1NPC - Atividade Avaliativa

Aluno: Diego Xavier Tavares
Disciplina: Segurança e Auditoria
Prof.: André Alves Nogueira, MSc.
Entrega: 04/05/2020 (prazo máximo para ser postado no educacional.ciesa.br)
Valor: 10,0 (completo) **OBS:**

- O arquivo com as respostas deverá ser postado/enviado no CIESA Educacional: "educacional.ciesa.br/Home/Graduação/Portal acadêmico/Minhas Disciplinas" na tarefa "Avaliação_1NPC", em formato "pdf", devidamente **identificado** com o **nome do aluno**.

I Parte – Conceitos básicos de Segurança da Informação (aula 01)

01. Conceitue a tríade da Segurança da Informação.

02. Conceitue os aspectos adicionais da Segurança da Informação

03. Conceitue:
a) Ameaça
b) Vulnerabilidade
c) Ataque
d) Controle
e) Probabilidade
f) Impacto

II Parte – Ciclo de vida da Informação e Controle de Ativo (aula 02)

04. Conceitue, resumidamente, cada uma das fases do ciclo de vida da Informação:
a) Identificação
b) Obtenção
c) Tratamento
d) Distribuição
e) Armazenamento
f) Uso
g) Descarte

05. O que é um ativo de informação e como o seu valor é obtido?

06. Quais são as formas que podemos classificar os Ativos de Informação?

07. As informações do setor público recebem uma classificação especial quanto a Confidencialidade e podem pertencer a três níveis (ou graus). Conceitue cada um destes níveis.

III Parte – Espionagem Americana no Brasil

08. Assista o vídeo <https://www.youtube.com/watch?v=mRuYKaE_DSc> e faça um resumo abordando principalmente as ferramentas e técnicas utilizadas pela espionagem americana no Brasil e México. (no mínimo uma página e meia).

Respostas

1. Está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: **confidencialidade**, **integridade**, **disponibilidade**.

   confidencialidade: Garantia de que os dados protegidos contra o acesso indevido, bem como de usa privacidade, algumas das medidas sugeridas é o controle de acesso, autentificação das conexões e implementação de política de permissões especificas.
   integridade: Garantia de que os dados não sejam modificados ou destruídos, mantendo todas as suas características originais, algumas medidas sugeridas são o monitoramento de redes, fortes políticas de auditoria, sistema de detecção de intruso
   disponibilidade: Garantia de que os dados estejam acessíveis, para os usuários autorizados quando necessário, algumas medidas sugeridas são monitoramento de ataques DoS, manter backups atualizados, adoção de plano de continuidade dos negócios.

2. Em tese, existem 5 aspectos adicionais da Segurança da Informação, estes são: Autenticação, Não-Repúdio, Legalidade, Privacidade e Auditoria.

   Autenticação: Garantir que um usuário é de fato quem alega ser.
   Não-Repúdio: Capacidade do sistema de provar que um usuário executou uma determinada ação.
   Legalidade: O uso da tecnologia de informática e comunicação deve seguir as leis vigentes do local ou país.
   Privacidade: Capacidade de um sistema manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações.
   Auditoria: Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

3. **A) Ameaça:** É um evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso. As ameaças normalmente aproveitam das falhas de segurança da organização. Possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica.
   B) Vulnerabilidade: Falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente

explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema.

C) Ataque: Agente externo em ação busca obter algum tipo de retorno atingindo algum ativo de valor. Este pode ser: ativo, passivo ou destrutivo.

D) Controle: Prevenção contra ataques combatendo as vulnerabilidades.

E) Probabilidade: É possível medir tanto a vulnerabilidade quanto ameaças.

F) Impacto: O impacto de um incidente de segurança é medido pelas consequências que possa causar aos processos de negócio suportados pelo ativo em questão

4. **A) Identificação:** A identificação das necessidades torna a informação mais útil aos seus destinatários.
   B) Obtenção: Nesta etapa são desenvolvidos procedimentos para captura e recepção da informação proveniente de uma fonte externa, ou da sua criação.
   C) Tratamento: Antes de ser aproveitada é comum que a informação precise passar por processos de organização, formatação, estruturação, classificação, análise, síntese, apresentação e reprodução, com o propósito de torná-la mais acessível, organizada e fácil de localizar pelos usuários.
   D) Distribuição: Levar a informação até seus consumidores. A informação precisa chegar a quem necessita dela para tomada de decisão.
   E) Armazenamento: Momento em que a informação é armazenada seja em um banco de dados compartilhado, em uma anotação de papel posteriormente guardada em um armário, ou ainda, em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo. (SEMOLA, 2003).
   F) Uso: Na etapa de uso, os objetivos de integridade e disponibilidade devem receber atenção especial: uma informação deturpada, difícil de localizar ou indisponível pode prejudicar os processos decisórios e operacionais da organização. O uso legítimo da informação pode levar a requisitos de confidencialidade, destinados a restringir o acesso e o uso de dados e informação às pessoas devidamente autorizadas. (BEAL, 2008).
   G) Descarte: Quando uma informação se torna obsoleta ou perde a utilizada para a organização, ela deve ser objeto de processos de descarte que obedeçam a normas legais, políticas operacionais e exigências internas.

5. A ABNT NBR ISO/IEC 27005 (2011) define que “um ativo é algo que tenha valor para a organização”. O valor da informação é dado pela sua:
   Exclusividade: lei da oferta e procura.
   Autenticidade: precisas, completas, confiáveis e verificáveis.

6.

- Software.
- Físico.
- Serviços.
- Pessoas.
- Documento em Papel.
- Informação.

7.

Secretos: dados ou informações referentes: a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência, a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

Confidenciais: dados ou informações: que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

Ultrassecretos: Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, bem como das áreas e instalações onde tramitam.

8.

É uma reportagem publicada pelo jornal sobre a conexão brasileira da rede de bisbilhotagem internacional montada pelos americanos e revelada pelo ex-técnico da agência de segurança nacional americana, **Edward Snowden**.

Revela que funcionou na embaixada de Brasília, uma estação de espionagem onde trabalharam agentes americanos da NSA, a Agência Nacional de Segurança, e da CIA, a Agência Central de inteligência. Mas não é possível afirmar se o trabalho continuou depois desse ano por falta de provas.

Agulha no palheiro: o palheiro significa o volume imenso de informações que a espionagem americana tem acesso todos os dias, interceptando comunicações das redes de telefones, internets e dos servidores de e-mails e rede sociais, já a agulha é quem eles escolherem.
Como funciona: quando selecionado o alvo são monitorados os números de telefones, os e-mails e o ip (identificação do computador), e é chamado de 1 Pulo, toda comunicação do alvo com os assessores, 1.5 Pulo quando seus assessores conversam entre eles e 2.0 Pulos quando os assessores possuem comunicação com outras pessoas.

Mainway: é um banco de dados mantido pela Agência de Segurança Nacional americana (NSA) que contém metadados para centenas de milhares de milhões de chamadas telefónicas feitas através das quatro maiores operadoras de telefonia dos Estados Unidos: AT&T, SBC, BellSouth (as três agora chamadas AT&T) e Verizon.

Association: pega as informações que circulam nas redes sociais, depois vai para outro filtro o **Dshfire:** que busca por determinadas palavras chaves.

Sementes: endereço eletrônicos e números de telefones monitorados
DNI selectors: capazes de fazer uma varredura por todos os dados de navegação de um usuário na internet, incluindo seus e-mails. Captura tudo que o usuário faz na internet (e-mails e sites visitados)**.**