BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 03 – Março/2020

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA
E-Ciber

O Decreto nº 10.222, de 5 de fevereiro de 2020, aprovou a Estratégia Nacional de Segurança Cibernética (E-Ciber), que traz dez Ações Estratégicas para que o País se torne mais forte no ambiente digital e nossa sociedade possa usufruir de um espaço cibernético mais seguro, mais confiável e mais democrático.

A E-Ciber surgiu para enfrentar o seguinte cenário, perigoso e ameaçador:

- **o Brasil ocupa o 66º lugar em tecnologia da informação e comunicação no ranking da Organização das Nações Unidas – ONU;**
- **apenas 11% dos órgãos federais têm bom nível em governança de TI;**
- **em 2018, o Brasil teve mais de setenta milhões de vítimas de crimes cibernéticos;**
- **em 2018, 89% dos executivos foram vítimas de fraudes cibernéticas;**
- **em 2018, os crimes cibernéticos resultaram em mais de US$ 20.000.000.000,00 (vinte bilhões de dólares) de prejuízo; e**
- **o Brasil é o 2º país com maior prejuízo com ataques cibernéticos**.

Com a E-Ciber, instituições públicas e privadas passam a ter uma ideia clara do que o governo pretende fazer nessa área estratégica, e podem planejar para alcançar objetivos mais claros e concretos.

EVENTO: CONHECENDO A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA (E-CIBER)

Participe

Dia: 19 de março de 2020

Neste evento, serão apresentados os principais pontos da E-Ciber, em uma visão prática e com ênfase na Administração Pública Federal.
Inscrições: https://suap.enap.gov.br/portaldoaluno/curso/861/

SEGURANÇA NO CARREGAMENTO DE CELULAR EM LOCAIS PÚBLICOS

As estações para **carregar o celular** com entradas USB têm-se tornado mais comuns nos aeroportos ou outros locais de grande circulação de pessoas. No entanto, elas podem representar um grande risco para a sua privacidade.

Hackers podem instalar um *malware* (*software* malicioso) **nas entradas de USB**. Quando você conecta o celular, o vírus se instala no seu aparelho ou faz o *download* dos seus dados.

Como se proteger

1. Levar o seu próprio carregador e plugá-lo em uma tomada, visto que, em uma entrada USB pública, não temos ideia de quem a usou e o que ali transitou;

2. Usar baterias portáteis, também conhecidas como carregadores portáteis;

3. Usar bloqueador de dados para entradas USB conforme figura; e

4. Desligar o celular para carregar, caso não consiga executar os itens 1, 2 ou 3.

Você sabia que — ao serem submetidos ao processo de habilitação e credenciamento de segurança para o tratamento da informação classificada — os órgãos devem possuir área de acesso restrito denominada **Posto de Controle**?

O Posto de Controle é o local onde são armazenadas e controladas as informações classificadas, em qualquer grau de sigilo, no âmbito de uma unidade de órgão público ou entidade privada e visa manter a segurança lógica e física das informações classificadas, que são aquelas imprescindíveis à segurança da sociedade e do Estado.

Para saber mais sobre esse assunto, consulte as normas do Gabinete de Segurança Institucional da Presidência da República – Instrução Normativa nº 02, de 5 de fevereiro de 2013 e Norma Complementar nº 01, de 27 de junho de 2013, por meio do link: http://dsic.planalto.gov.br/assuntos/publicacoes-1

Fonte: http://dsic.planalto.gov.br/ https://www.ctir.gov.br/

Editorial/redação/diagramação: DSI Sugestões: asscom.dsi@presidencia.gov.br

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO

GABINETE DE SEGURANÇA INSTITUCIONAL

PÁTRIA AMADA BRASIL GOVERNO FEDERAL