**COMO POTENCIALIZAR O TRABALHO REMOTO SEM RISCOS À CIBERSEGURANÇA?**

**Trabalho Remoto:**

Também chamado de teletrabalho e home office**, o trabalho remoto consiste em fazer atividades profissionais à distância,** usando a tecnologia para realizar as tarefas e se conectar com os colegas.

**A pandemia e o trabalho remoto:**

Diante da pandemia do coronavírus, que impôs medidas de restrição à circulação e aglomeração de pessoas, **11% dos trabalhadores ativos no Brasil exerceram suas atividades profissionais de forma remota.** É o que aponta um estudo divulgado nesta quinta-feira (15) pelo Instituto de Pesquisa Econômica Aplicada ([Ipea](https://g1.globo.com/tudo-sobre/ipea/)).

Empresas de todo mundo estão sendo impactadas pela reclusão social imposta pela pandemia do COVID-19. Isso está levando companhias a adotarem o modelo de trabalho remoto, cenário que exige a proteção dos ativos mais valiosos de uma organização: fator humano e dados

Os que mais caem em golpes virtuais ou vírus, são usuários novos que não entendem muito como funciona a web.

E para se manter seguro na internet existem diversos, softwares, hardwares, serviços e também, treinamento Constant de usuários, porque novos ataques cibernéticos surgem todo ano, de maneiras diferentes.

**Os principais alvos destes bandidos virtuais são:**

Empresas de diversos ramos instituições bancárias instituições governamentais figuras públicas e famosos.

**Desafios da quarentena**

As empresas devem criar um plano de continuidade para o home-office e avaliar o impacto causado pela quarentena para tomar medidas.

**Capacidade de funcionalidade**

Deve se fazer algumas perguntas para saber se a empresa realmente está preparada. Os funcionários tem infraestrutura para trabalhar em casa? A cadeia de suprimento vai funcionar? Temos internet de qualidade para toda essa gente? E VPN? É possível trabalhar sem VPN?  
  
VPN: Virtual Private Network (Rede Privada Virtual)  
As VPN’S criptografam seu tráfego na internet e disfarçam sua identidade online. Tem múltiplo fator de autenticação e camadas de monitoramento até os dados mais preciosos da empresa

**As melhores práticas**

* **Segurança na web:**  Permite o funcionário navegar na internet protegido contra conteúdos maliciosos.
* **E-mail seguro:** Garante a proteção das contas e a eliminar a falsificação de mensagens, malware em anexos e phishing.
* **Prevenção de vazamento de informações:** Faça a avaliação contínua dos dados e evite vazamentos.
* **Sistema interno de ameaças:** Monitore os usuários com acessos à dados confidenciais.
* **Análise do comportamento humano:** Monitore o comportamento dos usuários e aplique políticas de proteção.
* **Alavancar soluções em nuvens:** Garantir o controle de atividades e fluxo de dados em aplicativos em nuvem com o monitoramento adequado.
* **Controle de ameaças avançadas:** É preciso impedir que as ameaças escondidas em informações (principalmente sobre o vírus) chegue
* **Arquitetura flexível de soluções de segurança cibernéticas:** Possibilita ter modelos em nuvens ou híbridos com o mesmo nível de segurança em um cenário de localidade flexível
* **Reduções de controles de monitoramento e alerta:** Faça uma gestão de incidentes consolidadas.

**Nomes:** Alexandre da Silva Mendes Ferreira (nº 01), Leonardo Sales de Castro Monteiro (nº 12), Lívia Ester da Silva de Sousa (nº 13)

**Turma:** 1151 – Informática para Internet