GUIA DE BOAS PRÁTICAS PARA USO DOS EQUIPAMENTOS DE TIC

Este documento apresenta as regras estabelecidas pela Superintendência de Tecnologia da Informação (STI) para orientar aos usuários de TIC da UFPE quanto ao uso e conservação dos equipamentos de TIC sob seus cuidados.

ORIENTAÇÕES GERAIS

1. Em caso de incidentes (mal funcionamento, dano, inutilização do equipamento) deverei comunicar imediatamente à STI, através da Central de Serviços de TIC/CSTIC (http://cstic.ufpe.br/ ou pela ramal 7777);
2. Estando os equipamentos em minha posse, estarei sujeito à auditoria sem prévio aviso;
3. É vedado ao usuário abrir os computadores e monitores para qualquer tipo de reparo. Cabe ao usuário notificar à STI (via CSTIC) quando qualquer problema for identificado;
4. É vedado utilizar equipamentos e informações para outros fins, que não sejam atividades ligadas à instituição;
5. É vedado retirar ou danificar licenças/placas identificadoras de patrimônio afixadas nos computadores e periféricos ou travas e lacres de segurança disponíveis em tais equipamentos;
6. Por fim, é vedado ao usuário do computador e itens relacionados, realizar quaisquer atividades que estejam em não conformidade com as normas e políticas de tecnologia da informação e comunicação (TIC) vigentes na UFPE.

ORIENTAÇÕES PARA USO DOS MICROCOMPUTADORES NA UFPE

Diante das facilidades oferecidas pelo acesso dos recursos da Tecnologia da Informação (TI) e tendo como objetivo orientar aos usuários do nosso parque de computadores, disponibilizamos aqui algumas recomendações para otimizar a utilização de nossos equipamentos e serviços de acessos à internet na UFPE.

Boas práticas no uso dos recursos de TI partem do princípio do bom senso. A falta de prudência e os excessos cometidos no uso destes recursos podem terminar prejudicando outros usuários. Deve-se ter consciência sobre as

limitações e dependências dos recursos tendo por preocupação a utilização adequada das ferramentas disponíveis.

A seguir, algumas dicas de utilização adequada e segura dos nossos recursos.

1. Desligue o computador corretamente

Para evitar o corrompimento do sistema operacional e danos ao hardware, não desligue o computador puxando o cabo de força da tomada ou segurando o botão de *power*, pois algumas atualizações podem estar sendo instaladas e não devem ser interrompidas. Além disso, tal procedimento também poderá ocasionar a perda de dados e/ou os tornar irrecuperáveis.

2. Desligue ou suspenda o computador ao fim do expediente

Para garantir uma maior vida útil do equipamento mantenha-o desligado ou suspenso após o fim do expediente. Os componentes eletrônicos internos se deterioram com o passar do tempo devido à constante exposição a elevada temperatura interna.

3. Evite comer ou beber próximo ao computador

Mantenha o ambiente limpo para evitar o aparecimento de insetos. Líquidos podem gerar grandes problemas caso caiam nos circuitos elétricos de teclados ou mesmo do computador. Pense coletivamente!

4. Mantenha o sistema operacional e demais softwares sempre atualizados

Para garantir uma maior segurança e fluidez nas tarefas executados no computador, procure sempre manter o sistema operacional e outros softwares atualizados.

5. Mantenha o antivírus atualizado

Para garantir maior segurança na sua navegação online mantenha o antivírus sempre atualizado, tendo em vista que deixá-lo desatualizado poderá ocasionar infecção do computador e roubo de dados. Não ignore alertas de ameaças. Nunca remova o antivírus!

6. Não instalar softwares piratas

A instalação de softwares proprietários, sobretudo sistemas operacionais, sem a devida aquisição da licença pode ocasionar a abertura de brechas no sistema que facilitam a infecção do computador e roubo de dados, além de ser uma prática ilegal, prevista no código penal Art. 184 – "Violação de direitos autorais e os que lhes são conexos" sob pena de detenção de 3 meses a 1 ano ou multa.

7. Sempre deixe espaço livre no disco rígido

Procure sempre manter espaço livre no seu disco rígido para que o sistema operacional possa funcionar de maneira correta. Disco rígido com capacidade completa afeta diversos serviços do sistema operacional como, por exemplo, atualizações de segurança.

8. Realize backup dos seus dados com frequência

Mantenha sempre uma cópia atualizada dos seus dados. Isso pode ser feito de diversas maneiras (HD externo, pendrive ou em nuvem). Uma opção é a utilização do repositório para arquivos e documentos da UFPE, o Google Drive, disponível em: http://drive.ufpe.br/. **Mantenha suas operações ao máximo no Drive Online!**

9. Senhas são pessoais e intransferíveis

Troque suas senhas com frequência e faça uso de caracteres especiais, como / - @ # ! _, números e sempre alternando entre letras maiúsculas e minúsculas. Procure senhas que sejam fáceis de você lembrar, mas difíceis de serem descobertas por um terceiro. Quanto maior o número de caracteres mais seguro você estará. Jamais insira sua senha em sites não confiáveis nem as forneça a alguém, você será corresponsável por quaisquer ações realizados em seu nome.

10. Não acesse *Internet Banking* em computadores compartilhados e nem em redes de Wi-Fi públicas

Sobre hipótese alguma acesse o *Internet Banking* em computadores compartilhados por vários usuários, já que estes têm maior chance de estarem infectados por vírus. Evite também acessar seu *Internet Banking* utilizando redes de Wi-Fi públicas, já que o tráfego de informações em tais redes não são seguros e ficam expostos a potenciais *hackers*. Evite dor de cabeça!

11. Cuidado com links, e-mails e quaisquer notificações suspeitas

Nunca clique em algo sem antes ler e sempre questione a veracidade dos links, e-mails e notificações. Solicitações de atualização de cadastros bancários, alertas sobre conta bancária cancelada, propagandas prometendo aumento de desempenho do computador, sorteios e premiações, entre outros, são portas de entrada para o roubo ou sequestro das suas informações. Caso tenha dúvida, sempre solicite ajuda através da CSTIC.

12. Exclua arquivos pessoais de computadores compartilhados

Se você utiliza computadores compartilhados evite deixar quaisquer arquivos com dados pessoais na máquina. Exclua-os! Não deixe que outros tenham acesso às suas informações.

13. Não exerça atividades de cunho duvidoso

Não faça uso de mineradores de **criptomoedas** como Bitcoins ou semelhantes. Além de reduzir a vida útil do equipamento você estará arriscando infecções de malwares provenientes dos responsáveis pelo processamento dos programas. Além do mais, dificilmente você ganhará dinheiro.

Emitido em 28/09/2020

REGULAMENTO Nº 1/2020 - CGGT STI (11.29.04)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 28/09/2020 16:52)
CARLOS EDUARDO MEIRA DE MENEZES
DIRETOR
1133292

Para verificar a autenticidade deste documento entre em http://sipac.ufpe.br/documentos/ informando seu número: **1**, ano: **2020**, tipo: **REGULAMENTO**, data de emissão: **28/09/2020** e o código de verificação: **b916bae0c5**