BIM
Comunicar para Educar

Boletim Informativo Mensal – Abril/2021 – Ano 2 – Nº 15

Segurança na Internet para Crianças e Adolescentes

As crianças não percebem o mundo *online* como uma nova tecnologia. Para eles, esse mundo sempre existiu. É necessário explicar quais são os riscos que existem e o que pode ser seguido para a proteção no ambiente da internet. Não se trata apenas de proibir, ou restringir, uma atividade, mas de fazer com que eles compreendam a razão pela qual devem ser cuidadosos.

Converse com os seus filhos sobre algumas dicas de segurança:

1.ensine que eles devem adicionar e aceitar apenas solicitações de pessoas conhecidas pessoalmente;
2.oriente que, ao participarem de conversas/*chat online*, devem interagir apenas com pessoas que a família conheça;
3.explique porquê publicar informações pessoais na internet deve ser evitado;
4.antes de permitir que seus filhos tenham seus próprios endereços de *e-mail*, avise-os sobre *e-mails* suspeitos, converse sobre *phishing*;
5.peça que tenham cuidado ao compartilharem fotos e vídeos pessoais (da família e de amigos, também);
6.deixe claro para eles que as senhas precisam ser mantidas em segredo, exceto para os pais;
7.fale sobre o perigo de fazer amizade virtual com estranho! Seja taxativo com seus filhos - encontro presencial com pessoa desconhecida não pode ocorrer; e
8. atenção aos comentários! Eduque-os, para que não publiquem algo de que possam se arrepender mais tarde!

Cuidados ao Realizar Transações Online

Realizar pagamento online tornou-se uma opção bastante comum nos dias atuais. A praticidade, a rapidez e o conforto oferecidos pelos meios digitais, são os grandes motivos que levam ao uso dessa modalidade, como meio de transação comercial. Entretanto, com o crescimento do uso desse tipo de pagamento, aumentaram também os riscos de utilizá-lo.

Diante desse cenário, tenha prudência e atenção quando for realizar pagamentos online.

Seguem dicas de boas práticas a serem adotadas por todos nós:

- verifique se o estabelecimento fornece ambiente seguro, como certificações e/ou selos de segurança;
- busque por informações sobre o estabelecimento, como CNPJ, endereço, telefone, etc. Verifique o histórico de relacionamento com os clientes;
- não acesse site e loja a partir de e-mail não solicitado;
- prefira estabelecimentos que fornecem recursos variados em seu site, como atendimento online, descrição detalhada do produto e diferentes meios de pagamentos; e
- prefira fazer compra pelo site ou aplicativo oficiais das lojas.

Para saber mais sobre o tema, acesse o link abaixo:
https://canaltech.com.br/seguranca/aprenda-a-fazer-compras-online-de-forma-segura/

Visite também o Portal do Departamento de Segurança da Informação
https://gov.br/gsi/dsi

BIM
Comunicar para Educar

Boletim Informativo Mensal – Abril/2021 – Ano 2 – Nº 15

O Decreto Nº 10.641, de 2 de março de 2021, publicado recentemente, trouxe importantes aprimoramentos no Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a **Política Nacional de Segurança da Informação** (**PNSI**) e dispõe sobre a governança da segurança da informação. Destacamos abaixo **as alterações feitas no Decreto da PNSI**:

1. inclusão do Ministério das Comunicações na composição do CGSI e atualização do nome do Ministério da Ciência, Tecnologia e Inovações (art. 9º, XII-A e XIII);

2. remoção da exigência de que o membro do CGSI ocupe cargo em comissão, a fim de permitir maior flexibilidade na escolha de tal membro. Entretanto, ele(a) deverá ser agente público que possua atribuição para definir políticas ou normas relacionadas à tecnologia da informação ou à segurança da informação nos respectivos órgãos (art. 9º, §2º)

3. remoção da obrigatoriedade de que esse membro seja necessariamente o gestor de segurança da informação interno do órgão de que trata o art. 15, III (art. 9º, § 2º);

4. permissão para realização das reuniões do CGSI por meio de videoconferência (art. 9º, §5º). Todavia, o Decreto nº 10.416, de 7 de julho de 2020, já havia possibilitado isso por decisão do Coordenador do CGSI, **ad referendum** do Plenário;

5. adequação da vinculação administrativa do Departamento de Segurança da Informação (DSI) no âmbito do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) (art. 11). Lembrando que a Secretaria-Executiva do CGSI é exercida pelo DSI;

6. adequação da redação do **caput** do art. 12 de modo a compatibilizar-se com as competências do GSI/PR previstas no art. 10 da Lei nº 13.844, de 18 de junho de 2019;

7. formalização da competência específica do GSI/PR para articular-se com os centros nacionais de prevenção, tratamento e resposta a incidentes cibernéticos pertencentes a outros países (art. 12, X). Ressalta-se que o GSI/PR faz essa articulação há alguns anos, com base em competências mais abrangentes, por intermédio de seu Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov);

8. atualização do nome da Controladoria-Geral da União (art. 14);

9. inclusão da palavra "prevenção" em "equipe de prevenção, tratamento e resposta a incidentes cibernéticos" e em "Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo" (art. 15, VII);

10. remoção da obrigatoriedade de que o membro do comitê de segurança da informação interno aos órgãos ocupe cargo equivalente a DAS 5 ou superior (art. 15, § 2º);

11. por outro lado, inclusão da obrigação de que o gestor de segurança da informação seja designado dentre os servidores públicos ocupantes de cargo efetivo, empregados públicos e militares do órgão ou da entidade, com formação ou capacitação técnica compatível com as normas estabelecidas nos Decreto (art. 15, § 4º); e

12. adequação da redação do art. 18 de modo a compatibilizar-se com as competências privativas do GSI/PR previstas no inciso V do art. 10 da Lei nº 13.844, de 18 de junho de 2019, quanto à segurança da informação e à segurança cibernética no âmbito da administração pública federal.

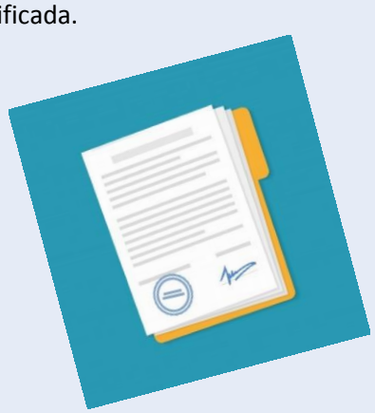
Identificamos, por meio das edições anteriores, **quem são autoridades que podem classificar informações**, bem como foram apresentadas **as informações passíveis de classificação**, cuja **divulgação ou acesso irrestrito podem pôr em risco ou prejudicar a segurança da sociedade ou do Estado.**

Vamos, hoje, **abordar algumas informações sobre o ato de classificação.**

De acordo com o **Art. 31, do Decreto Nº 7.724, de 2012**, a decisão de **classificar uma informação,** em qualquer grau de sigilo, **deverá ser formalizada no Termo de Classificação de Informação**, comumente **conhecido como TCI**, o qual deverá conter:

a)código de indexação de documento;
grau de sigilo;
b)categoria na qual se enquadra a informação;
c)tipo de documento;
d) data da produção do documento;
e)indicação de dispositivo legal que fundamenta a classificação;
f)razões da classificação;
g)indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final;
h)data da classificação; e
i)identificação da autoridade que classificou a informação.

O TCI seguirá anexo à informação e todas as informações acima deverão ser mantidas no mesmo grau de sigilo que a informação classificada.



Para saber mais sobre esse assunto, acesse:
http://gov.br/gsi/dsi

Fonte: **https://www.gov.br/gsi/dsi** **https://www.ctir.gov.br/**

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