BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 11 – Dezembro/2020

Ataque *hacker* – O que é e como se proteger

Quando se fala em ataque cibernético, sempre nos deparamos com o termo *hacker*. *Hacker* é um delinqüente, pessoa que se utiliza de meio ardiloso para explorar vulnerabilidades de sistemas ou descuidos de usuário, para obter ilicitamente dinheiro ou outra vantagem. O *hacker* age sozinho ou se organiza em grupo.

Muitos usuários acabam sendo vítimas desse tipo de cibercriminoso com sérias conseqüências para seus patrimônios, suas famílias, suas empresas e suas vidas.

Tenha um antivírus

Instalar um *software* antivírus é o item inicial para cuidar da segurança cibernética durante as atividades de navegação e de utilização de computadores, em casa ou no trabalho.

É necessário manter o programa sempre atualizado, com a versão mais recente instalada.

Utilize a verificação em duas etapas

A verificação em duas etapas, um recurso muito comum em redes sociais, *e-mails* e outros serviços de conta *online*, é uma proteção a mais, além da senha forte, e pode ser implementada em diversas aplicações como as de redes sociais e as de mensagens. Basta procurar nas configurações "verificação em duas etapas" e seguir os passos específicos para cada uma dessas aplicações. É uma medida simples que pode evitar muitos problemas.

Lembre sempre!!!

— Suspeitar de *e-mail* desconhecido! Não clicar em nenhum *link* nele contido!

— Não baixar arquivo de fonte desconhecida e não-segura!

— Suspeitar de anúncio muito atrativo, muito vantajoso! Não clicar nele! Pode ser armadilha e lhe trazer péssimas consequências!

Revisão dos normativos do Departamento de Segurança da Informação

Como escrevemos em edições anteriores, **o DSI é o órgão do Governo Federal responsável por elaborar normativos e requisitos metodológicos sobre assuntos relacionados com a atividade nacional de segurança da informação, no âmbito da administração pública federal.** Desde 2008 até o final de 2019, publicamos três Instruções Normativas e vinte e duas Normas Complementares.

Com a publicação do Decreto nº 10.139, de 28 de novembro de 2019, que determina a revisão e a consolidação de todos os atos normativos inferiores a decreto, editados pelos órgãos e pelas entidades da administração pública federal direta, autárquica e fundacional, iniciou-se o processo de revisão e consolidação dos normativos de segurança da informação do GSI.

Desde o início deste ano até o momento, foram publicadas três Instruções Normativas (IN) e revogadas uma Instrução Normativa e três Normas Complementares (NC). Para tanto, contamos com a colaboração dos órgãos da administração pública federal, que têm enviado importantes contribuições.

Dentre as novas INs publicadas, duas são resultantes do processo de revisão e de consolidação e uma é nova, elaborada para dispor sobre requisitos mínimos de segurança cibernética que devem ser adotados no estabelecimento das redes 5G.

➡ **Ressalta-se que as NC permanecem vigentes até o ato específico de sua revogação, mesmo se vinculadas a uma IN já revogada.**

➡ **Lembramos que o cumprimento das Normas é obrigatório para toda a administração pública federal, sendo necessário o acompanhamento da alta administração de cada órgão.**

Os normativos do DSI podem ser encontrados no nosso site em:

• **Instruções Normativas:**

https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao

• **Normas Complementares**:

http://dsic.planalto.gov.br/assuntos/editoria-c/normas-complementares

Fonte: https://www.gov.br/gsi/pt-br/assuntos/dsi https://www.ctir.gov.br/

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

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO

GABINETE DE SEGURANÇA INSTITUCIONAL

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 11 – Dezembro/2020

Proteja os equipamentos que seus filhos usam!

Qualquer dispositivo eletrônico com acesso à rede, utilizado por seus filhos, pode ser infectado por código malicioso (*malware*). Isso pode comprometer os dados gravados. Ele pode ficar lento e até parar de funcionar. Por isso, é importante que você tome alguns cuidados.

• Mantenha o equipamento seguro: realize todas as atualizações, e mantenha os aplicativos instalados com as versões mais recentes.

• Instale e mantenha atualizados mecanismos de segurança, como antivírus e *firewall* pessoal.

Alguns sistemas possuem recursos que permitem que o equipamento seja localizado à distância e que, para funcionar, é necessário a sua ativação. Esse serviço pode ser bastante útil para o caso de perda ou furto do equipamento, e para você saber onde seu filho está. Mas é necessário ter cautela! Quando o serviço de localização está ativado, outros aplicativos, como de redes sociais, podem ter acesso ao local onde está a criança, e postar, automaticamente, essa informação. Utilize sistemas que permitem configurações específicas por aplicativo.

Se você optar por ativar esse serviço, verifique — antes! — quais aplicativos terão acesso à localização do seu filho, e desabilite os que você não desejar.

Fonte: https://internetsegura.br

Contrato Sigiloso

Falamos em edições anteriores sobre os procedimentos previstos para o correto tratamento da informação classificada.

Você sabia que, no âmbito da administração pública federal, para a celebração de contrato sigiloso, medidas de segurança devem ser observadas?

A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada, em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é condicionada à assinatura de **Termo de Compromisso e Manutenção de Sigilo (TCMS**) e ao estabelecimento de cláusulas contratuais que prevejam, no mínimo, os seguintes requisitos:

• obrigação de manter sigilo relativo ao objeto e a sua execução;

• possibilidade de alteração do objeto, para inclusão ou alteração de cláusula de segurança não estipulada previamente;

• obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

• identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso à informação classificada, em qualquer grau de sigilo, e a material de acesso restrito;

• obrigação de receber inspeções para habilitação de segurança para o tratamento da informação classificada e sua manutenção; e

• responsabilidade em relação aos procedimentos de segurança relativos à subcontratação, no todo ou em parte.

Além disso, compete aos órgãos e entidades públicas, com que os contratantes mantêm vínculo de qualquer natureza, adotar procedimentos de segurança da informação classificada em qualquer grau de sigilo ou do material de acesso restrito em poder dos contratados ou subcontratados.

Para saber mais informações sobre esse assunto, ou outras informações sobre segurança da informação, acesse:

https://www.gov.br/gsi/pt-br/assuntos/dsi

Fonte: https://www.gov.br/gsi/pt-br/assuntos/dsi https://www.ctir.gov.br/

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