BIM
Boletim Informativo Mensal
Comunicar para Educar
Outubro/2022 – Ano 3 – nº 33

Você já ouviu falar que a competência para *classificar* uma informação é diferente da competência para *tratar* a informação classificada?

Quem possui a competência para *tratar*, nem sempre, pode *classificar*!

Classificar uma informação é submetê-la, temporariamente, à restrição de acesso público, em razão da imprescindibilidade para a segurança da sociedade e do Estado.

A **competência para classificar** uma informação é condicionada à função exercida pela autoridade classificadora, de acordo com o grau de sigilo necessário (reservado, secreto e ultrassecreto).

Art. 27 da Lei de Acesso à Informação/LAI - Lei nº 12.527/2011

Tratar uma informação é produzir, receber, classificar, utilizar, acessar, reproduzir, transportar, transmitir, distribuir, arquivar, armazenar, eliminar, avaliar, destinar ou controlar informação classificada em qualquer grau de sigilo.

A **competência para tratar** a informação classificada é concedida, por meio de **Credencial de Segurança**, para a pessoa física que tiver a **necessidade de conhecer**.

O nível de acesso da credencial é sempre igual ao grau de sigilo da informação que a pessoa indicada necessita tratar.

5.1 e 5.2 da Norma Complementar nº 01/IN02/NSC/GSI/PR

É importante lembrar que a autoridade que classifica em determinado grau de sigilo, poderá tratar uma outra informação classificada neste mesmo grau, desde que seja observada a **necessidade de conhecer**. Caso precise tratar uma informação com o grau de sigilo acima daquele que ele pode classificar, será necessária a concessão da credencial adequada ao nível de acesso desejado.

Avaliação de Conformidade de Segurança da Informação

O processo de avaliação de conformidade de segurança da informação consiste em proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

Esse processo deve dispor de um plano e um relatório.

- Plano de verificação de conformidade - deverá conter, no mínimo:
  - as unidades a serem abrangidas;
  - os aspectos a serem observados para verificação da conformidade;
  - as ações e atividades a serem realizadas;
  - os documentos necessários para fundamentar a verificação de conformidade; e
  - as responsabilidades.
- Relatório de avaliação de conformidade - deverá conter, no mínimo:
  - o detalhamento das ações e das atividades realizadas com a identificação do responsável pela análise;
  - o parecer de conformidade; e
  - as recomendações.

Importante! A alta administração do órgão ou da entidade deverá apreciar e aprovar o relatório de avaliação de conformidade e encaminhá-lo ao gestor de segurança da informação; além de promover ações de capacitação para os agentes responsáveis pela avaliação de conformidade, visando ao aperfeiçoamento de seus conhecimentos sobre a legislação vigente relativa à segurança da informação.

Finalmente, vale destacar que este é mais um dos importantes processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. Com ele, concluímos a explicação dos processos previstos na IN GSI/PR nº 3/2021.

Phishing

Mantenha sempre seu Antivírus atualizado

O **antivírus** é o principal recurso de proteção contra as ameaças virtuais.

Cuidado com *Phishing* no *E-Mail*

Técnica em que o criminoso envia *E-mails* fraudulentos para induzir uma pessoa a abrir um arquivo malicioso ou um *link*.

As redes sociais tornaram-se o principal alvo de *phishing*.

HTTPS://

verifique se o endereço do *site* da página começa com "HTTPS" e não apenas como "HTTP". O "S" significa "seguro".

sites falsos, criados com a mesma identidade visual das empresas que fingem representar, têm o objetivo de fazer com que o usuário se sinta seguro em navegar. No entanto, quando a pessoa digita suas informações, elas são imediatamente coletadas pelos criminosos.

Teste seu Conhecimento em Segurança Cibernética!

1. Qual senha é a mais segura?

a) 12345678

b) LhH*45!

c) WPh9Ze9

2. Marque a alternativa errada.

a) Se tiver que realizar transações bancárias ou compras *online*, prefira utilizar o seu pacote pessoal de dados móveis de *internet*.

b) *ransomware* é um tipo de código malicioso que impede que você acesse o seus dados.

c) Você pode guardar seus *backups* apenas com serviços pagos disponíveis na plataforma do fabricante do dispositivo usado.

3. Marque a alternativa correta.

a) *software* de controle parental são ferramentas utilizadas para auxiliar na segurança das crianças e dos adolescentes na *internet.*

b) *O software* de controle parental é responsável por fazer a instalação de aplicativos e programas automático de fontes desconhecidas.

Respostas: 1.b - 2.c - 3.a

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