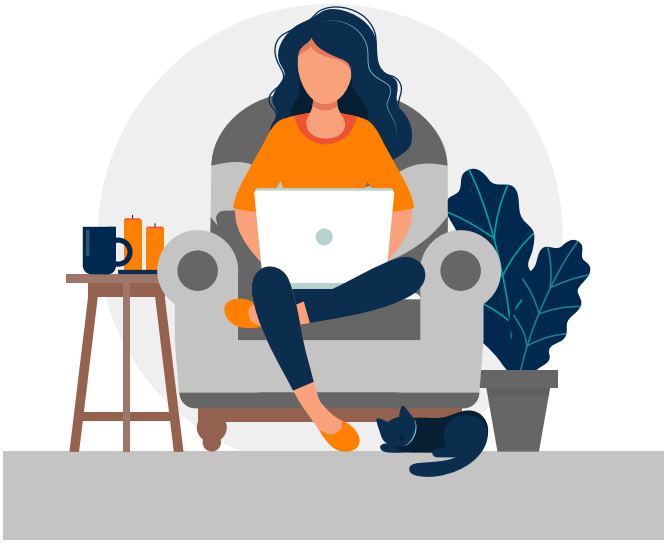
Trabalho remoto, como trabalhar digitalmente!

ESCOLA SUPERIOR DE REDES · RNP · gov.br · MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS · GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Esta é uma iniciativa do Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital.

Sumário

Boas-vindas



Com o trabalho remoto se tornando cada vez mais comum nas organizações atualmente, é importante adotar boas práticas para garantir eficácia, produtividade e segurança ao trabalhar remotamente.

Por este motivo, elaboramos este material que servirá com um **Guia de Boas Práticas para o Trabalho Remoto,** para garantir a segurança da informação em seu dia a dia.

Este guia oferece diretrizes para otimizar o trabalho remoto, de modo a superar desafios e maximizar benefícios. Ele faz parte do curso **Segurança da Informação para todos**, uma iniciativa do Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital (CEPS GOV.BR), desenvolvida pela Escola Superior de Redes (ESR), em parceria com a Escola Nacional de Administração Pública (ENAP).

Seguindo estas orientações, você estará mais preparado para alcançar um desempenho ainda melhor no seu trabalho, independentemente da sua localização.

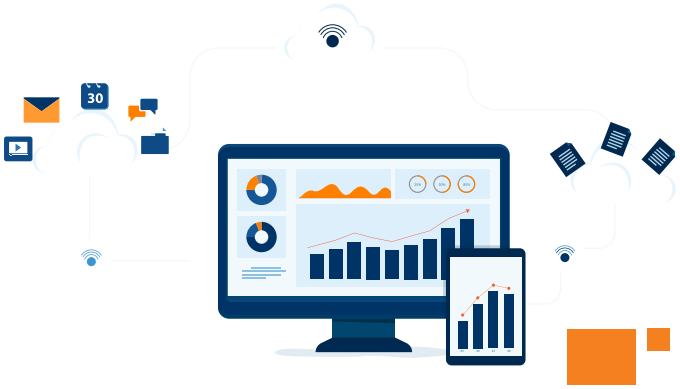
Vamos começar?

Acompanhe o conteúdo a seguir

Do pijama ao terno, tudo em um só lugar!

O avanço da tecnologia e a evolução das mentalidades organizacionais permitiram que cada vez mais profissionais realizassem suas atividades de onde quer que estivessem, e uma delas foi executar nossas demandas de trabalho no conforto do nosso lar.

Esse novo paradigma, que pode ser resumido como “do pijama ao terno”, traz consigo uma série de benefícios e desafios que merecem ser explorados.



A casa é minha, mas as informações, não!

Você já parou para pensar que, mesmo estando em casa, as informações que pertencem à instituição podem estar em risco?

Pois é, a segurança dos dados, ao nos conectarmos de um dispositivo residencial para as demandas do trabalho, é uma preocupação que merece atenção especial.

“A casa é minha, mas as informações, não!”

Essa frase resume bem a importância de protegermos nossos dados pessoais e organizacionais, especialmente quando muitos de nós utilizamos nossos próprios dispositivos domésticos para acessar e compartilhar informações sensíveis do trabalho.

Acompanhe, no tópico a seguir, os exemplos de boas práticas sobre a segurança para o trabalho remoto.

Boas práticas de segurança para o trabalho remoto

Trabalhar remotamente pode trazer muitos benefícios, mas também apresenta desafios únicos em termos de segurança da informação. Aqui estão algumas medidas de segurança essenciais para proteger seus dados enquanto trabalha remotamente.

Saiba mais!

Na página do Governo Digital, neste link, você encontra o fascículo sobre trabalho remoto e outros temas para complementar seus estudos.

Respeite as regras da empresa

Respeitar as regras da organização, especialmente quanto ao uso de recursos corporativos, requisitos de proteção de dados e procedimentos de segurança para trabalho remoto, evita incidentes e prejuízos.

Respeite as regras da organização!
Lembre-se de que o prejuízo também pode ser seu.

Checklist

- [x] Busque saber o que é esperado e quais as responsabilidades associadas. Caso não tenha uma política definida, consulte seu superior.
- [x] Não tente burlar mecanismos de segurança para facilitar acessos. Se algum controle for muito rígido, dificultando ou impedindo sua atividade, converse com seu superior.
- [x] 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 *malwares* ou à captura de credenciais de acesso.

Checklist

- [x] Evite usar computador corporativo para fins pessoais e vice-versa. Além disso, não permita que familiares utilizem esse dispositivo.
- [x] Instale e use apenas aplicativos autorizados e oficiais.
- [x] Se for prestador de serviço e usar computador próprio, tenha uma máquina exclusiva para trabalho.
- [x] Caso tenha que utilizar sua máquina particular compartilhada, crie um usuário próprio para trabalhar no sistema operacional. De forma, a separar os dados e acessos da organização dos demais usuários particulares.

Mantenha sistemas e aplicativos atualizados

Sistemas 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.

Checklist

- [x] Instale atualizações regularmente. Ative a atualização automática sempre que possível.
- [x] Use somente sistemas operacionais e aplicativos originais.

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*.

Checklist

- [x] Use senhas fortes, difíceis de adivinhar.
- [x] Não repita senhas. Uma senha vazada pode levar à invasão de outras contas. Conte com o auxílio de cofres de senhas.
- [x] 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!

Guarde as senhas de forma segura

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

Checklist

- [x] Use um cofre de senha.
- [x] Não salve senhas no navegador.

Utilize mecanismos de proteção no computador

Ferramentas 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.

Checklist

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

Use conexão segura para acessar os sistemas corporativos

Sua 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.

Checklist

- [x] Utilize a VPN da organização.
- [x] Use conexão segura de *internet* para acessar sistemas conectados diretamente à *internet* (ex.: https para *webmail*).

Trate dados sensíveis com cuidados extras

Copiar 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).

Checklist

- [x] Use apenas mecanismos aprovados pela organização para transferência de informações. Não use sem autorização serviços de compartilhamento em nuvem, dispositivos ou *e-mails* pessoais.
- [x] Ative criptografia em mídias externas para evitar acesso indevido em caso de perda ou furto.
- [x] Copie apenas os dados estritamente necessários. Apague-os assim que terminar o uso.
- [x] Atenção especial para os dados pessoais tratados pela organização, observando os controles de proteção de dados e privacidade visando o atendimento à LGPD.

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.

Checklist

- ☑ 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.

Checklist

- ☑ Não clique em *links* ou abra arquivos anexos se não tiverem relação direta com seu trabalho. Cuidado com *e-mails* com ofertas vantajosas demais, tentativas de intimidações ou procedimentos que fogem muito dos usuais. Cuidado é golpe!
- ☑ Na dúvida, busque confirmar a veracidade. Contate o autor via outro canal de comunicação, se for conhecido, ou peça ajuda da área de segurança da organização.

Faça *backups*

Os 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 um *malware*, como *ransomware*.

Ter cópias dos dados permite recuperá-los reduzindo os transtornos.

Checklist

- [x] Faça cópias periódicas de seus dados. Programe seus *backups* para serem feitos automaticamente, sempre que possível.

Deixe sua rede doméstica mais segura

Redes domésticas não têm os mesmos recursos de segurança que uma rede corporativa e, por isso, precisam de cuidados.

Vulnerabilidades no roteador podem levar à instalação de *malware* e à alteração de configuração para desvio de tráfego.

Checklist

- [x] Proteja o modem/roteador mantendo o *firmware* atualizado, troque a senha de administração e, se possível, ative o *firewall* do roteador, quando disponível.
- [x] Use *internet* de provedores de oficiais e com boa reputação. Não use internet compartilhada de terceiros ou aberta.

Cuide de sua privacidade

Fique atento ao que está sendo mostrado ou compartilhado sobre você, pois as pessoas podem gravar.

Não viralize!

Checklist

- Certifique-se que seu vídeo e microfone estão silenciados/desativados, sendo ativados somente quando necessário. Use um protetor para cobrir a *webcam*.
- Faça suas chamadas de áudio/vídeo em locais reservados, mesmo estando em casa. Sempre que possível use “plano fundo virtual”. A *internet* está cheia de vídeos virais com profissionais trabalhando em locais inusitados, como, por exemplo, em banheiros.
- Antes de compartilhar a tela do seu computador, feche todos os aplicativos, principalmente os de redes sociais, pastas e arquivos particulares. Desative o recurso de autocompletar dos navegadores ou de cofres de senhas, não permitindo a exposição dos seus dados pessoais.
- Dê preferência ao compartilhamento de aplicativos e janelas, utilize o compartilhamento de tela em último caso.

Fique atento ao ambiente ao seu redor

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.

Checklist

- ☑ Evite fazer chamadas de áudio/vídeo em locais públicos, como cafés.
- ☑ Ao fazer chamadas de áudio/vídeo use *headset*/ fones de ouvidos e fundo virtual.
- ☑ Antes de digitar credenciais de acesso, certifique-se de que não está sendo observado e filmado.
- ☑ Desligue dispositivos ativados por voz antes de fazer reuniões.
- ☑ Posicione seu monitor ou celular de forma que outras pessoas não vejam seu conteúdo ou utilize películas de privacidade.

Comunique à organização qualquer suspeita de problema

Clicou 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 à organização.

Quanto antes um incidente for detectado e contido, menores serão os transtornos e prejuízos.

Checklist

- ☑ Saiba quais são os canais oficiais para acionar o suporte técnico e/ou notificar potenciais incidentes de segurança.

Conclusão

O trabalho remoto oferece inúmeras vantagens, mas também apresenta desafios significativos em termos de segurança da informação. Ao adotar as melhores práticas e medidas de segurança abordadas neste módulo, os profissionais e as organizações podem mitigar os riscos associados ao trabalho remoto e proteger, de forma eficaz, seus ativos de informação.

Lembre-se: a segurança da informação é uma responsabilidade compartilhada por todos os envolvidos, do colaborador à alta direção da instituição.

Esse conteúdo foi elaborado com base nas melhores práticas e nos melhores princípios de segurança da informação e destina-se a fornecer orientações valiosas para profissionais que trabalham remotamente.

Fica a dica

Se você tiver alguma dúvida ou precisar de assistência adicional, não hesite em entrar em contato com um especialista em segurança da informação ou com a equipe de TI da sua organização.

Agora, você está preparado para enfrentar os desafios do mundo digital com confiança e segurança!