SEDUC
Secretaria de Estado
de Educação

Governo de
Mato
Grosso

Secretaria Adjunta de Gestão Educacional - SAGE
Superintendência de Políticas de Educação Básica – SUPEB
Superintendência de Políticas de Diversidades Educacionais – SUDE
Superintendência de Políticas de Desenvolvimento Profissional - SPDP
Superintendência de Políticas de Gestão Escolar - SUGE

Aprendizagem Conectada
Redação – 2020
PRÉ-ENEM DIGITAL

Prof. Sérgio Cintra
sergiocintraprof@gmail.com

Nome da Escola	
Nome do Estudante	
Ano/Ciclo	

Texto I

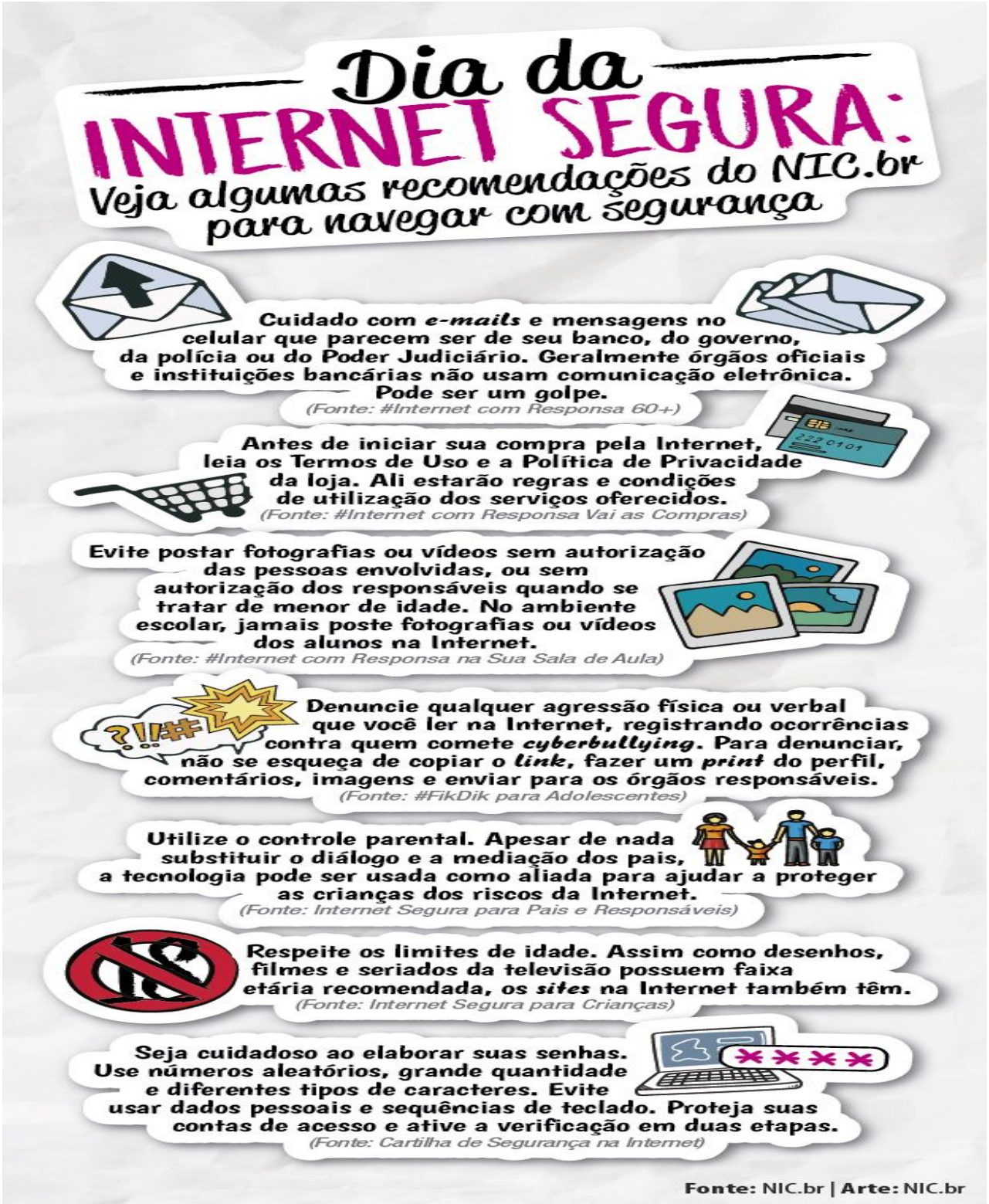
As redes sociais são legais, mas é preciso utilizá-las com segurança

Atualmente a internet é uma das grandes plataformas de conhecimento, entretenimento e interação entre as pessoas. Muitos usuários passam grande parte do dia conectados à rede mundial de computadores para esses fins. Com a chegada dos smartphones, *tablets* e outros dispositivos móveis, todos ligados a redes sem fio, o acesso se propagou ainda mais.

As redes sociais são um dos ambientes mais visitados pelos internautas quando o assunto é interação, compartilhamento e relacionamento, mas, para navegar nesses espaços virtuais, é preciso manter alguns cuidados relacionados à segurança.

https://blog.cancaonova.com/redacao/as-redes-sociais-sao-legais-mas-e-preciso-utilizar-com-seguranca/

Texto II



Disponível em: https://www.nic.br/noticia/na-midia/dia-mundial-da-internet-segura-especialistas-dao-dicas-de-navegacao/. Acesso em: 07 ago. 2020.

Texto III

Os usuários precisam entender que aqueles que agem de forma ilícita, como é o caso dos cibercriminosos, atacam três pilares básicos: sociedade em si, entidades públicas e, por fim, organizações privadas. Ainda que seja difícil conhecer integralmente as formas, seguras ou não, para o uso da internet, a educação digital deveria ser algo aplicado desde os anos iniciais das pessoas e perpassar toda sua vida, com acesso a atualizações constantes de informação, tanto numa perspectiva educacional quanto profissional.

O uso da tecnologia é um caminho sem volta e a internet não é utilizada apenas em dispositivos como computadores, *tablets* e *smartphones*. Já é encontrada em eletrodomésticos como televisores e geladeiras, e até mesmo em automóveis. A questão é que diariamente é alimentada por uma série de dados, inclusive aqueles mais sensíveis como informações bancárias. O fato é que ninguém deseja ser alvo de uma ameaça que deixe vulnerável a segurança da sua informação ou de pessoas e negócios relacionados a si. Eis, então, a necessidade de refletir sobre o uso da internet e o que deve ser feito para prevenir e manter a segurança dos dados.

https://canaltech.com.br/seguranca/o-que-torna-a-internet-insegura-109106/

Texto IV (usar como repertório sociocultural)

O que é segurança na internet?

Podemos entender como Segurança na Internet todas os cuidados que devemos ter para proteger as coisas que fazem parte da internet como a infraestrutura, que podem ser nossos computadores e as informações, que são as mais atacadas pelos cibercriminosos.

A segurança informática cria métodos, procedimentos e normas que buscam identificar e eliminar as vulnerabilidades das informações e dos equipamentos físicos, como os computadores.

Este tipo de segurança conta com bases de dados, arquivos e aparelhos que fazem com que as informações importantes não caiam em mãos de pessoas erradas.

Uma das melhores formas de se manter seguro na internet é usando antivírus nos computadores, por isso sempre recomendamos ter um instalado nos seus equipamentos.

Os principais riscos da Internet

Algumas das coisas que os cibercriminosos tentam fazer pela Internet são:

- Roubar informações
- Corromper informações
- Atacar sistemas ou equipamentos
- Roubar identidade
- Vender dados pessoais
- Roubar dinheiro

Os criminosos cibernéticos usam várias maneiras para atacar uma vítima na rede. Eles podem por exemplo, usarem vírus para tentar romper o sistema e alterar o funcionamento dos aparelhos eletrônicos. Outra modalidade é o *phishing*, onde o cibercriminoso se passa por uma pessoa diferente através de e-mails, mensagens instantâneas ou redes sociais, para conseguir informações confidenciais, como senhas\, números de cartões de crédito, e outros.

Como evitar?

Se alguém lida com muitas informações e possui vários equipamentos, como no caso das empresas, é melhor solicitar ajuda de profissionais que trabalham com segurança na Internet.

Por outro lado, como usuário comuns, podemos adotar várias medidas preventivas, tais como manter ativos e atualizados os antivírus em nossos aparelhos que acessam à Internet, evitar fazer transações financeiras em redes abertas ou em computadores públicos e verificar os arquivos anexos das mensagens de estranhos, evitando baixá-los se não tiver certeza do seu conteúdo.

Texto V (usar como repertório sociocultural)

Cuidados ao instalar um aplicativo

Não é segredo para ninguém que os aplicativos móveis são cada vez mais úteis, e em alguns casos têm se tornado uma necessidade. Com o avanço da tecnologia, ter um celular inteligente é cada vez mais simples e muitos deles já vem com muitos aplicativos instalados.

Com esses aplicativos fazemos transações bancárias, compramos produtos, reservamos viagens, nos divertimos com as redes sociais e jogos, e fazemos mais uma diversidade de coisas. Contudo, quando instalamos esses aplicativos, prestamos pouca atenção as permissões que nos pedem para que ele seja efetivamente baixado em nosso celular.

Sabia que quando instalamos alguns aplicativos fornecemos nossas informações a outras pessoas? Mostramos abaixo algumas permissões que podem pedir os aplicativos para serem instalados no seu celular. Observe:

Localização: Com esta permissão poderão ter informação detalhada de onde você está por meio do sistema GPS e também pela rede.

Armazenamento: Poderão alterar ou eliminar conteúdos de armazenamento USB, como por exemplo, as fotos que você tem salvas no seu celular.

Câmera: Com essa opção, permitimos que acessem a câmera para gravar vídeos e tirar fotos.

Suas Contas: O aplicativo poderá obter uma lista das contas que você criou usando seu aparelho.

Mensagens: Alguns aplicativos poderão ler suas mensagens de texto, editá-las e receber também as mensagens que você recebe.

Ferramentas do Sistema: Se você quiser por seu telefone no modo inativo, esta permissão poderia impedi-lo. Além disso, podem escrever a configuração e a sincronização e alterar o sistema global, como ativar e desativar o wi-fi.

Ferramentas de programação: Dando esta permissão, eles poderão comprovar o acesso a conteúdos protegidos.

Comunicação por rede: Neste caso, o criador do aplicativo poderá ver o estado da rede que você está conectado.

Cartão de apresentação: Permite o acesso aos dados dos contatos. Poderão escrever e ler os dados dos contatos. Também poderão ler os dados do perfil, informação confidencial e eventos do calendário.

Telefonemas: Esta opção permite aos criadores do aplicativo ler o estado do telefone, (se estiver falando por telefone ou não), o EMEI do aparelho e o número de identificação do telefone.

Serviços pagos: Permite que façam ligações a números telefônicos diretamente.

Proposta de Redação (Proposta inédita, elaborada por Sérgio Cintra)

A partir da leitura dos textos motivadores e com base nos conhecimentos construídos ao longo de sua formação, redija texto dissertativo-argumentativo em norma padrão da língua portuguesa sobre o tema "**Meios para garantir a segurança da informação na internet**", apresentando proposta de intervenção, que respeite os direitos humanos. Selecione, organize e relacione, de forma coerente e coesa, argumentos e fatos para defesa de seu ponto de vista.