

Sessão 2: Conceitos fundamentais em segurança da informação

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 <http://www.antispam.br/admin/porta25/> 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