Segurança da Informação

Alexandre Neves, Felipe Fidelis

18 de outubro de 2025

1 Introdução

Este é um documento mínimo em LaTeX. Substitua o conteúdo conforme necessário.

2 Política de Segurança e Uso dos Computadores dos Laboratórios

2.1 Objetivo

Estabelecer diretrizes e responsabilidades para garantir a segurança, integridade, disponibilidade e uso adequado dos recursos de informática (hardware, software e rede) presentes nos laboratórios do Instituto Federal Goiano - Campus Ceres, prevenindo acessos não autorizados, danos e mau uso.

2.2 Âmbito de Aplicação

Esta política aplica-se a todos os usuários (estudantes, professores, pesquisadores e técnicos) que utilizam os computadores localizados nos laboratórios da instituição.

2.3 Diretrizes Gerais de Uso (Para Todos os Usuários)

2.3.1 Uso de Contas de Acesso

1. **Contas Individuais e Não Compartilháveis:** Cada usuário (aluno e professor) deve utilizar sua conta de acesso pessoal e intransferível. **É**

estritamente proibido compartilhar senhas ou utilizar contas de terceiros.

2. **Senhas Fortes:** As senhas devem seguir os requisitos mínimos de complexidade definidos pela instituição (ex: mínimo de 8 caracteres, com letras maiúsculas, minúsculas, números e símbolos).

3. **Logout e Bloqueio:** Os usuários devem sempre efetuar *logout* ou bloquear a estação de trabalho ao se ausentarem, mesmo que por um breve período.

4. **Monitoramento:** A instituição reserva-se o direito de monitorar o uso dos equipamentos para fins de manutenção e segurança, conforme a legislação vigente.

2.4 Software e Configurações

1. **Instalação e Configuração de Ambiente de Desenvolvimento (Sistemas Multiusuários):** É proibida a modificação ou remoção de qualquer software, aplicativo ou arquivo executável que faça parte do sistema operacional base. **EXCEÇÃO - Configuração de Ambiente:** Nos laboratórios dos cursos de Sistemas de Informação, Informática para Internet e Inteligência Artificial, é permitido que o aluno realize a configuração do seu ambiente de desenvolvimento pessoal (*personal environment*) para fins curriculares, **desde que**:

   (a) A instalação de bibliotecas, pacotes e *frameworks* seja feita utilizando **gerenciadores de pacotes com escopo local** (ex: `pip -user`, `npm` em modo local, gerenciadores de ambientes virtuais como `conda` ou `venv`).

   (b) A configuração de variáveis de ambiente, como o `PATH`, seja feita estritamente através dos arquivos de configuração da *shell* no diretório `home` do usuário.

   (c) **Não seja utilizada a elevação de privilégios de administrador** (`sudo` ou `root`) para qualquer instalação ou configuração.

2. **Uso de Contêineres e Virtualização:** Para tarefas que exijam contêineres (*Docker, Podman*), o aluno deve, prioritariamente, utilizar soluções *rootless* (que não requerem acesso de administrador) ou am-

bientes de desenvolvimento pré-configurados e aprovados pela TI. A concessão de acesso ao grupo `docker` é proibida por representar risco de segurança à máquina hospedeira.

3. **Downloads Não Autorizados:** É proibido o download e/ou armazenamento de conteúdo ilegal, malicioso (*vírus, malware*), pornográfico ou que viole direitos autorais.

4. **Alteração de Configurações:** É proibida a alteração de configurações de sistema, rede, papel de parede, *screensaver* ou qualquer ajuste que comprometa o padrão operacional da máquina.

2.4.1 Uso da Rede e Internet

1. **Acesso Remoto (*SSH, VNC, RDP*):** O acesso remoto entre estações de alunos é estritamente proibido. O uso de protocolos de acesso remoto para fins acadêmicos ou de pesquisa deve ser formalmente solicitado e limitado a servidores específicos da instituição, conforme as regras de *firewall* e segurança.

2. **Comportamento Ético:** É proibido utilizar a rede para fins que violem a lei, promovam *hacking, phishing* ou qualquer atividade que cause prejuízo à instituição ou a terceiros.

2.5 Diretrizes Específicas para Alunos

1. **Uso Exclusivo para Fins Acadêmicos:** Os computadores dos laboratórios destinam-se primariamente a atividades de ensino, pesquisa e extensão. O uso pessoal excessivo (jogos, redes sociais, *streaming*) pode ser restringido.

2. **Armazenamento Temporário:** Arquivos pessoais devem ser salvos em serviços de armazenamento em nuvem da instituição (se disponíveis) ou em mídias externas. A instituição não se responsabiliza por arquivos salvos no disco local, que podem ser apagados a qualquer momento (ex: no *reboot* da máquina).

2.6 Diretrizes Específicas para Professores/Docentes

2.6.1 Segurança da Estação Docente (Mesa do Professor)

1. **Desativação de Serviços Desnecessários:** O serviço **SSH (ou qualquer outro serviço de acesso remoto como VNC ou RDP)** deve ser **desativado** na estação do professor por padrão. Ele só poderá ser ativado temporariamente para propósitos didáticos específicos, e deve ser desativado imediatamente após o uso.

2. **Firewall Rigoroso:** O *firewall* da estação docente deve estar sempre ativo e configurado para **bloquear todas as conexões de entrada**, exceto aquelas absolutamente necessárias para o funcionamento em sala de aula (ex: projeção de tela).

3. **Contas de Usuário:** O professor deve utilizar uma **conta de usuário padrão (não administrador)** para as aulas, reservando a conta de administrador para tarefas de manutenção ou instalação de software, se necessário.

4. **Autenticação Dupla (Se Possível):** Em máquinas com acesso a sistemas sensíveis, considerar o uso de autenticação de dois fatores ou o bloqueio por senha robusta no *login* inicial.

5. **Acesso Físico:** O professor deve garantir que a estação docente esteja fisicamente segura (ex: *case* com trava ou cabo de segurança), limitando o acesso a portas USB ou físicas por alunos.

2.6.2 Responsabilidades do Professor em Sala de Aula

1. **Conscientização:** O professor deve orientar os alunos sobre esta política no início de cada disciplina.

2. **Monitoramento:** O professor é o responsável imediato por monitorar o comportamento dos alunos no laboratório e reportar atividades suspeitas ou violações de segurança ao setor de TI.

3. **Projeção de Tela:** Antes de iniciar a projeção (*datashow*), o professor deve verificar a tela, garantindo que nenhuma aplicação não autorizada esteja sendo executada.

2.7 Medidas Disciplinares

O não cumprimento desta Política de Segurança e Uso constitui uma violação das normas internas da instituição e acarretará as seguintes medidas disciplinares:

1. **Advertência:** Em casos de primeira ocorrência e infração leve.
2. **Suspensão de Acesso:** Suspensão temporária do acesso aos laboratórios e/ou à rede institucional.
3. **Processo Disciplinar:** Em casos de infrações graves, reincidência ou prejuízos à instituição, o usuário será submetido a um processo disciplinar, podendo resultar em expulsão (para alunos) ou outras medidas cabíveis.
4. **Ações Legais:** A instituição poderá tomar medidas legais em casos de crimes cibernéticos ou danos materiais e morais, conforme a legislação brasileira.

2.8 Revisão da Política

Esta política será revisada e atualizada anualmente ou sempre que houver mudanças significativas na infraestrutura tecnológica ou nas necessidades de segurança da instituição.