

# Sessão 2: Conceitos fundamentais em segurança da informação



As atividades desta sessão serão realizadas em sua máquina física (hospedeira).

#### 1) Listas e informações complementares de segurança

- 1. Visite e assine a lista de e-mail do CAIS/RNP:
  - https://memoria.rnp.br/cais/listas.php
- 2. Visite e assine as listas de algumas das instituições mais respeitadas sobre segurança no mundo:
  - http://www.securityfocus.com/archive/
  - http://www.sans.org/newsletters/
  - https://www.us-cert.gov/mailing-lists-and-feeds
  - http://seclists.org/

Você é capaz de dizer em poucas palavras a diferença entre as listas assinadas, principalmente no foco de abordagem?

- 3. O Cert.br disponibiliza uma cartilha com informações sobre segurança na internet através do link https://cartilha.cert.br/. Acesse o fascículo *Segurança na internet*. Você consegue listar quais são os riscos a que estamos expostos com o uso da internet, e como podemos nos prevenir?
- 4. Veja os vídeos educativos sobre segurança do NIC.BR em http://antispam.br/videos/. Em seguida, pesquise na Internet e indique um exemplo relevante de cada categoria:
  - Vírus
  - Worms
  - Cavalos de troia (trojan horses)
  - Spyware
  - Bot
  - Engenharia social
  - Phishing
- 5. O site <a href="http://www.antispam.br/admin/porta25/">http://www.antispam.br/admin/porta25/</a> apresenta um conjunto de políticas e padrões chamados de *Gerência de Porta 25*, que podem ser utilizados em redes de usuários finais ou de caráter residencial para:
  - · Mitigar o abuso de proxies abertos e máquinas infectadas para o envio de spam.
  - Aumentar a rastreabilidade de fraudadores e spammers.

Estude no que consiste e quais são os benefícios da gerência da porta 25, e responda: sua instituição tem políticas de mitigação para os riscos apresentados? Quais seriam boas medidas operacionais para detectar e solucionar problemas relacionados à porta 25?



## 2) Segurança física e lógica

- 1. Delineie, de forma sucinta, qual seria seu plano de segurança para uma empresa em cada um dos tópicos abaixo:
  - · Contenção de catástrofes.
  - Proteção das informações (backup).
  - Controle de acesso.
  - Garantia de fornecimento de energia.
  - Redundância.
- 2. Quantos níveis de segurança possui a rede da sua instituição? Quais são? Faça um desenho da topologia da solução.
- 3. Cite 5 controles que podemos utilizar para aumentar a segurança física de um ambiente.
- 4. Cite 5 controles que podemos utilizar para aumentar a segurança lógica de um ambiente.
- 5. Informe em cada círculo dos diagramas seguintes o equipamento correto para a rede, através dos números indicados a seguir, que proporcione um nível de segurança satisfatório. Justifique suas respostas.
  - 1. IDS
  - 2. Modem
  - 3. Firewall
  - 4. Proxy
  - 5. Switch
  - 6. Roteador

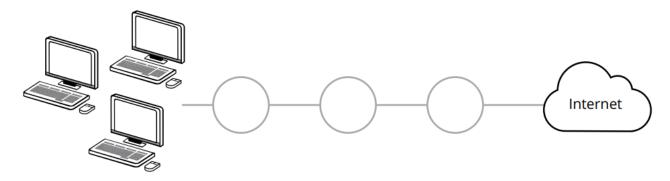


Figura 12: Segurança lógica: Topologia 1

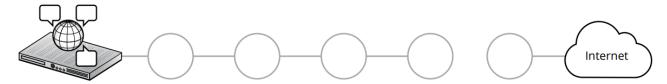


Figura 13: Segurança lógica: Topologia 2



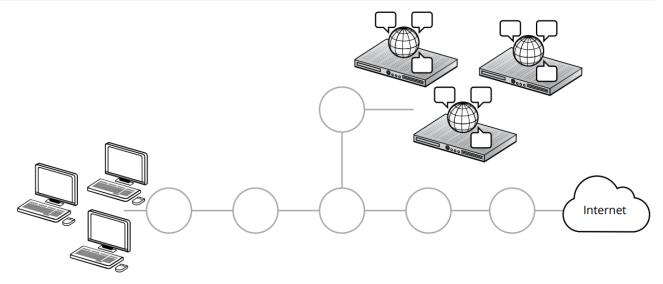


Figura 14: Segurança lógica: Topologia 3

#### 3) Exercitando os fundamentos de segurança

- 1. Como vimos, o conceito de segurança mais básico apresentado consiste no CID (Confidencialidade, Integridade e Disponibilidade). Apresente três exemplos de quebra de segurança em cada um desses componentes, como por exemplo:
  - Planilha Excel corrompida.
  - · Acesso não autorizado aos e-mails de uma conta de correio eletrônico.
  - · Queda de um servidor web por conta de uma falha de energia elétrica.
- 2. Associe cada um dos eventos abaixo a uma estratégia de segurança definida na parte teórica.
  - Utilizar um servidor web Linux e outro Windows 2016 Server para servir um mesmo conteúdo, utilizando alguma técnica para redirecionar o tráfego para os dois servidores.
  - Utilizar uma interface gráfica simplificada para configurar uma solução de segurança.
  - · Configurar todos os acessos externos de modo que passem por um ponto único.
  - Um sistema de segurança em que caso falte energia elétrica, todos os acessos que passam por ele são bloqueados.
  - Configurar um sistema para só ser acessível através de redes confiáveis, para solicitar uma senha de acesso e em seguida verificar se o sistema de origem possui antivírus instalado.
  - Configurar as permissões de um servidor web para apenas ler arquivos da pasta onde estão as páginas HTML, sem nenhuma permissão de execução ou gravação em qualquer arquivo do sistema.

## 4) Normas e políticas de segurança

1. Acesse o site do DSIC em http://dsic.planalto.gov.br/assuntos/editoria-c/instrucoes-normativas e leia a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e as normas complementares indicadas. Elas são um bom ponto de partida para a criação de uma Política de Segurança, de uma Equipe de Tratamento de Incidentes de Segurança, de um Plano de Continuidade de Negócios e para a implementação da Gestão de Riscos de Segurança da Informação.



2. Leia o texto da Política de Segurança da Informação da Secretaria de Direitos Humanos da Presidência da República, de 2012 (disponível na seção Links Úteis e Leituras Recomendadas do AVA, pasta PoSIC), e procure identificar os principais pontos na estruturação de uma PoSIC. Faça uma crítica construtiva do documento com vistas a identificar as principais dificuldades encontradas na elaboração de uma PoSIC.