

A person is shown from the side, sitting at a desk and working on a laptop. The scene is dimly lit, with the primary light source being the laptop screen and keyboard. The person's hands are visible on the keyboard, and they are wearing a watch on their left wrist. The background is dark and out of focus, suggesting an office environment.

AVIVATEC

Trabalho Remoto com Segurança

Conheça pontos importantes para executar o trabalho remoto visando a segurança das informações.



Evandro Ribeiro

ITIL EXPERT, ISO 20.000 SPECIALIST,
CYBER SECURITY, ETHICAL HACKING

e.ribeiro@avivatec.com.br

Experiências profissionais:

- . Head da equipe de Respostas a Incidentes e Cyber Security na Avivatec;
- . Especialista Cyber na Câmara Interbancária de Pagamentos (CIP);
- . Coordenador de Resposta a Incidentes na Telefônica | Vivo – 10 anos;
- . Mesa de Crise Telecom;
- . Revisão de Processos Cyber Security;
- . Implantação de SOC (Security Operation Center) em clientes com administração dos concentradores de VPN para engenharia, monitoração e resposta à incidentes de Segurança da Informação.

O protagonista do trabalho
remoto é **VOCÊ!**





Confiança

Para crescer como time, é preciso **praticar e aumentar a confiança no trabalho remoto**. Isso só é possível quando todos sabem suas respectivas responsabilidades.



Comprometimento

Para o trabalho remoto funcionar é necessário **disciplina na comunicação e comprometimento**.



Trabalho em Equipe

Construir redes de relacionamento é fundamental para criar uma cultura de trabalho na qual, independentemente da posição ocupada, **todos agem e tomam decisões**.



Tecnologia e Segurança

Pandemia (COVID-19) > aumento na demanda por acesso remoto seguro.

É preciso definir pontos de atenção na estratégia de segurança para a continuidade das operações em diferentes cenários de maturidade e infraestrutura.

Dicas de segurança





E-mails e acesso remoto

Não cadastrar e-mail corporativo em sites externos.

Enviar **anexos com senha**.

Se o tema for muito complexo,
ligar antes de enviar mensagem.



E-mails e
acesso remoto

Não conectar o computador
em redes Wi-Fi públicas.

Evitar deixar máquinas
desbloqueadas.

Compartilhamento de documentos
internos através dos meios corporativos
como e-mail e armazenamento
em nuvem.



E-mails e acesso remoto

Evitar comentar sobre o trabalho em áreas comuns.

Trocar informações apenas no e-mail corporativo.

Atenção aos *phishings* e *fake news*.
E-mails com promessas de curas milagrosas e prevenção garantida podem acessar seus dados.

VPN

Por meio da VPN, o colaborador pode acessar os serviços de rede e informações confidenciais da empresa à distância.

É como se o computador estivesse no escritório, logo, todos os cuidados devem ser iguais.



Proteção contra golpes de suporte técnico

Golpistas podem fazer abordagens pelo telefone e fingir ser representantes da empresa.

Com acesso ao um equipamento interno, podem ter controle total, comprometendo os dados e a companhia.

Conectar apenas aos canais de suporte formais oferecidos pela empresa e seguir sempre as orientações da equipe de TI.



Uso de dispositivos externos

Caso o acesso a USB e HD externos, por exemplo, seja liberado, é importante seguir algumas recomendações:

Uso exclusivo > Para garantir que os dispositivos contêm somente conteúdo de conhecimento próprio e sejam utilizados apenas em equipamentos seguros.

Scan > Antes do acesso ao dispositivo, deve ser feito um scan.

Conteúdo > Não misturar conteúdos pessoais com arquivos de uso corporativo.

Criptografia > Criptografar conteúdos com soluções já fornecidas e homologadas pela TI da empresa.



Proteção de senhas

Dicas para uma senha forte:

- **Ter 8 ou mais caracteres.**
Quanto maior, melhor.
- **Combinação de letras** maiúsculas e minúsculas, números e símbolos.
- **Evitar palavras que podem ser encontradas em um dicionário.**
- **Não utilizar** nomes próprios, mês ou ano como parte da senha.
- **Não criar senhas sequenciais** como @01, @02, diferindo das senhas anteriores.



Proteção de senhas



Nunca compartilhar senha com ninguém e nunca escrever em papel ou em aplicativos de notas.

Nunca utilizar a opção de “memorizar minha senha” oferecida pelos navegadores da Internet.

Nunca fornecer senha para contatos de suporte, por telefone, mensagem, formulários ou e-mail.

Phishing

Algumas maneiras de identificar



- **Erros de ortografia e gramática** > Mensagens de e-mail repletas de erros podem ser golpe.
- **Links suspeitos** > Se suspeitar que uma mensagem de e-mail seja golpe, não abra nenhum link contido nela. Dica: posicionar o cursor do mouse sobre o link – sem clicar – para ver se o endereço corresponde ao link digitado na mensagem.
- **Ameaças** > E-mails que tentam causar sensação de pânico para serem respondidos rapidamente. Podem incluir declarações como "Você deve retornar até o fim do dia" ou sinalizar penalidades financeiras caso não sejam respondidos.

Phishing

Algumas maneiras de identificar



- **Falsificação** > Links que levam a sites falsos ou exibem janelas pop-up com aparência legítima.
- **Endereços da web alterados** > Uma forma de falsificação é a utilização de endereços muito parecidos com nomes de empresas conhecidas, mas ligeiramente alterados, como “www.micorsoft.com” ou “www.mircosoft.com”.
- **Saudação** > Nome da pessoa incorreto, por exemplo.
- **Incompatibilidade** > O texto do link e URL são diferentes um do outro, ou o nome do remetente, assinatura e URL são diferentes.

Phishing

Algumas maneiras de identificar



As técnicas não se aplicam somente aos e-mails, mas também a mensagens de texto ou chamadas telefônicas.



Criminosos sofisticados organizam call centers para ligar ou mandar SMS automaticamente para os números de possíveis alvos.

As mensagens geralmente incluem telas que induzem a inserção de número PIN ou algum outro tipo de informação pessoal.

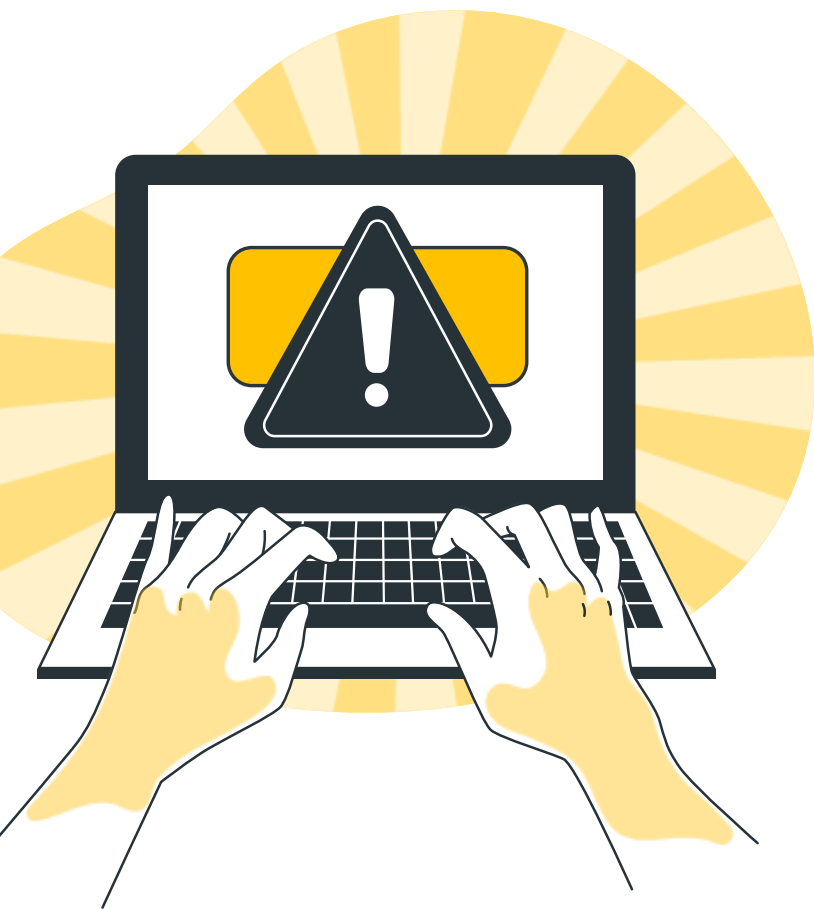


Vazamento de informações

Manter o trabalho funcionando é muito importante, **mas é preciso lembrar que os dados manuseados são da empresa, por isso:**

- **Não gravar, fotografar ou fazer print screen** de conteúdos apresentados em reuniões sem o consentimento dos demais participantes;
- **Não fazer cópias de arquivos** para dispositivos pessoais, como notebook, celular, HDs e pen drives;
- **Evitar o compartilhamento de informações** para redes sociais, e-mails pessoais e outros grupos que não sejam da empresa.

Vazamento de informações



É responsabilidade de todos cuidar e proteger os dados de clientes, colaboradores e fornecedores.



O não cumprimento pode implicar sanções legais, como multas descritas na Lei Geral de Proteção de Dados.

Obrigado!

Plataformas Digitais

- Fábrica de Software
- Desenvolvimento de API's
- Desenvolvimento de escopo aberto e fechado
- Squads multidisciplinares
- Criação de APP e Site
- UX / UI
- Sustentação de Aplicações
- Atuações em Backlogs

Gestão de Infraestrutura e Nuvem

- Multicloud
- NOC
- Service Desk
- Plano de Migração de Ambientes
- Office 365
- Gerenciamento de Backup
- DR
- Redes
- Telecom
- Telefonia Voip

Gestão de Segurança e Cyber Security

- Assessment
- SOC
- Gestão de Vulnerabilidade
- Code Review
- Controle de Acessos
- Desenvolvimento Seguro
- Antivírus
- Criptografia
- DLP

Ficou com alguma dúvida?

Fale com o nosso time de especialistas, nós temos uma solução que se encaixa com a sua necessidade!

