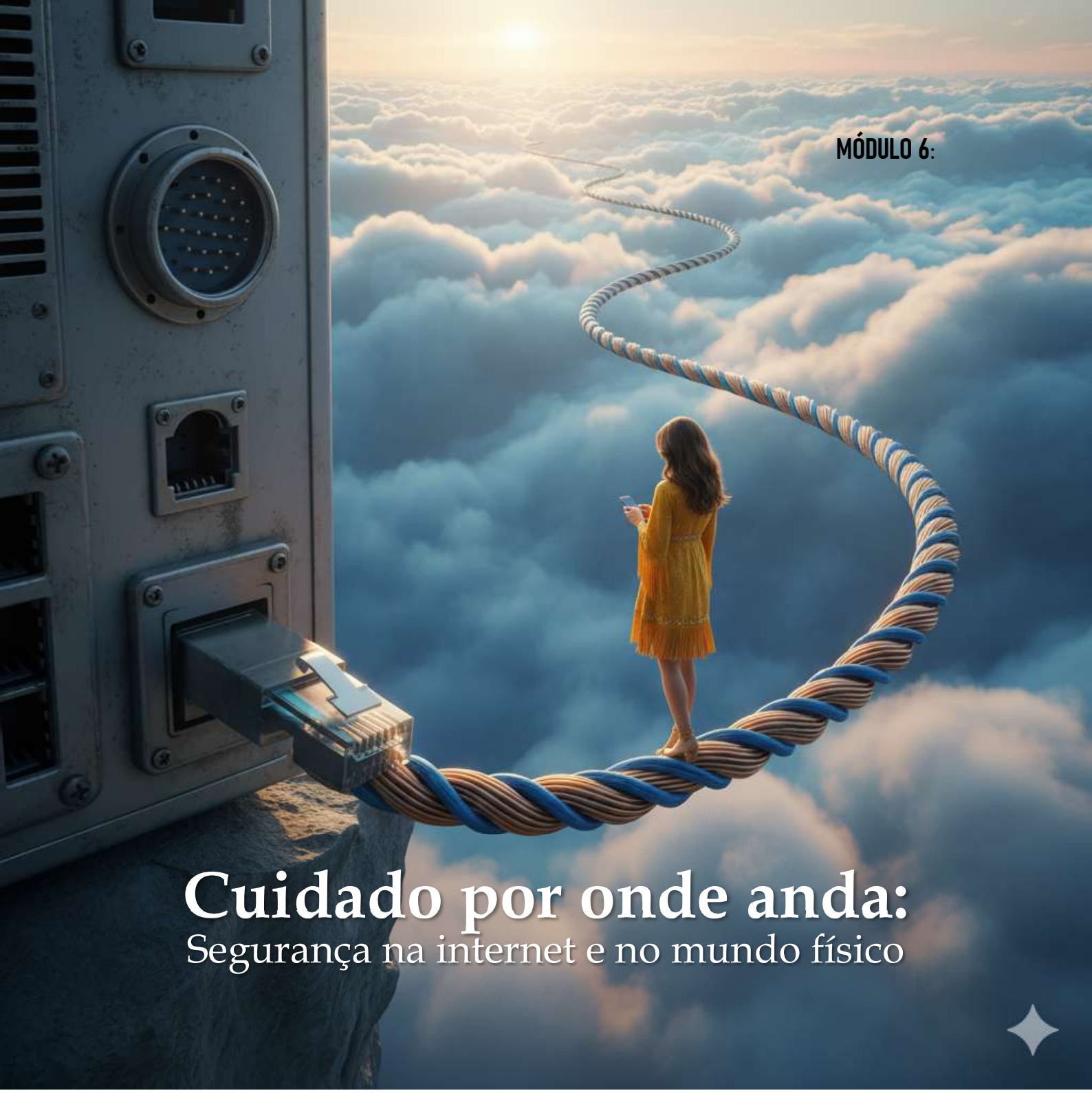


MÓDULO 6:

Cuidado por onde anda:

Segurança na internet e no mundo físico

Cuidado por onde anda: Integrando a segurança cibernética e física no dia a dia da cooperativa

A segurança da informação não se restringe ao ambiente digital; ela se estende ao **mundo físico** e aos hábitos diários do colaborador. Este artigo foca em práticas essenciais que integram a segurança digital e física, essenciais para a proteção da cooperativa. Detalhamos a importância dos hábitos de **"Mesa Limpa" e "Tela Bloqueada"** para prevenir o acesso não autorizado. Analisamos os **perigos das redes Wi-Fi públicas** e como elas podem ser portas de entrada para ataques. Por fim, estabelecemos uma **política clara para o uso de *pen drives* e *downloads* seguros**, minimizando a introdução de *malware* na rede corporativa.

Palavras-chave: Segurança Física, Mesa Limpa, Tela Bloqueada, Wi-Fi Público, Segurança de Dispositivos Removíveis, Download Seguro.

---

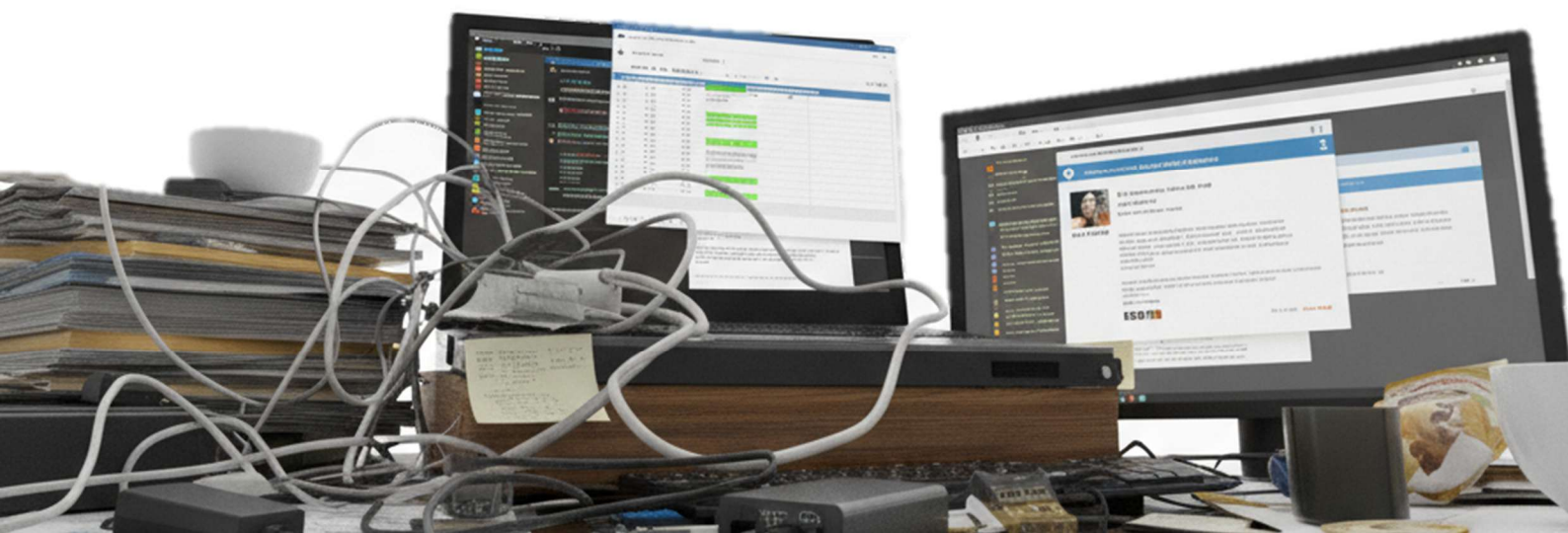
1. Introdução: A segurança é 360 graus

A segurança cibernética é frequentemente associada a *softwares* e *firewalls*. No entanto, uma das maiores vulnerabilidades de uma organização reside na interface entre o mundo digital e o físico. Um criminoso pode obter acesso a dados confidenciais simplesmente observando um papel na mesa ou acessando um computador desbloqueado.

Este módulo visa conscientizar o colaborador de que a segurança é uma postura **360 graus**, que deve ser mantida tanto na frente do computador quanto ao se afastar dele, seja no escritório ou em um ambiente externo.

2. Os hábitos da "Mesa limpa" e "Tela bloqueada"

Estes dois hábitos são a base da segurança física no ambiente de trabalho e previnem o acesso não autorizado a informações confidenciais por visitantes, terceiros ou até mesmo colegas desavisados.



2.1. Mesa Limpa (*Clean Desk Policy*)

A Política de Mesa Limpa determina que, ao final do dia ou ao se ausentar da mesa por um longo período, **nenhum documento confidencial ou material sensível deve ficar exposto** [1].

Item	Ação Correta	Risco de Não Conformidade
Documentos Impressos	Guardar em gavetas trancadas ou destruir em trituradora de papel segura.	*Shoulder Surfing* (observação por cima do ombro), roubo de informações.
Anotações e Rascunhos	Não anotar senhas ou informações de cooperados em *post-its* ou cadernos.	Exposição de credenciais e dados sensíveis.
***Pen Drives* e Dispositivos**	Guardar em local seguro e trancado.	Roubo ou perda, que pode resultar em vazamento de dados.

2.2. Tela bloqueada (*Screen lock*)

A regra da Tela Bloqueada é simples e absoluta: **Ao se ausentar da mesa, mesmo que por um minuto, bloqueie a tela do seu computador.**

- **Comando Rápido:** Use a combinação de teclas **Windows + L** (ou equivalente no Mac) para bloquear instantaneamente a tela.
- **Risco de Não Conformidade:** Um computador desbloqueado permite que qualquer pessoa acesse sistemas, envie e-mails em seu nome ou copie dados em segundos.

3. Os perigos das redes Wi-Fi públicas

Trabalhar remotamente ou em viagens de negócios exige cautela, especialmente ao se conectar a redes Wi-Fi públicas (aeroportos, cafés, hotéis). Essas redes são um campo fértil para criminosos digitais.

3.1. Ataque do "Gêmeo maligno" (*Evil Twin*)

O criminoso cria uma rede Wi-Fi falsa com um nome semelhante ao da rede legítima do local (ex: "Aeroporto-Free" em vez de "Aeroporto-Oficial"). Ao se

conectar à rede falsa, todo o seu tráfego de internet passa pelo computador do criminoso, que pode roubar suas senhas e dados [3].

3.2. Ataques *man-in-the-Middle* (Homem no meio)

Em redes Wi-Fi públicas, o tráfego de dados não é criptografado. Um *hacker* pode interceptar a comunicação entre seu dispositivo e o site que você está acessando, visualizando dados confidenciais.

Diretriz para Implementação:

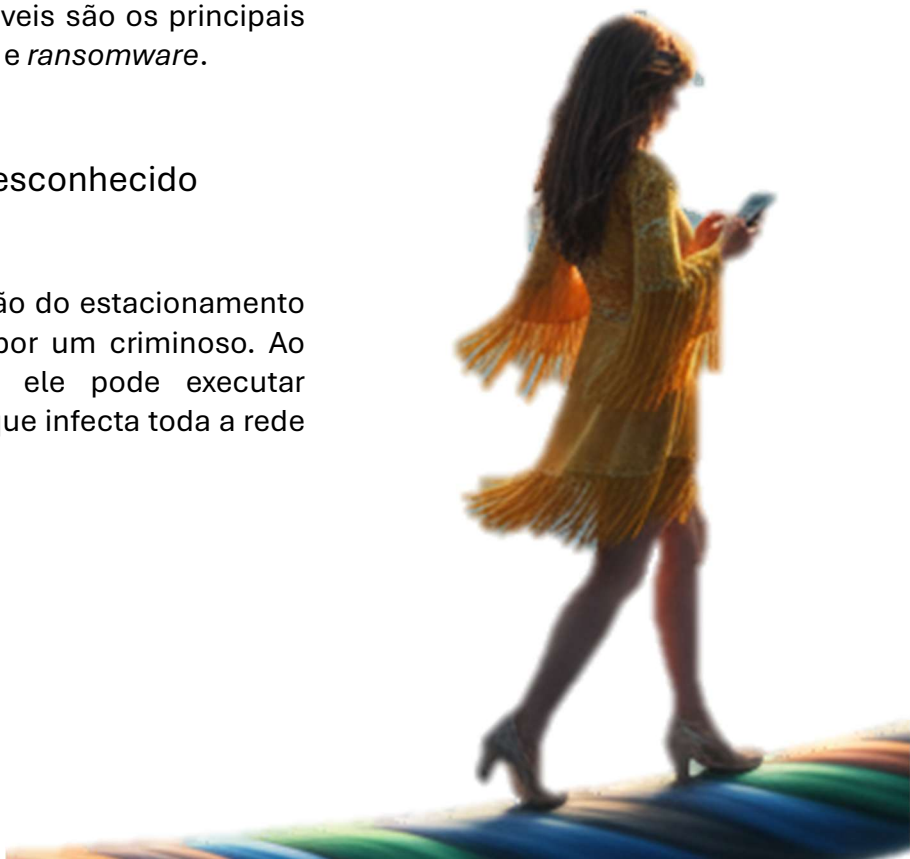
- **Evite:** Nunca acesse sistemas internos da cooperativa ou realize transações financeiras em redes Wi-Fi públicas.
- **Use VPN:** Se precisar trabalhar em um local público, **sempre utilize a Rede Privada Virtual (VPN)** fornecida pela cooperativa. A VPN criptografa seu tráfego, tornando-o ilegível para *hackers*.
- **Verifique a URL:** Certifique-se de que o site que você está acessando começa com **https://** (o "s" indica segurança e criptografia).

4. Política para uso de pen drives e downloads seguros

Dispositivos de armazenamento removível e *downloads* de fontes não confiáveis são os principais vetores de infecção por *malware* e *ransomware*.

4.1. O Perigo do *Pen Drive* desconhecido

Um *pen drive* encontrado no chão do estacionamento pode ser uma "isca" plantada por um criminoso. Ao inseri-lo no seu computador, ele pode executar automaticamente um *malware* que infecta toda a rede da cooperativa.



Diretriz Prática:

- **Proibição:** A política da cooperativa deve proibir a conexão de *pen drives* pessoais ou desconhecidos em computadores de trabalho.
- **Uso Autorizado:** Utilize apenas dispositivos de armazenamento removível fornecidos e criptografados pela cooperativa.
- **Verificação:** Qualquer dispositivo autorizado deve ser submetido a uma varredura de antivírus antes do uso.

4.2. Downloads Seguros

O *download* de *softwares* piratas, *freewares* de fontes desconhecidas ou arquivos de anexos de e-mail suspeitos é um risco direto de segurança.

Diretriz Prática:

- **Fontes Oficiais:** Baixe *softwares* ou arquivos apenas de fontes oficiais e autorizadas.
- **Consulte o TI:** Se precisar de um *software* específico, solicite-o à equipe de TI. **Não instale nada por conta própria.**
- **Verifique o Anexo:** Aplique as regras do Módulo 3 (*Phishing*) para garantir que um anexo é legítimo antes de baixá-lo.

5. Conclusão

A segurança da informação é uma disciplina que abrange tanto o digital quanto o físico. Ao adotar os hábitos da **Mesa Limpa e Tela Bloqueada**, ao ser cauteloso com as **redes Wi-Fi públicas** e ao seguir rigorosamente a **política de uso de dispositivos removíveis**, o colaborador garante que o ambiente de trabalho, seja ele físico ou remoto, permaneça uma fortaleza contra as ameaças. O cuidado por onde anda é o cuidado com a cooperativa.

Referências Bibliográficas

[1] Portal Gov.br - LNNC. **A importância e a necessidade da Política de Mesa Limpa e Tela Limpa**. Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-

informacao/2025/a-importancia-e-a-necessidade-da-politica-de-mesa-limpa-e-tela-limpa
[2] Symbioti. **Posso usar pen drive na empresa?**. Disponível em: https://www.symbioti.com.br/saiba-quais-sao-os-perigos-do-pen-drive-no-ambiente-empresarial/
[3] Global Suite Solutions. **Você conhece os riscos de trabalhar conectado a redes Wi-Fi públicas?**. Disponível em: https://www.globalsuitesolutions.com/pt/voce-conhece-os-riscos-de-trabalhar-conectado-a-redes-wi-fi-publicas/[4] (Adicionar referências adicionais conforme aprofundamento da pesquisa, se necessário).