Estações de trabalho institucionais

De acordo com a POLÍTICA DE USO ACEITÁVEL DE ESTAÇÕES DE TRABALHO DO IFSP:

Qualquer dispositivo computacional, de propriedade do IFSP e utilizado para acessar os recursos de TI da instituição, incluindo:

- **Desktops e Notebooks Institucionais:** Equipamentos de propriedade do IFSP, fornecidos aos usuários para o desempenho de suas atividades.
- **Dispositivos Móveis:** Smartphones e tablets, institucionais, que acessam contas e serviços do IFSP (e-mail, sistemas, etc.).

Este capítulo trará os principais pontos de atenção e de ações técnicas para fortalecimento da segurança cibernética das estações de trabalho institucionais:

- **As ações listadas nesta seção devem ser realizadas exclusivamente pelas equipes de TI locais (CTIs):**

- Segurança aplicada à estações de trabalho institucionais:

Segurança aplicada à estações de trabalho institucionais:

Os termos e ações descritas neste documento, não são taxativos e não isentam os responsáveis pela aplicação das ações, da leitura e compreensão integral da Política de Uso Aceitável de Estações de Trabalho do IFSP.

Para que os usuários tenham acesso às estações de trabalho, tais estações deverão estar previamente configuradas com os seguintes requisitos técnicos de segurança iniciais:

Princípio do Menor Privilégio:

Evitar que os sistemas operacionais das estações de trabalho institucionais sejam utilizados com privilégios de "Admin
padrão

A eleva
TI ou realizada por meio de uma conta administrativa separada e de uso pontual.

Criação de contas individuais:

Usuários distintos no sistema operacional para cada pessoa, mantendo a obrigatoriedade de definição de uma senha individual e intransferível.

Contas Microsoft (Windows): Desabilitar a opção que permite o uso de contas Microsoft de usuários em sistemas Windows, priorizando contas de domínio ou locais.

Bloqueio automático de Tela Obrigatório:

Em ambientes institucionais **sugere-se o tempo de 10 minutos de inatividade;**

Em ambientes públicos ou compartilhados **sugere-se o tempo de 5 minutos de inatividade;**

Segurança Avançada:

Estações de trabalho institucionais utilizadas por servidores que, devido às suas atribuições, necessitem de acessos para gerenciamento de infraestruturas ou a sistemas e dados institucionais classificados como críticos ou confidenciais, deverão

ser configuradas e mantidas pela equipe de TI em conformidade com as seguintes diretrizes de segurança avançada:

Criptografía de Dispositivo: A criptografía de de dispositivo, seja disco completo ou específica do sistema operacional (ex: BitLocker para Windows nas versões PRO, FileVault para mac OS, LUKS para Linux, etc) deve ser obrigatoriamente ativada para proteger os dados em repouso em caso de perda ou roubo do equipamento, especialmente em notebooks.

Softwares Antivírus/Antimalware e Firewall:

Manter softwares antimalware/antivírus, nativo do sistema operacional ou de terceiros, instalados e atualizados em dispositivos institucionais (fixos e móveis), realizando varreduras frequentes.
Habilitar o firewall do sistema operacional da estação de trabalho.

Hardening do Sistema Operacional e de outros softwares:

As configurações padrões do sistema operacional e de outros softwares nele instalados devem ser revistas e fortalecidas, o que inclui a desativação de serviços e portas de rede desnecessários e a remoção de softwares não essenciais.

Navegadores em Estações em todos os cenários:

Manter navegadores de internet sempre atualizados.
Impeça o usuário de instalar extensões;

Navegadores em Estações de Uso Público/Compartilhado:

Definir políticas de segurança rígidas para navegadores de internet em estações públicas, compartilhadas ou em ambientes de laboratório:

Impeça o usuário de salvar senhas;
Impeça o usuário de instalar extensões;
Impeça o usuário de preencher campos automaticamente;
Impeça o usuário de reter históricos;
Impeça o usuário de sincronizar contas;
Configurar para exclusão automática de dados de navegação (histórico, cookies, dados de cache) ao final de cada sessão ou ao fechar o navegador.
A cada logout, reinício, desligamento do sistema operacional os dados do navegador sejam removidos;
Forçar o uso de abas anônimas em ambientes onde isso é tecnicamente possível.
Priorizar o uso de perfis de "convidados" ou modos efêmeros.

Gestão de Ativos de Softwares:

Impedir a instalação de softwares não autorizados, não licenciados ou com finalidades que possam oferecer riscos à segurança cibernética, integridade ou imagem da instituição.
Em nenhuma hipótese faça uso de softwares ou sites ilegais.
A instalação de softwares em dispositivos institucionais é atribuição exclusiva do setor de TI local.

“Congelamento” de sistemas:

Utilização de softwares de "reset/congelamento de sistemas" em ambientes de estações públicas e laboratórios pode auxiliar a evitar o reaproveitamento não autorizado dos conteúdos, reverter comprometimentos e alterações de configurações.

Uso de Diretiva de Grupos (GPOs):

Utilize Diretivas de Grupo (GPOs) para forçar restrições nas estações de trabalho.

Controle de Acesso Remoto:

Remover, desabilitar e/ou impedir a instalação de softwares ou serviços de acesso remoto nos sistemas operacionais das estações institucionais de modo geral, como por exemplo SSH / RDP / WinRM / VNC / TeamView / AnyDesk e outros softwares de terceiros.

Filtrando e impedindo o tráfego dessas aplicações na entrada, saída e entre vlans, utilizando para isso o firewall local do s.o. e o firewall da rede.
Se necessário, o acesso remoto deve ser restrito a usuários técnicos, com tráfego de origem exclusivo das redes das equipes de TI.

É importante ressaltar que muitos desses softwares possuem apenas licenças comerciais e seu uso sem o devido licenciamento é ilegal.

Redes e Compartilhamentos:

Desabilite diretivas de compartilhamento inseguro entre estações de trabalho:

Protocolos legados:

Remoção de protocolos de compartilhamento legados, como o SMBv1 (vulnerável, descontinuado e utilizado frequentemente em ataques de ransomware). Caso ainda haja serviços locais que dependam deste protocolo, eles devem ser descontinuados o mais rápido possível;
Verificação da exsitência de outros protocolos vulneráveis de compartilhamento.

Compartilhamento Anônimo:

Impedir o sessões anônimas ou de visitantes para acesso a compartilhamentos;
Desativar a opção de compartilhamento sem senha;
Desativar o compartilhamento de pastas públicas;
Desativar a descoberta de rede;
Em ambiente de estações compartilhadas ou de uso público, desative o compartilhamento de arquivos e impressoras e faça o mesmo em outros ambientes em que os compartilhamentos locais não são necessários.

Segmentação de redes:

Verifique as regras definidas em seu firewall de rede, mantenha a segmentação das redes através de VLANs e filtre o tráfego entre elas por serviços.

Com atividade prática para analisar os serviços acessíveis entre vlans, utilize um host linux que será conectado a cada VLAN, uma de cada vez, e execute: ***sudo nmap -v -Pn -p- --open [ip/16 da rede interna do campus]****. Esse procedimento permite identificar os serviços acessíveis entre VLANs, cabendo julgamento de deveria ou não estar acessível e tomar as providências.*

Controle de Tráfego:

Verifique as regras definidas em seu firewall de rede e fique atento às portas de rede liberadas e aos tráfegos de entrada e saída.

Via de regra, a recomendação é de que apenas serviços essenciais (DNS, DHCP, HTTP, HTTPS, NTP) tenha conexões conexões permitidas. Valide as regras de entrada, saída e entre vlans da sua rede.

Wi-Fi Seguro:

Na arquitetura de redes wifi, prefira protocolos de criptografia fortes e seguros para a autenticação dos usuários e o tráfego de rede. Recomendados minimamente WPA2 ou superior (WPA3).
Cada usuário deve ter suas credenciais individuais e intransferíveis de acesso à rede.
Crie redes específicas de acordo com o público alvo e a sua finalidade. Destine redes específicas, segmentadas com controle de acesso de usuários e de dispositivos. Isso evita a propagação de ataques e explorações laterais que podem dar acesso a dispositivos ou dados sensíveis.

Outras informações e boas práticas em redes wi-fi, podem ser encontradas na página da ETIR/IFSP, na aba “Publicações Técnicas” > “[Guia Técnico ETIR/IFSP #10] Boas práticas de segurança nas configurações de redes wireless ”

Conexões Bluetooth:

A conexão Bluetooth do dispositivo deve ser mantida desligada quando não estiver em uso e configurada como "não detectável" para evitar conexões não autorizadas.

Redes Hotspot:

É VEDADA a criação de um ponto de acesso sem fio (hotspot) a partir de redes institucionais para conectar uma estação de trabalho institucional ou quaisquer outros dispositivos.

Desative a funcionalidade de hotspot das estações de trabalho institucionais

Conexão de equipamentos:

É expressamente VEDADA a conexão de equipamentos de rede particulares (roteadores, switches, repetidores) ou não homologados pela ANATEL à infraestrutura de rede do IFSP.

Excepcionalmente, dispositivos voltados exclusivamente para estudos e pesquisas, poderão ser conectados à rede do campus, desde que autorizados e acompanhados pela equipe de TI local. Nesses casos, deverão ser aplicadas configurações específicas de isolamento de rede e monitoramento ativo de tráfego, garantindo que tais dispositivos não tenham acesso às demais redes institucionais.

Nos casos onde não for possível o isolamento do equipamento, a equipe de TI local poderá negar o acesso e conexão do dispositivo.

Monitoramento e vigilância:

Fique atento a comportamentos anômalos nas estações institucionais e no tráfego de rede de entrada e de saída.

Ferramentas Institucionais para monitoramento do seu tráfego de rede:

Logs do seu firewall de rede;

Monitoramento do tráfego de rede através da plataforma: https://monitoramento.ifsp.edu.br

Em breve estará disponível na página da ETIR/IFSP, na aba de Publicações Técnicas, o “[Guia Técnico ETIR/IFSP] Análise de tráfego anômalo”, fique

atento!

Controle de periféricos:

As portas USB das estações de trabalho institucionais devem ser utilizadas exclusivamente para finalidades institucionais, conectando apenas dispositivos confiáveis.

Periféricos de armazenamento:

Implementar políticas de restrição ao uso de dispositivos de armazenamento removíveis (pen drives, HDs externos, etc.) para mitigar riscos, conforme o nível de risco da atividade do usuário e do ambiente onde a estação está inserida. Tais riscos envolvem, mas não se limitam a: infecção por malwares, acessos não autorizados e roubo de dados e credenciais.

Outros tipos de periféricos

É vedado conectar a equipamentos institucionais qualquer dispositivo ou periférico USB (incluindo, mas não se limitando a, pen drives, HDs externos, teclados, mouses, adaptadores e carregadores de celular) de origem desconhecida, não confiável ou duvidosa.

É vedado conectar dispositivos desconhecidos encontrados, recebidos como brindes de fontes não verificadas ou emprestados de terceiros sem garantia de procedência representam um risco de segurança elevado e não devem ser conectados.

Esta vedação se deve ao risco de ataques do tipo "BadUSB", nos quais um periférico aparentemente inofensivo pode executar comandos não autorizados, instalar malware, capturar informações digitadas ou comprometer a segurança da estação de trabalho e da rede institucional.

Registro de logs e eventos:

As configurações de auditoria e registro de logs de segurança do sistema operacional devem ser ativadas para permitir a análise e a investigação de incidentes de segurança, e o IFSP se reserva o direito de registro de tráfego em sua rede interna, ou nas tentativas de acesso à infraestrutura do IFSP.

Fim da vida útil da estação de trabalho:

Equipamentos e mídias que contenham Dados Institucionais e que chegaram ao fim de sua vida útil devem ser entregues exclusivamente ao setor de TI da unidade, que garantirá a destruição segura e permanente dos dados antes do descarte ou alienação do ativo.

Encerramento de vínculo ou alterações de alocação do usuário:

Compete à chefia imediata e ao setor de TI local garantir que os procedimentos de devolução de estações e remoção de acessos ou alteração de permissões sejam cumpridos antes da finalização do processo de encerramento do vínculo do usuário com determinada área, setor, projeto ou com a instituição.
Sejam vínculos de sistemas locais ou a formalização da solicitação de interrupção de acesso a sistemas institucionais em que não possua autonomia para interrupção do acesso, via chamado técnico.