BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

JUSTIÇA ELEITORAL
www.tre-es.jus.br | STI

BOAS PRÁTICAS
EM SEGURANÇA DA INFORMAÇÃO

JUSTIÇA ELEITORAL
www.tre-es.jus.br | STI

Material produzido pelo TRE-ES, com direito de uso cedido pelo Tribunal de Justiça do MS, em resposta ao Ofício STI nº 08/2018.

Secretaria de Tecnologia da Informação
Av. João Baptista Parra, 575, Praia do Suá
Vitória-ES • 29052-123
Geral (27) 2121-8500

SUMÁRIO

APRESENTAÇÃO

Esta cartilha tem a finalidade de apresentar os conceitos essenciais de segurança da informação no âmbito do Tribunal Regional Eleitoral do Espírito Santo (TRE/ES). Vamos entender melhor os conceitos de confidencialidade, integridade e disponibilidade relacionadas à proteção das informações.

VAMOS PROTEGER NOSSA INFORMAÇÃO?

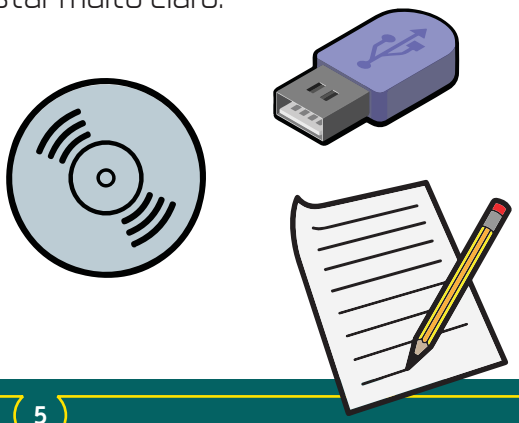
O que é uma informação de valor?

É toda estrutura de dados, organizada e significativa, que gera valor para nossa organização.

Sua manifestação independe de forma, ou seja, a informação poderá apresentar-se em formato impresso, digital (imagem, áudio) ou verbal, entre outros.

A informação afetada em sua confidencialidade, integridade ou disponibilidade poderá causar graves prejuízos ou danos à organização. Uma informação é considerada ativo intangível, ou seja, é um recurso que não pode ser medido de forma palpável.

Como organização, é muito importante que saibamos identificar uma informação de valor. Para protegê-la isso deve estar muito claro.



Por terem tanto valor, as informações poderão estar expostas a inúmeros riscos e ameaças, tais como:

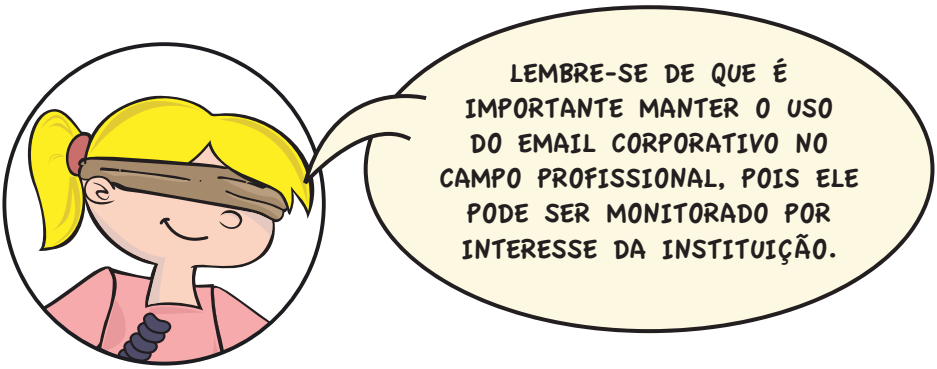
- ***Acesso indevido;***
- ***Furto;***
- ***Vazamento de informações críticas;***
- ***Ataques de hackers;***
- ***Fraude eletrônica;***
- ***Falsificação de identidade;***
- ***Dano a dados arquivados;***
- ***Uso indevido de imagem ou marca.***

USO DO E-MAIL

Todo magistrado, servidor e colaborador deve zelar pela segurança e confidencialidade das informações trafegadas e armazenadas nos e-mails corporativos.

Aliás, toda informação referente ao trabalho desenvolvido deverá tramitar pelo serviço de e-mail oficial oferecido pela STI, quando se tratar de mensagem de correio eletrônico.

Não é permitida a utilização de e-mails particulares ou criados em provedores gratuitos, como Hotmail, Gmail, Bol, entre outros, para enviar informações sensíveis referente ao nosso trabalho.



As mensagens enviadas ou recebidas através do e-mail corporativo poderão ser monitoradas, inspecionadas ou auditadas, com a finalidade de garantir o cumprimento de nossas políticas.

Não deve ser exibida, arquivada, distribuída ou editada qualquer mensagem ou arquivo anexo contendo conteúdo sexual, hacker, criminoso, pedófilo, racista, discriminatório e mensagens do tipo corrente.

Então, se você receber conteúdo inapropriado em seu e-mail, deverá imediatamente excluí-lo.

O hábito de ler sua caixa de e-mails diariamente e apagar os desnecessários, evita acumular mensagens eletrônicas. Ajude a STI a manter a boa qualidade do serviço de e-mail.

ACESSO À INTERNET

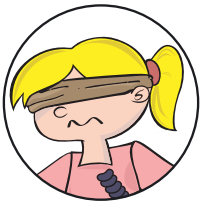
O acesso à Internet deverá ser somente para a execução das rotinas de trabalho de cada setor do TRE/ES.

Não é permitido acesso a sites de conteúdo inadequado ao ambiente de trabalho, como por exemplo, sites de conteúdo erótico, racista, homofóbico, discriminatório, hacker, entre outros.

O conteúdo de sites suspeitos pode trazer surpresas desagradáveis, tais como vírus, cavalos de tróia, espiões e outras pragas digitais. Assim, tome cuidado com o download de materiais pela Internet.

Todo acesso a páginas da Internet é registrado individualmente e monitorado.

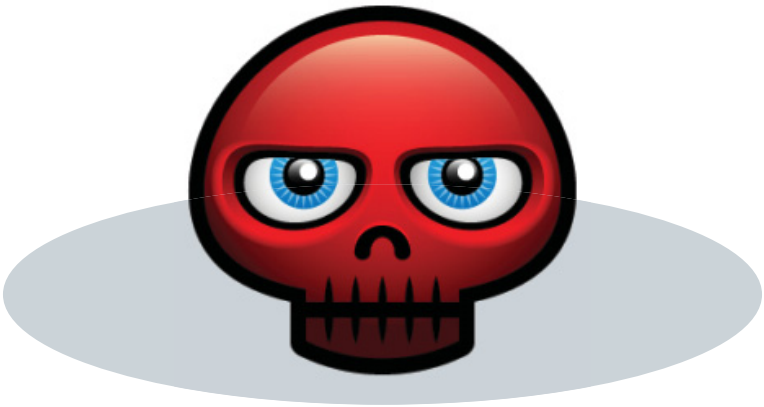
AMEAÇAS DIGITAIS
(VÍRUS, WORMS ETC.)



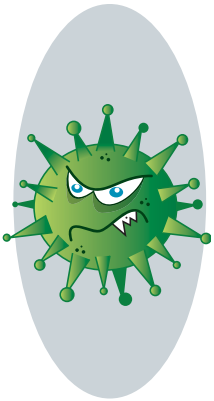
Falando em ameaças e pragas digitais, tome cuidado com o conteúdo enviado por e-mail ou acessado em sites na Internet.

Certifique-se de que a fonte é de boa procedência e não realize o download de qualquer arquivo na rede. Na dúvida, não faça!

Vírus, worms, cavalos de tróia, spyware, entre outras ameaças, geralmente se utilizam de técnicas furtivas para se propagar como, por exemplo, virem escondidos em arquivo que você acredita ser válido... como aquela foto de seu artista favorito.



Veja algumas definições:

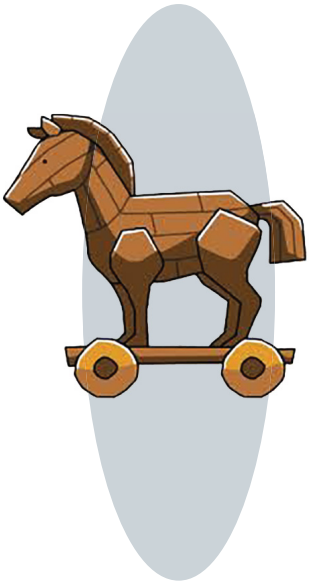


VÍRUS: programa de computador malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, é preciso que um programa já infectado seja executado pelo usuário.

WORM: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo, de computador para computador. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

CAVALO DE TRÓIA (TROJAN OU TROJAN-HORSE): programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem

o conhecimento do usuário. Geralmente, trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Esses programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.



SPYWARE: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima, quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

GOLPES VIRTUAIS

Cuidado com golpes virtuais, tais como e-mails contendo links para sorteio de prêmios, solicitações de recadastramento de CPF e de conta bancária, entre outros.

Tais golpes são conhecidos na Internet como pshising (algo como pescaria) e visa a "pescar" usuários descuidados e desinformados.

Ao acessar seu Internet banking, ou sites que exigem uso de senhas, verifique se há um pequeno cadeado no canto inferior, às vezes superior, de sua tela, assim como o uso do https no início da URL do endereço. Isso indica que o site é legitimo e possui segurança necessária para tramitar senhas.

POLÍTICA DA MESA E TELA LIMPAS

Nunca deixe sobre sua mesa papéis e documentos importantes enquanto você não está próximo. Alguém não autorizado pode acessá-lo.

Se for sair, guarde seus documentos e informações em gavetas ou armários, devidamente fechados com chave.

Além disso, outra boa prática é pressionar as teclas "WINDOWS + L" para travar a tela de seu computador quando você estiver fora. Isso evita que alguém não autorizado acesse indevidamente seu computador, enquanto você estiver longe de sua mesa.

USO DA SENHA

Sua senha é pessoal e intransferível, por isso, tome conta dela muito bem.

Não empreste sua senha ou a deixe visível em papéis anotados e colados em sua área de trabalho.

Crie uma senha forte. Geralmente senhas fortes são aquelas que misturam letras, números e caracteres especiais (como @,#,$,*) e têm, no mínimo, 8 caracteres.

Evite senhas que sejam associações simples, tais como, data de nascimento de filho ou cônjuge, nome de pai ou de mãe, nome de filhos, nome de cachorro e senhas padrões como 123, ou ainda repetições do nome do usuário.

Nunca passe sua senha a ninguém, nem mesmo a alguém que se identifique como da área de suporte ou da TI.

ENGENHARIA SOCIAL É O TERMO USADO PARA DEFINIR HACKERS DE PESSOAS. ESSES INDIVÍDUOS SÃO ESPECIALISTAS EM ENGANAR PESSOAS DESAVISADAS PARA OBTER INFORMAÇÕES PRIVILEGIADAS.

BOM USO DOS EQUIPAMENTOS

Somos responsáveis por cuidar bem dos equipamentos fornecidos pela área de TI para o nosso trabalho.

Computadores, notebooks, celulares e demais equipamentos fornecidos devem ser utilizados apenas para as nossas atividades funcionais.

SOFTWARES SEGUROS

Só utilize softwares autorizados pela STI.

Não instale software de origem duvidosa ou obtido em sites de compartilhamento de arquivos, como aqueles encontrados em blogs, 4shared, piratebay, entre outros.

USO DE PENDRIVES E OUTROS DISPOSITIVOS DE ARMAZENAMENTO MÓVEIS

Dispositivos de armazenamento móvel, tais como pendrives e cartões de memória, devem ser usados com cautela. Na necessidade de uso, consulte a STI.

Esses dispositivos são excelentes meios de proliferação de pragas digitais e devem ser evitados ao máximo.

Dispositivos de armazenamento móveis não deverão ser utilizados para transportar informações sensíveis, pois se forem extraviados, as informações poderão cair em mãos erradas. Pense nisso!

CELULARES E SMARTPHONES

Hoje, é muito comum o uso de dispositivos de telefonia móvel no ambiente de trabalho. Assim, devem ser utilizados com cautela.

Não utilize mensagens eletrônicas de aplicativos, como SMS, WhatsApp, Viber e outros para enviar mensagens sensíveis de sua unidade. Tais informações ficam extremamente expostas a vulnerabilidades como invasão a celular, extravio, entre outras.

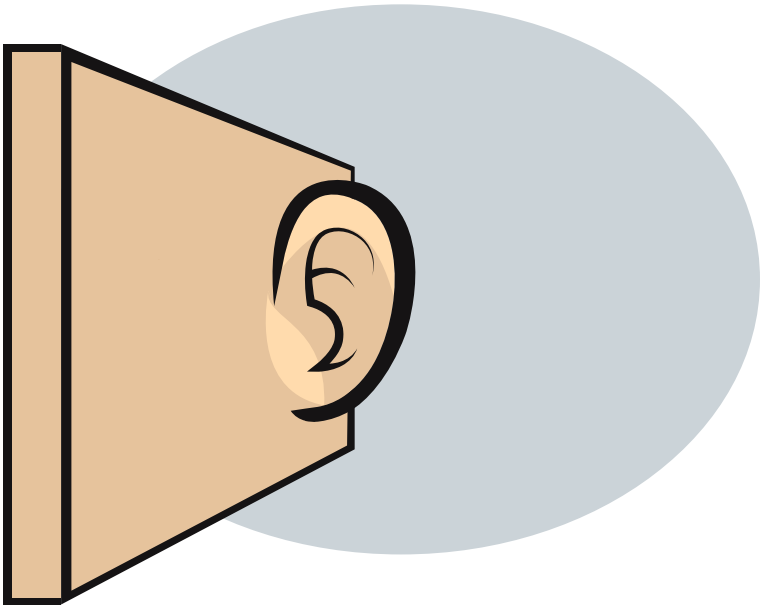
Cuidado para não deixar seu smartphone sem senha de bloqueio sobre mesas de reunião ou em locais públicos.

CUIDADO COM O QUE SE FALA

A informação encontra-se em diversos formatos. Mesmo em uma conversa falada, ela se manifesta.

Tome cuidado com a divulgação de informações críticas em ambientes públicos, tais como conversas em restaurantes, banheiros e corredores.

Tenha cuidado com o que se fala por aí. Como diz aquele velho ditado... "as paredes têm ouvidos"!



INCIDENTES DE SEGURANÇA

Incidente de Segurança é todo evento que pode, de alguma forma, expor nossas informações. Assim, uma invasão por hacker; contaminação por vírus; venda ou vazamento de informações; esquecimento de documentos confidenciais sobre mesas ou em impressoras, entre outros, deverão ser reportados pelo responsável daquele ativo de informação.

Nos casos graves, utilize a ferramenta de abertura de chamados (CESTIC) para registrar os Incidentes de Segurança, de modo que possam ser investigados e tratados conforme diretrizes da Política de Segurança da Informação da Justiça Eleitoral.

USO DE CERTIFICADOS DIGITAIS

O certificado digital é a forma eletrônica de comprovarmos a integridade e a autenticidade de documentos, garantindo validade jurídica.

Tome muito cuidado com seu token! Ele é pessoal e intransferível, tal como suas senhas pessoais. Não o empreste a pessoa alguma.

CONHEÇA A PSI DA JUSTIÇA ELEITORAL

A Política de Segurança da Informação da Justiça Eleitoral foi aprovada pelo TSE por meio da Resolução 23.644/2021, e é nosso documento de maior importância nesse contexto, trazendo diretrizes paraa produção das normas de segurança, no âmbito dosTribunais Regionais Eleitorais. Por isso, é importanteque você esteja sempre atualizado em sua leitura.

No TRE/ES, existem, ainda, outras normas de Segurança da Informação (NSIs) que tratam detalhadamente de assuntos específicos relacionados ao tema, tais como a NSI - 001 - Acesso à Internet, a NSI - 002 - Acesso à Rede sem Fio, a Resolução TRE/ES nº 114/2018 - Acesso à Informação e Classificação da Informação , NSI - 003 - Controle de acesso físico, NSI 004 - Uso de aplicativos de mensagens, entre outras. É nossa obrigação estar ciente dessas normas, e colocá-las em prática.

VAMOS JUNTOS CONSTRUIR UM AMBIENTE MAIS CONSCIENTE E SEGURO!

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

JUSTIÇA ELEITORAL
www.tre-es.jus.br | STI

PODER JUDICIÁRIO DE MATO GROSSO DO SUL