BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 04 – Abril/2020

Você conhece os termos e conceitos de Segurança da Informação?

No Glossário de Segurança da Informação, você encontra 349 termos dentre os mais usuais e recorrentes sobre o assunto. O Glossário está em constante evolução com novos termos que vão surgindo. Ele foi publicado no Diário Oficial da União em 01/10/2019/Edição:190 / Seção 1/ Página 3, Portaria no 93, de 26 de setembro de 2019.

Confira no *link*: http://dsic.planalto.gov.br/arquivos/documentos-pdf/glossario_completo.pdf/view

Computação em Nuvem

Computação em nuvem é um tipo de serviço que permite ao usuário, independente de sua localização, acessar um conjunto de informações, ou utilizar recursos, que antes estavam disponíveis somente em um computador pessoal ou da organização, tais como recursos de armazenamento, programas de escritório, e outros aplicativos e serviços.

A computação em nuvem oferece benefícios, como economia e eficiência, sendo por isso cada vez mais utilizada, tanto pela Administração Pública Federal, quanto pela sociedade em geral. Porém, os riscos relacionados à segurança da informação não podem ser ignorados, de modo a proteger dados, informações e serviços. Nesse sentido, o Departamento de Segurança da Informação publicou, em 2018, a Norma Complementar nº 14, com o objetivo de estabelecer princípios, diretrizes e responsabilidades relacionados com o *tratamento da informação em ambiente de computação em nuvem*, nos órgãos e entidades da Administração Pública Federal.

A Norma Complementar nº 14 está disponível no link: http://dsic.planalto.gov.br/arquivos/documentos-pdf/NC_14_R01.pdf

Segurança no uso de redes *Wifi* em locais públicos

O *wifi* (rede de *internet* sem fio) em locais públicos (aeroportos, *shoppings* e outros) pode ser muito cômodo em viagem, quando, muitas das vezes, a rede do celular, *notebook* ou *tablet* não está disponível; porém, essas redes públicas podem oferecer sérios riscos para sua segurança *online*.

Como se proteger

1. **Antes** de sair de casa, ou de seu trabalho, verifique se o antivírus está atualizado, seja no *notebook*, seja no celular.
2. Quando disponível, prefira rede privativa, ou paga;
3. Não pense duas vezes em perguntar ao dono do lugar se aquela rede realmente pertence a ele;
4. Não digite nenhuma senha bancária;
5. Não permita a opção de salvar suas senhas;
6. Não habilite o compartilhamento de arquivos; um *hacker* pode transferir *spywares* maliciosos ao seu computador, copiar ou modificar seus arquivos;
7. Verifique o endereço dos *sites* que acessa; prefira sempre os que iniciam com HTTPS; e
8. Desligue o *wifi* depois de terminar seu acesso.

Você conhece quais são as responsabilidades do Gestor de Segurança e Credenciamento (GSC)?

Não !?

Bem, cabe ao Gestor de Segurança e Credenciamento, no âmbito do órgão público a que pertence:

- manter a qualificação técnica necessária à segurança de informação classificada;
- implantar controle e funcionamento dos protocolos de documentos classificados;
- zelar pela conformidade e pelo sigilo dos processos de credenciamento e habilitação;
- propor à Alta Administração normas para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restrito;
- gerir os recursos criptográficos das Credenciais de Segurança e dos materiais de acesso restrito; e
- assessorar a Alta Administração no tratamento de informações classificadas.

A competência do GSC está regulada pelo artigo 17 da Instrução Normativa nº 02 do GSI/PR. Para saber mais informações sobre esse assunto ou outras informações sobre segurança da informação acesse http://dsic.planalto.gov.br/

Fonte: http://dsic.planalto.gov.br/ https://www.ctir.gov.br/

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

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO

GABINETE DE SEGURANÇA INSTITUCIONAL

PÁTRIA AMADA BRASIL GOVERNO FEDERAL