

**Introdução à Segurança da Informação (ISO 27.001 e 27.002)**  
**Exercícios – Objetivos e Controles de um SGSI**

1º) Com base nos objetivos e controles normativos estudados, associe as situações aos respectivos itens da norma:

- ( ) Após a abertura de sua primeira loja virtual, uma cadeia de lojas com um sistema de segurança certificado conforme a norma 27.001 passou a enfrentar incidentes de negação de serviços gerados por ataques externos.
- ( ) O diretor de uma empreiteira encontra-se à volta com o desaparecimento de uma caixa de arquivos com conteúdo confidencial que foi roubada de dentro de um automóvel de um funcionário que ajudava na mudança para a sede nova da empresa.
- ( ) A detecção de um problema de exposição indevida das ligações telefônicas de uma construtora feitas através de um servidor Asterix não pode ser tratado adequadamente. Isso porque, após a implantação do novo sistema de telefonia IP, o responsável pela área de telefonia foi afastado, e nem o gestor administrativo nem o gestor de informática se julgam responsáveis pelo servidor Asterix.
- ( ) O diretor comercial de uma agência de publicidade está enfrentando problemas com um de seus clientes, pois o mesmo descobriu que na área compartilhada para troca de arquivos com clientes estava armazenada toda a campanha publicitária de lançamento dos produtos de seu concorrente (o que ele imaginou que poderia acontecer também com a sua empresa).
- ( ) Um incidente de segurança provocada pelo vazamento indevido de informações de uma transportadora não pode ser tratado adequadamente porque o responsável pelo departamento de RH não considera que o vazamento seja motivo suficiente para o afastamento do funcionário responsável pelo problema.
- ( ) Uma empresa enfrenta uma ação judicial de um ex-funcionário que alega desconhecer qualquer regra que o impedisse de instalar software piratas na sua estação de trabalho.
- ( ) O diretor de TI de uma corretora de ações está tendo dificuldades para contratar um novo gerente de segurança de informação, pois não tem contatos nesta área.
- ( ) Uma fábrica de automóveis está com sua produção paralisada devido à queda de um link de comunicação com seu departamento de controle da produção em outra unidade, e está às voltas com o impacto da paralisação durante todo o final de semana, pois o problema aconteceu na sexta-feira à noite, logo depois do expediente administrativo.

**Introdução à Segurança da Informação (ISO 27.001 e 27.002)**  
**Exercícios – Objetivos e Controles de um SGSI**

2º) Dadas as seguintes tecnologias de informática aplicáveis para o tratamento de riscos de seu SGSI, identifique os objetivos e controles normativos que poderiam ser associados a cada uma delas, explicando a sua aplicação:

VLANs: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Token de Usuário: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Firewall: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Switch de Camada 3: \_\_\_\_\_  
\_\_\_\_\_

**Introdução à Segurança da Informação (ISO 27.001 e 27.002)**  
**Exercícios – Objetivos e Controles de um SGSI**

---

---

Arranjo RAID de discos: \_\_\_\_\_

---

---

---

Criptografia de HD: \_\_\_\_\_

---

---

---

3º) Exercício: Dadas as seguintes áreas e setores de uma corporação, identifique pelo menos dois controles normativos que poderiam ser associados a cada uma delas, explicando a sua aplicação:

Presidência: \_\_\_\_\_

---

---

---

**Introdução à Segurança da Informação (ISO 27.001 e 27.002)**  
**Exercícios – Objetivos e Controles de um SGSI**

Diretoria Administrativa: \_\_\_\_\_

---

---

---

Diretoria de TI: \_\_\_\_\_

---

---

---

Equipe de TI: \_\_\_\_\_

---

---

---

Usuários (diversos) : \_\_\_\_\_

---

---

---

**Introdução à Segurança da Informação (ISO 27.001 e 27.002)**  
**Exercícios – Objetivos e Controles de um SGSI**

---

Diretoria de TI de parceiro prestador de serviços: \_\_\_\_\_

---

---

---