de seus dados
  - programe seus *backups* para serem feitos automaticamente, sempre que possível



Veja mais dicas no fascículo "Backup".



## DEIXE SUA REDE DOMÉSTICA MAIS SEGURA

**R**edes domésticas não tem os mesmos recursos de segurança que uma rede corporativa e precisam de cuidados. Além disso, vulnerabilidades no roteador podem levar à instalação de *malware* e à alteração de configuração para desvio de tráfego.

- » Proteja o *modem*/roteador:
  - mantenha o *firmware* atualizado
  - troque a senha de administração, se possível
  - ative o *firewall* do roteador, quando disponível
- » Na rede Wi-Fi, ative criptografia forte e troque as senhas padrão
- » Idealmente, tenha redes separadas para trabalho e uso doméstico

# FIQUE ATENTO AO AMBIENTE AO SEU REDOR

**S** seja ao digitar credenciais de acesso ou fazer videoconferências, alguém pode estar observando. Para não expor informações sensíveis é preciso analisar o entorno e ficar atento a curiosos, câmeras de vídeo e dispositivos ativados por voz, como assistentes pessoais.

- » Evite fazer chamadas de áudio/vídeo em locais públicos, como cafés
- » Antes de digitar credenciais de acesso, certifique-se que não está sendo observado ou filmado
- » Desligue dispositivos ativados por voz antes de fazer reuniões





## COMUNIQUE À EMPRESA SUSPEITAS DE PROBLEMAS

**C**licou no *link* de um *e-mail* e depois descobriu que era *phishing*? O computador está “estranho”? Notou um acesso indevido à sua conta? Em situações assim é melhor avisar a empresa. O quanto antes um incidente for detectado e contido, menores serão os transtornos e prejuízos.

» Saiba quais são os canais oficiais para:

- acionar o suporte técnico
- notificar potenciais incidentes de segurança





## SAIBA MAIS

- » Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **<https://cartilha.cert.br/>**
- » Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **<https://internetsegura.br/>**

## cert.br

O CERT.br (<https://cert.br/>) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

## nic.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (<https://nic.br/>) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

## cgi.br

O Comitê Gestor da Internet no Brasil (<https://cgi.br/>), responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.