BIM
Boletim Informativo Mensal
Comunicar para Educar
Ano 2 - Nº 17– Junho/2021

O que é Segurança da Informação?

Embora estejamos escrevendo sobre Segurança da Informação desde nossa primeira edição, consideramos importante escrever um pouco mais sobre o que é a Segurança da Informação.

Em edições anteriores, vimos que as ações de Segurança da Informação objetivam viabilizar e assegurar a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade das informações, e que esses quatro importantes princípios podem ser memorizados, por meio da palavra formada pelas suas letras iniciais (DICA).

Além de rever esse conceito, é importante destacar que, apesar de muitas pessoas acreditarem que Segurança da Informação está relacionada, apenas, à proteção do que está armazenado em equipamentos eletrônicos, ou do que é transmitido por meio digital, isso não é verdade.

A verdade é que Segurança da Informação é muito mais do que **proteção** digital. Ela se refere à proteção de todos os aspectos relacionados à proteção de informações e de dados, incluindo os que estão em papéis e até os que estão na cabeça das pessoas.

Ataque *ransomware* – O que é e como se proteger !

Quando falamos do contexto de **ataques cibernéticos**, o *ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso do usuário.

Agora que você já sabe o que é um *ransomware,* vamos ver dicas importantes de proteção que você pode adotar contra esses ataques e evitar passar por essa situação.

Tenha um antivírus

Ter instalado na máquina um *software* antivírus é o primeiro passo para cuidar da segurança durante a navegação *web*. Mantendo o programa atualizado em sua versão mais recente, ele poderá alertar caso você acesse um site suspeito ou baixe um arquivo não confiável. Com isso, é possível evitar com eficiência algumas dores de cabeça.

Ser cuidadoso ao clicar em *links* ou abrir arquivos

Uma dica simples de proteção contra *ransomware* é evitar acessar *links* oriundos de fonte desconhecida, e também evitar abrir arquivos cujos nomes não sejam de seu conhecimento. Isto é: na dúvida, não acesse! Consulte o profissional de segurança cibernética e da informação de sua corporação ou de sua rede de confiança.

Fazer *backups*(cópias) de seus arquivos regularmente

Uma ação simples que evita danos causados por *ransonware* é manter, em local separado e seguro, tais cópias, evitando o desespero de ter seus dados violados e perdidos definitivamente.

Para saber mais sobre esse assunto, acesse:

www.gov.br/gsi/dsi

Fonte: http://www.gov.br/gsi/dsi https://www.ctir.gov.br/
Editorial/redação/diagramação: ASSESI Sugestões: asscom.dsi@presidencia.gov.br

BIM
Boletim Informativo Mensal
Comunicar para Educar
Ano 2 - Nº 17 – Junho/2021

VOCÊ SABIA?

Você sabia que a celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção, cujo objeto ou execução contenha informação classificada, é condicionada à assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS)?

Além disso, devem ser estabelecidas cláusulas contratuais que prevejam os seguintes requisitos:

- obrigação de manter sigilo relativo ao objeto e à 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 de 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 submeter-se à inspeção para habilitação de segurança e sua manutenção; e
- responsabilidade pelos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

Aos órgãos e entidades públicos, com os quais os contratantes mantêm vínculo de qualquer natureza, caberá adotar procedimentos de segurança da informação classificada, ou do material de acesso restrito, em poder dos contratados ou subcontratados.

O modelo do Termo de Compromisso de Manutenção de Sigilo (TCMS) encontra-se no anexo I do Decreto nº 7.845, de 14 de novembro de 2012.

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

O que é *Phishing*

É uma tentativa de fraude pela *internet* que utiliza "iscas". Isto é, artifícios para atrair a atenção de uma pessoa, e fazê-la realizar alguma ação, na tentativa de obter dela dados pessoais e financeiros.

Saiba como se proteger de um possível *Phishing*

- Não abra *e-mails* de remetente com o qual não esteja familiarizado ou proveniente de fonte duvidosa.

- Caso você receba um *e-mail*, mesmo que seja de uma pessoa conhecida, não clique em nenhum *link, só* realize acessos manualmente .

- Revise suas contas regularmente e verifique atividade não autorizada.

Entenda os perigos da exposição de seus filhos nas redes sociais.

O que pode parecer inocente para você, pode não ser para um pedófilo. Tenha muito cuidado com a imagem infantil que posta ou compartilha, pois, infelizmente, nos últimos anos, os crimes sexuais contra menores aumentaram consideravelmente. Como as crianças não têm o controle sobre o que será postado, cabe aos pais ficarem atentos para garantir o respeito e a segurança da criança.

A grande questão da internet é a fácil disseminação de dados. Uma vez que o conteúdo se tornou público, não há possibilidade de controle de sua propagação. Por mais que a conta seja privada, não há garantia de que os seus seguidores sejam sempre bem intencionados.

Hoje, com o avanço da tecnologia e da internet, é comum vermos os pais compartilharem cada momento especial de seu filho. Esse fenômeno é conhecido como *sharenting*, e isso pode ser um fator ruim para o futuro da criança, pois não é apenas algo que possa ser usado por pessoas mal intencionadas, mas podem servir para que a criança seja vítima de *bullying,* ou até mesmo virar motivo para "meme" e piada na internet. Isso poderá ser constrangedor em sua vida adulta.

O indivíduo tem direito de escolher o que será postado, e cabe aos pais, ou responsáveis, protegê-los, enquanto criança, de vulnerabilidades. Isso evitará possíveis constrangimentos. Tenha bastante cuidado com o que compartilha, ou posta, sobre imagem infantil.

Para proteger as crianças brasileiras contra essa prática, a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no ano de 2019, estabelece, em seu Artigo 14, que os dados das crianças e adolescentes devem ser coletados e tratados "em seu melhor interesse". Ou seja, um dos pais, ou o responsável legal, deve consentir a coleta e o uso dos dados da criança em *games* e redes sociais e, ao completar 18 anos, ela poderá decidir se quer apagar os dados da plataforma.

Evite postar, ou compartilhar, foto de crianças em banho ou com pouca vestimenta. O que parece fofo para você, pode ser deturpado por outros. Tenha bastante cuidado! Não poste foto da rotina de seus filhos, como escola ou lugares que eles frequentam regularmente.

O direito de imagem é de personalidade, pertence ao indivíduo. A criança é a titular e o adulto, o guardião, mas sempre no melhor interesse dos filhos.

Fonte: http://www.gov.br/gsi/dsi https://www.ctir.gov.br/
Editorial/redação/diagramação: ASSESI
Sugestões: asscom.dsi@presidencia.gov.br