BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 23– Dezembro /2021

Como tornar a sua casa mais "*CIBERSEGURA*"

A chegada da tecnologia 5G no Brasil é mais uma oportunidade para a popularização da internet de alta velocidade. Desta maneira, *smartTV*, geladeira inteligente, ar-condicionado com controle pelo celular e outras maravilhas do nosso tempo começam a povoar nossa lista de desejos. Embora estes dispositivos possam melhorar a forma como vivemos e trabalhamos, vale a pena lembrar que tudo o que está ligado à Internet pode ser vulnerável a ataques cibernéticos.

Os usuários de equipamentos ligados à i*nternet* devem ficar atentos à segurança. Algumas medidas que podem ser tomadas para proteger a sua casa:

- implementar senhas para todos os seus dispositivos e certificar-se de que estas senhas sejam fortes, preferencialmente, ativar a autenticação de dois fatores (Ex: senha + código verificador), disponível na maioria dos dispositivos;
- verificar os seus aplicativos e baixar todos eles diretamente das lojas oficiais, como *Google Play, Apple App Store* ou fabricante do seu equipamento, pois é a forma mais segura de ter o aplicativo legitimo e suas atualizações;
- verificar as definições de privacidade das suas contas nas redes sociais, muito usadas como fonte para coleta de dados por *hackers*, selecionar os parâmetros que o deixe confortável sem se expor. Refletir cuidadosamente sobre as informações disponíveis e visíveis no seu perfil. As plataformas solicitam informações que você não é obrigado a fornecer; e
- quando disponíveis, ativar as atualizações automáticas de todos os dispositivos e criar cópias de segurança dos seus dados.

O ideal é separar os seus dispositivos profissionais, dos pessoais. O dispositivo utilizado para trabalho deve ter uso exclusivo para esse fim e ter aspectos de segurança mais rigorosos, na tentativa de minimizar as perdas em caso de comprometimento do equipamento.

Não deixe de conversar com seus familiares sobre o tema – uma casa com cultura de segurança cibernética é um ambiente mais "ciberseguro".

Fonte: Centro Nacional de Cibersegurança/Portugal – Guia de boas práticas
https://dyn.cncs.gov.pt/pt/boaspraticas/

Informação Classificada como RESERVADA

Em edições anteriores falamos dos graus de sigilo da Informação Classificada, quais sejam: RESERVADO, SECRETO ou ULTRASSECRETO.

Uma informação pode ser classificada como RESERVADA, quando for considerada imprescindível à segurança da sociedade ou do Estado, levando em conta o risco, ou o dano à segurança, e o prazo.

O prazo máximo de classificação da informação classificada RESERVADA é de até 5 anos. As autoridades que possuem competência para classificar nesse grau são aquelas com função de direção, comando ou chefia, do Grupo-Direção e Assessoramento Superior - DAS, nível DAS 101.5 ou superior, e seus equivalentes, consideradas as equivalências trazidas pela Lei nº 14.204, de 16 de setembro de 2021.

A competência para classificar no grau RESERVADO é prevista também para os agentes públicos que classificam informação no grau SECRETO E ULTRASSECRETO.

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

BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 23– Dezembro /2021

Ministros do Brasil e da Finlândia celebraram Memorando de Entendimento sobre cooperação na área de Segurança Cibernética

Um importante instrumento na relação entre países é o Memorando de Entendimento, pois, por meio dele, podem ser definidos mecanismos que possibilitem uma cooperação mais efetiva entre os países participantes.

Pensando na importância, não só deste instrumento, mas de todas as formas de cooperação internacional para o fortalecimento da segurança cibernética do País, destacamos hoje uma das ações estratégicas estabelecidas na Estratégia Nacional de Segurança Cibernética brasileira: ampliar a cooperação internacional do Brasil em segurança cibernética.

Em consonância com essa ação estratégica, o Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, General Augusto Heleno, assinou, em 9/11/2021, Memorando de Entendimento com o Ministério dos Transportes e Comunicações da República da Finlândia.

Com isso, os dois países pretendem facilitar a cooperação, trocando informações sobre incidentes cibernéticos e compartilhando as melhores práticas de segurança, de modo a promoverem interesses mútuos e um espaço cibernético mais seguro e resiliente para as instituições de Estado e para suas populações.

A segurança da informação em ambientes físicos

Estamos acostumados a associar segurança da informação aos ambientes virtuais, aos controles lógicos, à proteção de *softwares*, à criptografia de dados etc, mas só isso não é suficiente. A verdadeira proteção depende do equilíbrio entre a parte lógica e a parte física do ambiente.

É necessária a adoção de medidas que contribuam para a proteção dos ativos que representam valor para a organização, incluindo equipamentos e recursos humanos.

Atenção ao ambiente físico!

- Não deixe papéis com informações relevantes ou confidenciais expostos, mesmo que sejam *post-its* e rascunhos.
- Bloqueie o computador sempre que for se ausentar da sua mesa.
- Não fotografe o ambiente de trabalho. Você pode acabar expondo informações presentes em telas de outros computadores, quadros brancos, papéis etc.
- Ao final de reuniões, mantenha a sala limpa, verifique quadros brancos, *flip charts* e materiais impressos deixados sobre a mesa.
- Os dispositivos móveis, como *tablets*, *notebooks* ou celulares, utilizados em áreas externas ao ambiente de trabalho, devem ter películas de privacidade para restringir o campo de visão de tela, evitando que os dados sejam vistos e registrados por outros.
- Dentro das salas, o ideal é que os computadores sejam posicionados de forma que o ângulo de visão seja restrito, para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização.
- Ambientes com informações sensíveis devem ter acesso restrito e controlado. É importante que as áreas sejam separadas fisicamente e possuam controle de acesso, seja por biometria ou por crachá de proximidade.

Seguir as recomendações e procedimentos de segurança, principalmente, quando depende apenas da sua atitude, é o princípio básico de segurança. Informe-se se o seu órgão ou sua instituição possui uma Política de Segurança da Informação e a siga!

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