BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 08 – Setembro/2020

Gestor de segurança da informação

O gestor de segurança da informação é o profissional responsável pelas ações de segurança da informação no âmbito da organização. **Na administração pública federal, a designação deste profissional é mandatória.**

Cabe a ele – em ligação com a alta administração do órgão ou da entidade - definir de que forma a segurança da informação será tratada; é necessário planejar uma estratégia e monitorar o cumprimento dessas práticas.

Destacam-se:

- a promoção de divulgação das normas internas de segurança da informação a seus integrantes;
- o estímulo à capacitação e à profissionalização de recursos humanos em temas relacionados à segurança da informação; e
- o incentivo a estudos de novas tecnologias e de seus reflexos relacionados à segurança da informação.

Para facilitar acesso e fortalecer a cultura de Segurança, o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República disponibiliza em seu site uma compilação da legislação vigente a fim de subsidiar trabalhos de operadores, técnicos e juristas da área de Segurança da Informação. Acesse: http://dsic.planalto.gov.br/

ACESSO RESTRITO

Você sabia que é considerado **Material de Acesso Restrito** qualquer produto, matéria, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado?

O material que, por sua utilização ou finalidade, demandar proteção, terá o acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Alguns exemplos do que pode vir a ser considerado Material de Acesso Restrito:

- equipamentos, máquinas, modelos, moldes, maquetes, protótipos, artefatos, aparelhos, dispositivos, instrumentos, representações cartográficas, sistemas, suprimentos e manuais de instrução;
- armamentos e seus acessórios, as munições e os aparelhos, equipamentos, suprimentos e insumos correlatos;
- aparelhos, equipamentos, suprimentos e programas relacionados à tecnologia da informação e comunicações, inclusive à inteligência de sinais e imagens;
- recursos criptográficos; e
- explosivos, líquidos e gases.

Os órgãos ou entidades do Poder Executivo federal encarregados da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de elaboração de projeto, prova, produção, aquisição, armazenagem ou emprego de Material de Acesso Restrito deverão expedir instruções adicionais necessárias à salvaguarda dos assuntos a eles relacionados.

Para saber mais informações sobre esse assunto, ou outras informações sobre segurança da informação, acesse: http://dsic.planalto.gov.br/.

Segurança da Informação durante o teletrabalho: aja preventivamente!

A execução do teletrabalho, ou trabalho à distância (*work-from-home*), vem aumentando significativamente desde o início da pandemia de COVID-19. Seja no setor público, seja no privado, a força de trabalho global tem empregado computadores, celulares e redes de dados pessoais para atividades profissionais à distância.

Esta utilização implica riscos de segurança para as organizações e para os próprios profissionais, uma vez que redes e equipamentos residenciais não possuem, em geral, os mesmos recursos de proteção de dados que existem em ambientes corporativos.

Neste cenário, como se prevenir de ameaças cibernéticas e como manter seguras as atividades laborais? Confira a seguir algumas dicas.

- Mantenha atualizados o Sistema Operacional e as ferramentas de proteção como antivírus, *antimalware* e *antispyware*.
- Utilize apenas programas de acesso remoto (VPN) certificados pela administração da rede de sua corporação, utilizando autenticação de duplo fator e evitando instalar programas de terceiros em lojas de aplicativos.
- Esteja sempre atento às táticas de engenharia social destinadas a colher informações confidenciais. Cuidado com *e-mails* suspeitos (*phishing*). Uma técnica de defesa simples nestes casos é: quando se deparar com um *link*, pare e analise-o antes de clicar (PARE – PENSE – CLIQUE, ou NÃO).
- Não compartilhe *links* para reuniões remotas, videoconferências ou salas de aula virtuais em *sites* abertos ou redes sociais abertas.
- Não forneça nomes de usuário, senhas, datas de nascimento, dados financeiros ou informações de familiares em resposta a *e-mails* inesperados ou telefonemas suspeitos.
- Utilize senhas diferentes para serviços diferentes, ou seja, não use uma mesma senha para várias contas.
- Evite usar videoconferência para tratar de assunto sensível ou classificado; dê preferência a uma reunião presencial com os devidos cuidados.

A prioridade nesta crise global é permanecer fisicamente seguro e saudável. Estamos reaprendendo a viver e a trabalhar em ambientes diferentes do tradicional. Este novo cenário traz consigo riscos inéditos para a segurança da informação relacionada a pessoas e organizações.

Desta forma, é necessária uma atitude proativa e a adoção de um novo estilo de vida virtual seguro, que possibilite eficácia e segurança na execução de atividades profissionais, mesmo em ambiente doméstico.

Fonte: http://dsic.planalto.gov.br/ 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