

Nesta edição

- Conceito de boas praticas
- O que é Backup
- Detectar vulnerabilidade de Hardware e Software
- Dicas para uma navegação segura
- Formatar ou Restaurar
- Periféricos
- Passo a Passo

LINKS PERMANENTES

POSITIVO

Link de acesso para acionamento da garantia

POSITIVO

MULTILASER

Link de acesso para acionamento da garantia Multilaser

E-mail Corporativo da Educação

Acesse seu e-mail institucional da escola ou Pessoal

Portal SEI
Sistema Eletrônico de Informação

Acesse os Manuais e Procedimentos do NIT Núcleo de Informação e Tecnologia

Conceito das Boas práticas de segurança da informação e tecnologia

A origem da fechadura remonta a um passado distante, há milhares de anos. Depois dela, no decorrer da história, as ideias e tecnologias sobre segurança e privacidade foram se transformando. Com a revolução digital, isso tomou outra forma; a fechadura de ferrolho e gancho da Antiguidade vagarosamente deu lugar a novas proteções para um mundo abstrato: a internet – que, no entanto, pode impactar a vida humana tanto quanto qualquer outra coisa material. Por isso, atualmente, fala-se muito sobre **boas práticas de segurança da informação**.

Você tem conhecimento sobre os riscos a que todos nós estamos sujeitos no universo digital? Entende a importância da segurança da informação? Normalmente, quem não sabe sobre o assunto, busca saber mais; quem entende, busca implementá-la no lugar onde trabalha. Independentemente do grupo com o qual você se identifica entre esses dois, este artigo lhe mostrará a importância da segurança da informação e alguns passos práticos que sua instituição pode aderir.

Dito isso, veja a seguir boas práticas de segurança da informação para utilizar dentro da sua organização:

O que é Backup

Uma informação que é de conhecimento de todos hoje em dia é que depois do triste ataque ao World Trade Center em 11 de setembro de 2001, muitas empresas que funcionavam no local sofreram perdas irreparáveis, além de seus escritórios destruídos. Algo que nem todos sabem, no entanto, é que

SITES

SECRETÁRIA DA
EDUCAÇÃO

EFAPE

SED

CONTABILIZASP

GDAENET

ENTRE EM CONTATO COM O NIT

*Para solicitar agendamento
técnico, informações ou tirar
dúvidas ligue para:
(11) 3866-3800 /3866-3801
/3866-3802*

*E-mail
dectonit@educacao.sp.gov.br*

algumas dessas empresas puderam reestruturar o trabalho novamente pouco depois. Talvez você deva estar se perguntando o mesmo que muitos se perguntaram: “como eles conseguiram fazer isso depois de vivenciarem um acontecimento tão devastador?” A resposta é: por meio da restauração dos dados, que eram frequentemente armazenados em cópias de segurança.

O Backup, **também chamado de cópia de segurança**, é um importantíssimo recurso que ajuda na preservação dos dados em caso de roubos ou danos acidentais. Com esse mecanismo é possível recuperar rapidamente informações perdidas.



Ele pode ser armazenado em dispositivos físicos, como servidores de backup, pendrive e HD externo, ou em nuvem. O mais aconselhável é que sejam feitas, no mínimo, duas cópias das bases de dados, e guardadas em locais seguros e longe do escritório da sua empresa.

Detectar vulnerabilidade de Hardware e Software

Todo hardware (parte física de um computador) pode apresentar defeitos de fabricação, erros de instalação ou utilização, entre outros problemas. Da mesma forma, os softwares (sequência de instruções executadas em um computador) podem ter falhas técnicas e de segurança. Isso tudo pode comprometer a segurança da informação de um indivíduo ou organização.

Apesar disso, ao adquirir produtos tecnológicos, muitas pessoas e empresas levam mais em conta o valor a pagar do que os aspectos técnicos e a qualidade do equipamento, o que pode tornar vulnerável toda a infraestrutura e a segurança de informações.

Portanto, avalie sempre as possíveis vulnerabilidades de hardware e software, para a tomada rápida de providências, caso seja necessário.

Dicas para o uso consciente e seguro da internet

1 - Verificar e Atualizar

Verifique as configurações de privacidade nas redes sociais e as atualize sempre que necessário. Não deixe dados pessoais acessíveis a desconhecidos.

2 Sites seguros

Utilize sempre que possível. Aqueles que possuem “**https**” (navegação criptografada), por exemplo, pois, são mais seguros.

3 Atenção aos “Termos e Condições”

Se não tiver tempo de ler todos os termos e condições quando realizar o registro em um site novo, recorra a ferramentas como **EULAlyzer**, por exemplo. Esse tipo de programa analisa as licenças.

4 Denuncie conteúdos impróprios

Todos são responsáveis por denunciar conteúdos impróprios encontrados na Web. **Faça a sua parte!**

5 Cuide dos seus dados pessoais

Lembre-se que as relações estabelecidas na internet merecem os mesmos cuidados do contato pessoal. Portanto, **não revele a estranhos informações pessoais, nem deixe seus dados salvos em conversas on-line ou e-mails.** Você pode perder dispositivos mobile ou ter algum tipo de desentendimento com a pessoa para a qual enviou tais informações.

6 Não compartilhe intimidades on-line

Se tiver algo de íntimo ou sigiloso para dizer a alguém e queira guardar segredo, fale pessoalmente, ou faça uma chamada. Sistemas de mensagens de texto, vídeo e áudio podem ser facilmente copiados ou compartilhados.

7 Pense antes de agir

É fundamental pensar antes de publicar qualquer conteúdo. **Controle o que e para quem pública.** Por exemplo, em algumas redes sociais você pode escolher o que pretende tornar público

e o que somente seus amigos podem ver.

8 Cautela e discricção

Evite fornecer endereços de lugares onde frequenta, mora ou estuda. Muito cuidado também com o Check-in.

9 Cuidado com estranhos

Evite fazer videochamadas com estranhos. Sua imagem pode ser manipulada, ser usada para montagens em situações humilhantes que podem ser divulgadas entre amigos e familiares.

10 Sua imagem é sua

Não se deixe fotografar em cenas comprometedoras, nem mesmo envie qualquer foto sua a terceiros. Por mais que confie em quem está recebendo o material, o conteúdo pode cair em mãos erradas.

11 Faça o registro de conversas e mensagens

Opte por gravar conversas quando se sentir ameaçado. Bloqueie o contato dos agressores no celular, chat, e-mail e rede de relacionamento.

12 Senhas fortes

Mesclando números, letras e outros caracteres. Não compartilhe suas senhas com ninguém. Não repita suas senhas e, caso precise armazená-las, que seja em local protegido. Serviços oferecem “tokens” no celular para dificultar roubo de senhas.

13 Mantenha segura sua rede

Coloque uma senha em sua rede Wi-Fi e troque a senha padrão do roteador.

14 Sistema atualizado e protegido

Instale um antivírus em seu computador e o mantenha devidamente atualizado. Habitue-se a manter as mais recentes atualizações disponíveis do fabricante do sistema operacional.

15 Segurança em todos os momentos

Bloqueie suas telas sempre que se ausentar do computador e acostume-se a fechar sua sessão ao utilizar computadores públicos, ou então, use o modo anônimo do seu navegador preferido.

16 Evite senhas em dispositivos de uso coletivo

Faça operações que envolvam senhas apenas em dispositivos

pessoais ou de uso individual.

17 Saiba como se proteger

Aprenda a deletar ou bloquear as informações do smartphone de forma remota, em caso de roubo, você pode manter seus dados seguros.

O que é Formatação de Computadores

Formatar o computador será a única solução para se livrar de certos problemas em sua máquina. Com o passar do tempo, os **computadores** costumam apresentar certas intermitências, que dificultam as atividades do usuário. É claro que esse não é o único fator que torna o funcionamento dos **computadores** falho.

As **condições de armazenamento, o tempo** e a **forma de utilização** também influenciarão nessa decisão. Por isso, é sempre importante tomar certos **cuidados com o seu computador**.

Quase sempre, em **situações muito críticas**, será necessário realizar a **formatação do computador**. Casos como **infestações de vírus, sequestro de dados** ou **pane geral** – a famosa **Tela Azul** da morte – são alguns exemplos.

Para evitar equívocos, é importante entender os principais **fatores que levam os computadores a serem formatados**.

Identificando alguns sinais, será mais fácil acionar a sua equipe ou **consultoria de TI** para solucionar o caso.

FORMATAR OU RESTAURAR?

Na prática, estes dois conceitos são bastante diferentes um do outro. Cada um deles é indicado para casos diferentes.

Formatar um computador implica em apagar totalmente o seu conteúdo, sendo necessário **reinstalar seu sistema operacional do zero. Imagens, fotos e documentos são eliminados**, e não podem ser recuperados novamente.

A **formatação** é um último recurso para solucionar os problemas dos computadores, caso nenhuma outra ação seja capaz de resolvê-lo. Principalmente em caso de **computadores** que já possuem mais tempo de uso.

O usuário também pode optar apenas por **restaurar o computador**. Essa é uma decisão menos radical, antes de pensar em **formatar a máquina**.

Nessa situação, o **sistema operacional voltará as configurações de fábrica iniciais** e os arquivos armazenados no dispositivo serão mantidos.

A **restauração** é indicada para máquinas com até 2 anos, que ainda estão em plena condição de uso. Essa é uma forma de fazer uma “limpeza”, que deixará o seu computador mais ágil novamente.

Quando Formatar um Computador ?

Existem dezenas de razões que **levam um computador a ser formatado**. Entre alguns dos motivos mais comuns estão:

- **Infestação de vírus** ou **sequestro de dados**;
- Venda e/ou doação do **computador** para terceiros;
- Pane geral do **sistema operacional**;
- **Lentidão** ao utilizar o **computador**;
- Quando a **restauração da máquina** não foi suficiente para resolver o problema.
- **Atualizações de sistema** malsucedidas.
- Troca de **hardware**.

NOTA IMPORTANTE

*Os Desktops, Notebooks e dispositivos utilizados nas dependências Administrativas e Pedagógicas das nossas unidades escolares possuem arquivos **próprios para realização da Formatação, fornecidos pela SEDUC através do NIT.***

*Para acessar esses arquivos clique no link [PASTA PROATEC](#) , escolha o arquivo de acordo com o **DISPOSITIVO** que irá ser Formatado.*

Lembre-se

Algumas aplicações são indispensáveis, independentemente de quem for utilizar a máquina, como **pacote Office, navegadores e driver, estes** serão instalados durante o processo sendo necessário apenas instalar driver da

impressora após a formatação.

Com base nas atividades para as quais o **computador** for destinado, outros **programas** serão necessários, para tanto será necessário a intervenção do NIT ou auxílio do PROATEC.

Outro ponto extremamente importante antes da **formatação**, é **realizar um backup completo de seus dados**.

Além de garantir a segurança de seus arquivos, caso haja algum contratempo durante a formatação, você poderá utilizar o **backup** para reiniciar o processo.

PERIFÉRICO

Na *informática*, um **dispositivo periférico**, ou simplesmente **periférico**, é um dispositivo externo auxiliar (ou acessório) usado para enviar ou receber informações do computador ligado à CPU (unidade central de processamento)^[1]

Existem três categorias de dispositivos periféricos, com base no seu relacionamento com o computador:

1. um *dispositivo de entrada* envia dados ou instruções para o computador, como mouse, teclado, scanner
2. um *dispositivo de saída* fornece dados de saída do computador, como monitor, projetor, impressora.
3. um *dispositivo de entrada/saída* executa simultaneamente as funções de entrada e saída, como um dispositivo de *armazenamento de dados* do computador.

Muitos dispositivos eletrônicos modernos, como *smartphones* e *relógios digitais* (que possuem conexão com a Internet), possuem interfaces que os permitem ser usados como periféricos de computadores.

Exemplos:

- e entrada: basicamente enviam informação para o computador: mouse, teclado, mesa digitalizadora, scanner de imagem, leitor de código de barras, controlador de jogo, caneta leve, microfone, câmera digital, webcam, dance pad, memória de somente leitura, manipulador eletrônico (*joystick*);

- De saída: transmitem informação do computador para o utilizador: monitor de vídeo, projetor, impressora, fones de ouvido e alto-falante;
- De processamento: processam a informação que a máquina (unidade central de processamento) enviou;
- De entrada e saída (ou mistos): enviam e recebem informação do computador: [monitor tátil](#), [drive](#) gravador de CD e DVD, [modem](#). Muitos destes periféricos dependem de uma placa específica, como no caso das caixas de som, que precisam da [placa de som](#);
- De armazenamento: armazenam informações do computador e permitem sua recuperação futura: [pen drive](#), [disco rígido](#), cartão de memória, etc.
- Externos: equipamentos que são adicionados a um periférico; equipamentos a parte que fornecem e/ou encaminham [dados](#).

Outras funções que são adicionadas ao processador através de cabos próprios: é o caso da [Internet](#), pela [placa de rede](#) ou um [aparelho roteador](#) (*router*).

Fonte Wikipédia

PASSO A PASSO

No `Passo a Passo desta edição vamos guiá-lo a realizar um teste de PING.

Mas o que é PING? O termo Ping é uma abreviação para **Packet Internet Groper**, termo em inglês que significa '**Medidor de pacote de internet**'.

O Ping é uma funcionalidade usada para **medir o tempo de envio e recebimento de dados** entre equipamentos conectados à mesma rede.

Também conhecido como **latência**, o Ping consegue testar se as máquinas estão disponíveis e recebendo os pacotes de dados, além de **analisar a qualidade da conexão**, ou seja, quanto tempo a rede leva para receber e enviar dados.

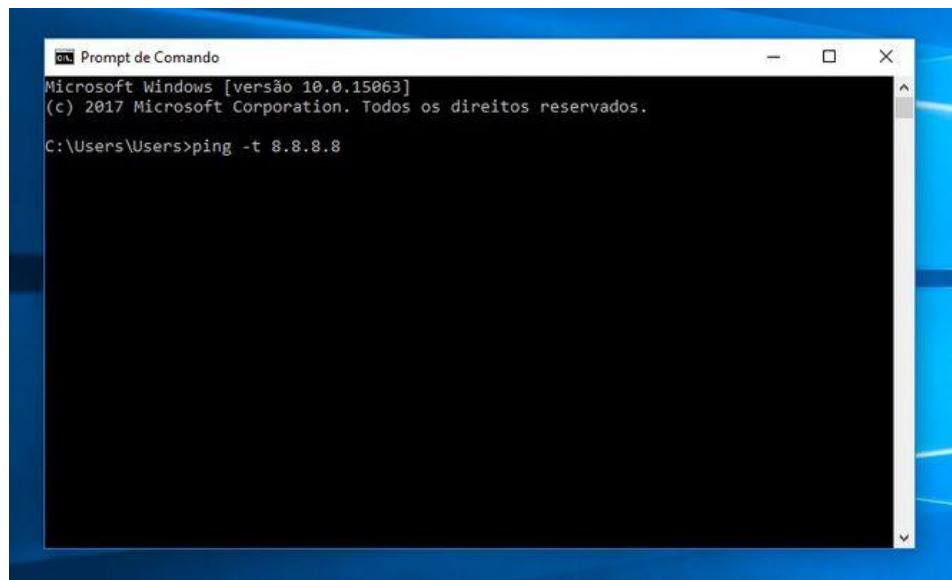
Vamos ao procedimento.

1º Passo

Abra o Prompt de Comando digitando na pesquisa "CMD" (não é necessário ativar as permissões de administrador) e utilize o seguinte comando (sem as aspas): "ping -t 8.8.8.8".

Teclle Enter para iniciar a análise de conexão.

Esse comando envia pacotes de dados para o servidor DNS do Google, que é um dos servidores com menor latência. Caso queira realizar o processo de ping em outro servidor, basta substituir o 8.8.8.8 por um endereço de sua preferência;

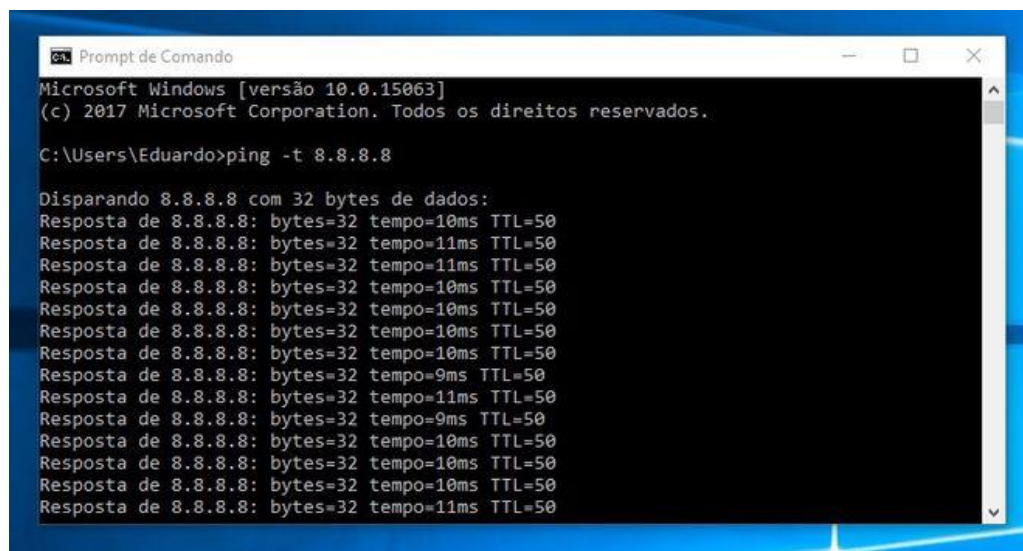


```
Microsoft Windows [versão 10.0.15063]
(c) 2017 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Users>ping -t 8.8.8.8
```

2º Passo

Ao iniciar o ping, o sistema dispara dados para o servidor, a cada segundo, para medir o tempo de resposta entre o envio e o retorno deles (em milissegundos).



```
Microsoft Windows [versão 10.0.15063]
(c) 2017 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Eduardo>ping -t 8.8.8.8

Disparando 8.8.8.8 com 32 bytes de dados:
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=9ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=9ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=50
```

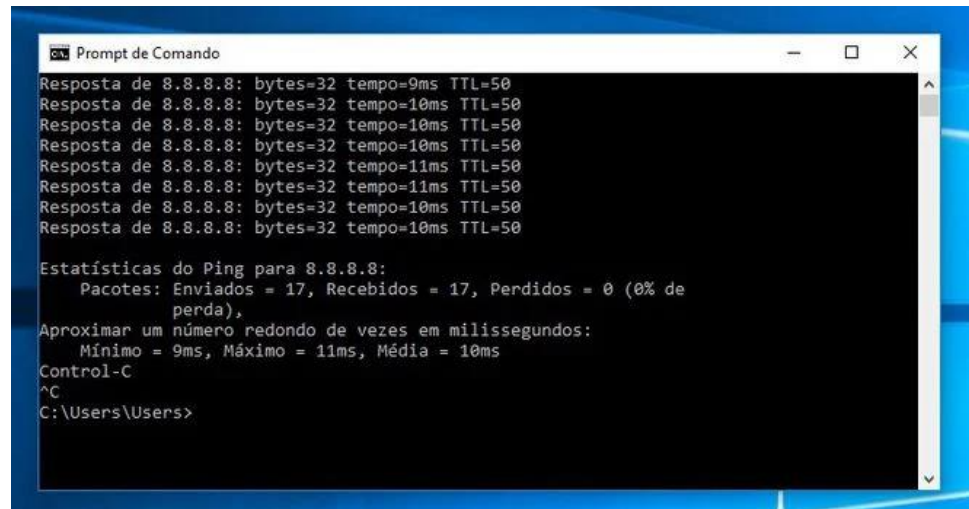
Ao iniciar o ping, o sistema dispara dados para o servidor, a cada segundo, para medir o tempo de resposta entre o envio e o retorno deles (em milissegundos).

Se a conexão apresentar instabilidade durante a análise, a seguinte mensagem será exibida na tela: **"Esgotado tempo limite do pedido"**. Caso a conexão com a internet seja interrompida por completo, o Prompt de Comando mostrará o erro "Falha gera".

3º Passo

Se você não receber nenhuma das duas mensagens de erros, atente-se aos valores indicados em "Tempo". Se o tempo de resposta variar muito entre um ping e outro, sua conexão pode estar com problemas de latência, o que pode ocasionar eventuais lags em jogos e quedas de qualidade ao ver filmes na Netflix ou no Youtube.

Para interromper o processo de ping, **pressione as teclas CTRL + C**. Feito isso, a ferramenta exibirá um relatório geral da análise nas últimas linhas. Você também pode verificar a taxa máxima e mínima de latência e qual foi a porcentagem de perdas de pacote durante o teste.



```
Prompt de Comando
Resposta de 8.8.8.8: bytes=32 tempo=9ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=11ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50
Resposta de 8.8.8.8: bytes=32 tempo=10ms TTL=50

Estatísticas do Ping para 8.8.8.8:
  Pacotes: Enviados = 17, Recebidos = 17, Perdidos = 0 (0% de
  perda),
  Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 9ms, Máximo = 11ms, Média = 10ms
Control-C
^C
C:\Users\Users>
```

Considerações Importantes

Ao testar a sua conexão com o comando ping, é preciso tomar cuidado ao relacionar o **tempo de resposta com a velocidade contratada** junto ao seu provedor, pois são aspectos completamente distintos. A velocidade da sua conexão afeta apenas a quantidade de dados que a sua máquina consegue transferir e receber em um intervalo de tempo, não influenciando, necessariamente, no tempo de resposta entre a sua máquina e o servidor.

Além de instabilidades no provedor de acesso à internet, outros fatores podem influenciar na variação do ping, tais como o uso de conexões por [VPN](#) e a utilização de roteadores para dividir a conexão com outras máquinas.