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

(10.6.1) Após a abertura de sua primeira loja virtual, uma cadeia de lojas com um sistema de segurança certificado conforme a norma ISO 27.000 passou a enfrentar incidentes de negação de serviços gerados por ataques externos.

(10.8.3) 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.

(7.1.2) 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.

(6.2.2) 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).

(8.2.3) 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.

(8.1.1) 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.

(6.1.7) 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.

(6.1.6 e 10.2.1 e 14.1.1) 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.

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:

11.4.5 – Segregação de Redes. O recurso de VLAN permite separar grupos de usuários em redes virtuais separadas.

Token de Usuário:

11.4.2 – Autenticação de Usuários Remotos -

Firewall:

10.6.1 – Controle sobre a Rede
11.4.6 – Controle de conexão à Rede

Switch de Camada 3:

11.4.7 – Controle das Rotas de Tráfego de Informações

Arranjo RAID de discos:

14.1.3 – Desenvolver e implementar planos de continuidade de negócios envolvendo sistemas de informação
10.6.1 – Controle sobre a Rede

Criptografia de HD:

10.8.3 – Proteção de Mídia em Trânsito
10.6.1 – Controle sobre a Rede

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

Presidência:

6.1.1 - Comprometimento da gerência com a Segurança da Informação

Diretoria Administrativa:

6.1.6 -
6.1.7 -

Diretoria de TI:_____

_____

_____

_____

Equipe de TI: _____

_____

_____

_____

Usuários (diversos) :_____

_____

_____

_____

Diretoria de TI de parceiro prestador de serviços:_____

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