BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 19– Agosto/2021

Grau de Exposição nas Mídias Sociais

As mídias sociais fazem parte da vida de quase todas as pessoas. Elas criaram um espaço para a livre circulação de ideias, informações e opiniões de maneira ágil. O ser humano tem uma necessidade natural de se conectar, de ser visto. Ama as curtidas, os comentários. As redes sociais estimulam a sensação de ser importante para alguém, por conta das visualizações recebidas nas postagens. Essa interpretação leva a publicar cada vez mais dados pessoais.

A exposição na rede deve ser tratada com cautela, pois existem pessoas que podem usar suas informações para lhe fazer mal. Hábitos que parecem inofensivos, como realizar um *check-in* em um restaurante, pode se tornar algo bastante perigoso.

Lembre-se!

- Uma foto é capaz de revelar os locais que você frequenta; a localização exata da sua casa; a escola onde seu filho estuda; bens que você possui.
- Mesmo que seu perfil seja fechado, restrito, considere como se ele fosse aberto a todos. Configurações de segurança podem falhar e acabar expondo dados que você não pretendia disponibilizar.
- Fique atento, pois informações nas redes sociais são, em alguns casos, indexadas a ferramentas de busca online e facilmente rastreadas por terceiros.
- Ao adicionar pessoas de pouco contato (colegas, fornecedores casuais, conhecidos etc.), verifique o grau de exposição de seu perfil e implemente restrições, se necessário. Configure a rede social de forma adequada ao grau de intimidade que você mantém com cada pessoa ou grupo.
- Procure manter sua bolha virtual apenas com os indivíduos que você conhece pessoalmente.

É preciso tomar cuidado com a superexposição nas mídias sociais. O que está em jogo é muito mais do que algumas curtidas – é a sua segurança!

Instituição Formal da Rede Federal de Gestão de Incidentes Cibernético (ReGIC)

Em 19/07/2021, foi instituída a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), por meio da publicação do Decreto nº 10.748/2021, fruto de árduo trabalho do GSI/PR, em especial das equipes da CGGSI, do CTIR Gov e do DGES, bem como da SAJ/PR e de várias secretarias do Ministério da Economia, que detalha a governança dessa Rede e a forma como entidades de fora do Poder Executivo federal e organizações privadas poderiam participar dela.

A ReGIC está prevista na Política Nacional de Segurança da Informação (PNSI) e tem por finalidade manter e aprimorar a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional, para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação.

Para tanto, a ReGIC tem como objetivos:

- divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
- compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
- divulgar informações sobre ataques cibernéticos;
- promover a cooperação entre os seus participantes; e
- promover a celeridade na resposta a incidentes cibernéticos.

BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 19– Agosto/2021

Considerações Sobre o Uso de Rede *Wi-Fi* (sem fio) Pública

Atualmente, estabelecimentos como cafés, *shoppings*, aeroportos, hotéis, consultórios médicos e muitos outros oferecem a seus clientes acesso gratuito à internet, por meio de uma rede *Wi-Fi* pública.

A estrutura desse tipo de rede permite, sem restrição, várias conexões simultâneas, possibilitando aos mal-intencionados invadir para captura, exclusão ou alteração de dados de qualquer dispositivo conectado na rede. Poucas pessoas realmente entendem os riscos associados a esse tipo de conexão. Esta não é tão segura quanto pensamos – qualquer pessoa pode acessá-la, inclusive *hackers*.

Se houver a necessidade de conectar-se a este tipo de rede *Wi-Fi*, faça-o de maneira segura!
Tenha instalado e mantenha atualizado um programa antivírus em cada um dos seus aparelhos.

- Ao entrar em local público, que ofereça serviço de *Wi-Fi*, confira se a rede é legitima: procure pela placa indicativa que menciona a rede e as instruções de acesso. Se você simplesmente visualizar a relação de *Wi-Fi* que aparece no seu dispositivo, pode terminar por conectar-se a uma rede falsa, criada por *hackers,* para capturar dados pessoais.
- Se tiver que realizar transações bancárias ou compras online, prefira utilizar o seu pacote pessoal de dados móveis de internet.
- Evite conectar-se a *sites* ou aplicativos em rede social, pelos quais os criminosos virtuais têm facilidade de capturar suas informações pessoais, senhas etc.
- Certifique-se de que o *site* a ser acessado possui o protocolo HTTPS, pois este transmite os dados por conexão criptografada.
- Caso esteja utilizando *laptop*, desative o compartilhamento de arquivos. Isso evita que outra pessoa, conectada à mesma rede, tenha acesso aos seus arquivos.

Cuidados e precauções nunca são demais quando se trata de segurança em rede sem fio pública.

Segurança da Informação Classificada

Os sistemas de informação são constituídos por programas e redes de computadores destinados a armazenar, processar e transmitir dados. Esses sistemas devem incluir algumas características de segurança para que possam ser utilizados para o tratamento de informação classificada.

Uma das características que um sistema deve apresentar para a transmissão de informação classificada é a utilização de canal de comunicação seguro*, que deve ser estabelecido no âmbito da rede corporativa, conforme previsto no § 1º do art. 38 do Decreto 7.845, de 14 de novembro de 2012.

O uso de certificado digital para garantir a autenticidade da identidade do usuário é outra funcionalidade obrigatória prevista no § 2º do art. 38 do Decreto 7.845, de 14 de novembro de 2012. Isso significa que os usuários somente terão acesso ao sistema por meio de um certificado digital, e não apenas de um nome de usuário e senha.

O sistema de informação também deve garantir que cada usuário terá acesso apenas às informações às quais foi autorizado, ou seja, deve implementar diferentes níveis de acesso, de acordo com o § 3º do art. 38 do Decreto 7.845, de 14 de novembro de 2012.

O armazenamento e a transmissão da informação classificada devem ser realizados de forma criptografada, seguindo os padrões e parâmetros de criptografia estabelecidos pela Instrução Normativa GSI Nº 3 - 6 de março de 2013 (disponível em https://www.gov.br/gsi/dsi)

Essas características visam a mitigar o risco de quebra de segurança da informação classificada.

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

* Canal seguro é qualquer via de comunicação que permita a transmissão de dados sem que ocorra o risco de interceptação, adulteração ou espionagem.

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

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