# Recomendações de **segurança** da informação para o **teletrabalho** na UNILA

**Não caia na rede**

UNILA

Com a adesão ao teletrabalho pelos servidores da UNILA, torna-se necessário que todos tenhamos mais atenção com a Segurança da Informação. Dentro do ambiente da instituição, há segurança lógica e física dos equipamentos e dados, mas, em teletrabalho, é essencial que essa preocupação seja absorvida no cotidiano dos servidores.

Dentro da rede da UNILA, existem diversos mecanismos de segurança, como segregação de redes de trabalho de redes públicas, firewalls e sistemas de detecção de intrusão, antivírus, computadores com atualizações de segurança automáticas, entre outros mecanismos que auxiliam na redução de vazamento de dados e demais fraudes digitais.

Quando o servidor passa a atuar a partir de locais externos à universidade, os riscos à segurança da informação crescem e, individualmente, precisamos nos preocupar e resolver questões como a falta de controles físicos de segurança, com o uso de redes inseguras e com o uso de computadores pessoais que possam estar com a segurança comprometida.

Por essa razão, **a maioria dos ataques e vazamento de dados começa por falha humana** – especialmente por aqueles que pensam que “isso nunca aconteceu comigo, então não preciso me preocupar” ou “o que esses hackers vão querer comigo, eu não tenho nada a esconder”.

**Motivos para dar atenção à segurança da informação**

Hoje, o mundo digital permeia nossas vidas, tanto em âmbito pessoal quanto no profissional. Compras são feitas digitalmente, o gerenciamento de dinheiro é feito usando aplicativos, processos no trabalho são movidos e assinados eletronicamente, as pessoas se comunicam sobre trabalho e vida pessoal por meios digitais, etc. Assim, por ser um ambiente tão rico em possibilidades, atrai muito a atenção de aproveitadores e estelionatários. Seus dados pessoais, dados sensíveis da UNILA e de outras pessoas relacionadas à instituição devem permanecer seguros, para evitar que caiam em mãos erradas e que possam alimentar esse “mercado de fraudes digitais”.

Assim, elencamos a seguir algumas recomendações que podem auxiliar na configuração do ambiente de teletrabalho. Iniciamos, assim, com a definição do propósito deste guia, seguido por cuidados do local de trabalho e rede de dados, e cuidados com as estações de trabalho utilizadas para acesso a recursos da UNILA.

**Propósito deste guia**

Este guia apresenta um conjunto de controles essenciais para o teletrabalho, a fim de estabelecer um nível mínimo de segurança para evitar problemas relacionados a confidencialidade, integridade e disponibilidade das informações institucionais, bem como de informações pessoais, uma vez que:

- se alguém não autorizado pode acessar sua rede, ele também pode acessar informações sensíveis suas e da UNILA;
- se o seu computador ou roteador residencial estiver comprometido (com vírus ou sistema espião), ele pode se tornar parte de uma *botnet* (rede de computadores “zumbis”), que pode ser usada para atacar outros sistemas de computação (da sua casa ou de organizações diversas conectadas à internet);
- dados da UNILA e da comunidade acadêmica devem ser mantidos em segurança, para evitar vazamentos e para manter consonância com a Lei Geral de Proteção de Dados (LGPD).

**Recomendações sobre local de uso, rede e acesso à internet**

- Utilize um local que ofereça privacidade, de forma a evitar que terceiros tenham acesso a informações sensíveis exibidas em seu computador ou em documentos físicos que venham a ser manuseados, ou ao conteúdo de conversas sobre temas sensíveis;
- Evite usar computadores públicos (como de hotéis e lan houses), pois eles podem possuir sistemas que monitoram o que é digitado no teclado (*keyloggers*) e podem capturar indevidamente suas senhas;
- Ao elaborar documentos, prefira utilizar serviços em nuvem oferecidos pela instituição (como o Google Docs e Drive), para evitar o acúmulo de informações institucionais em seu computador e para evitar a necessidade de backup desses documentos;
- Evite usar redes públicas (como as de aeroporto e lan houses) – é comum que redes oferecidas gratuitamente (como redes WiFi públicas) sejam utilizadas por hackers para interceptar a comunicação e se apropriarem de credenciais de acesso ou de informações sensíveis;
- Para a configuração de roteadores/modems/pontos de acesso, tenha os seguintes cuidados:
    - Trocar o nome da rede de forma que não indique seu nome, endereço ou modelo do dispositivo;
    - Colocar uma senha longa, porém, fácil de ser lembrada (para que não seja preciso anotar em papel);
    - Trocar a senha padrão de administrador do dispositivo;
    - Usar senhas diferentes para a administração e para a utilização do dispositivo;
    - Criar rede separada para convidados caso seu dispositivo tenha essa opção (SSID diferente na wi-fi);
    - Codificar o tráfego de informações usando codificação WPA2 ou WPA3 (e não WEP ou WPA);
    - Desativar a função WPS, que permite que dispositivos sejam conectados à rede apenas pressionando o botão frontal do equipamento (pois alguém pode usar esse momento para obter acesso indevido à sua rede);
    - Habilitar o recurso de firewall.

**Caso esteja usando uma estação de trabalho da UNILA**

- As estações de trabalho da UNILA aplicam automaticamente atualizações de segurança;
- Não permita o uso desses dispositivos por terceiros;
- Prefira armazenar documentos de caráter institucional em nuvem, por meio de ferramentas fornecidas pela instituição, como o Google Docs ou Drive (usando sua credencial de acesso da UNILA);
- Para trocar a senha de acesso ao computador, é necessário conectar-se à rede VPN da instituição (será aplicada no computador a mesma senha utilizada pelas credenciais @unila);
- Ter pleno conhecimento da norma de uso das estações de trabalho da UNILA.

**Caso esteja usando uma estação de trabalho pessoal**

- Configure o bloqueio automático da tela e uma senha forte para acesso ao dispositivo;
- Evite, na medida do possível, compartilhar o computador que usa para o teletrabalho com outros membros da família. Se não for possível, é interessante que sejam criados usuários distintos no computador, sendo ao menos um usuário para quem faz o teletrabalho, onde ele faça logoff sempre que encerrar suas atividades, e ao menos um usuário para o restante da família;
- Utilize no dia a dia, sempre que possível, uma conta que não seja administrador local do computador. Reserve a conta de administrador local para utilização apenas quando necessário, para, por exemplo, instalar novos softwares em seu computador;
- Evite navegar na internet, abrir e-mails, whatsapp, etc, com essa conta de administrador local;
- Prefira não armazenar documentos de caráter institucional em seu dispositivo pessoal. Opte pelos sistemas da instituição e ferramentas de edição em nuvem (como o Google Docs ou Drive), usando sua credencial de acesso da UNILA;
- Utilize apenas softwares originais, com destaque para o sistema operacional (Windows, MacOS, Linux) – pois, ao instalar um software pirata, você pode estar comprometendo a segurança de seu dispositivo;
- Utilize um antivírus e mantenha-o atualizado diariamente. A Microsoft disponibiliza o Windows Defender gratuitamente para os usuários do Windows 10 e Windows 11;
- Mantenha atualizações de segurança automáticas diárias do sistema operacional, antivírus e demais sistemas do dispositivo.

**Cuidados adicionais**

- Ao se ausentar do ambiente de trabalho, mesmo que por alguns minutos, bloqueie o computador (Tecla ⊞ + L);
- Use senhas seguras e diferentes para fins pessoais e profissionais;
- Não anote senhas em papel, crie uma senha segura e fácil de lembrar, como uma frase (ver guia de recomendações de senhas);
- Caso perceba alguma anormalidade nos serviços de TI ou perceba que houve vazamento de informações da UNILA, comunique a ETIR (Equipe de Prevenção, Tratamento e Resposta de Incidentes Cibernéticos) pelo e-mail etir@unila.edu.br ou pelo sistema de chamados da instituição;
- Tenha pleno conhecimento da Política de Segurança da Informação da UNILA e suas normas complementares;
- Evite o uso de pendrives e discos USB externos para carregar dados pessoais de membros da UNILA e, caso seja indispensável, utilize uma ferramenta de criptografia para os dados.

**Referências**

- CIS - *Center for internet security: Telework and Small Office Network Security Guide*.
- NIST - *National Institute of Standards and Technology: Guide to Enterprise Telework and Remote Access Security*.