QUESTÕES BASEADAS NA NBR ISO/IEC 17799 - ATIVIDADE EM GRUPO

Grupo: Gabriela Silverio, Gabriele Batagiero, Gabriela Aries, Ariane e Daiely.
Questionário:

- O que é a informação e como ela pode existir dentro de uma organização? Por que é importante protegê-la?
  R:A informação é um ativo importante para os negócios, geralmente tem muito valor para a organização e necessita ser protegida. Pode existir em muitas formas, impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou meios eletrônicos, mostrada em filmes ou em conversas. Confidencialidade da informação pode ser essencial para preservar o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado.

- Quando falamos de segurança da informação o que significa os termos: confidencialidade, integridade e disponibilidade?
  R:A confidencialidade, integridade e disponibilidade da informação são requisitos essenciais para preservar a privacidade dos dados de uma empresa. Sendo assim cada requisito tem seu significado:
  -Confidencialidade: é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
  -Integridade: é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
  -Disponibilidade: é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

- Como podemos obter Segurança da Informação?
  R:Pode ser obtida a partir da implementação de um conjunto de controles, que incluem a tecnologia, políticas, processos, práticas, procedimentos e a própria estrutura organizacional de cada empresa.

- Quais são os principais tipos de ameaças à segurança da informação?
  R: Vulnerabilidade das informações e das instalações feitas no local e suas ocorrências.

- Como uma organização pode identificar os seus requisitos de segurança?
  R: Existem três fontes principais, a primeira fonte é derivada da avaliação de risco dos ativos da organização. Através da avaliação de risco são identificadas as ameaças, as vulnerabilidades e a probabilidade de ocorrência é avaliada.
  A segunda fonte é a legislação dos estatutos, a regulamentação, cláusulas contratuais, seus parceiros contratados e prestadores de serviço têm que atender.
  A terceira fonte é o conjunto de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

- Como realizar análises críticas periódicas dos riscos de segurança e dos controles?

R: Podemos analisar a efetividade da política, que é demonstrada pelo impacto dos incidentes de segurança registrados; pelos custos dos controles que estão na eficiência dos negócios; e por fim os efeitos das mudanças na tecnologia.

- Quais são os controles considerados essenciais para uma organização?
  R:Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem:
  a) proteção de dados e privacidade de informações pessoais (ver 12.1.4);
  b) salvaguarda de registros organizacionais (ver 12.1.3);
  c) direitos de propriedade intelectual (ver 12.1.2).

- Quais são os controles considerados como melhores práticas para a segurança da informação?
  R: Os controles considerados como melhores práticas para a segurança da informação incluem:
  a) documento da política de segurança da informação (ver 3.1);
  b) definição das responsabilidades na segurança da informação (ver 4.1.3);
  c) educação e treinamento em segurança da informação (ver 6.2.1);
  d) relatório dos incidentes de segurança (ver 6.3.1);
  e) gestão da continuidade do negócio (ver 11.1).

- Quais são os fatores críticos para o sucesso da implementação da segurança da informação dentro de uma organização?
  R: A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma organização:
  a) política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;
  b) um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;
  c) comprometimento e apoio visível da direção;
  d) um bom entendimento dos requisitos de segurança, avaliação de risco e gerenciamento de risco;
  e) divulgação eficiente da segurança para todos os gestores e funcionários;
  f) distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e
  fornecedores;
  g) proporcionar educação e treinamento adequados;
  h) um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança
  da informação e obtenção de sugestões para a melhoria.

- As empresas podem criar suas próprias recomendações de segurança
  R: Sim, e ainda podem se basear nas normas ou em outros conjuntos de controles.

- Qual a diferença entre avaliação de risco e gerenciamento de risco?
  R: A avaliação de risco e avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade

de sua ocorrência. já o gerenciamento de risco é o Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

- Qual o objetivo de uma Política de segurança da informação e o que deve conter este documento?
  R: Objetivo: Prover à direção uma orientação e apoio para a segurança da informação deve constar no documento:
  a) definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação (ver introdução);
  b) declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação;
  c) breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
  1) conformidade com a legislação e cláusulas contratuais;
  2) requisitos na educação de segurança;
  3) prevenção e detecção de vírus e software maliciosos;
  4) gestão da continuidade do negócio;
  5) conseqüências das violações na política de segurança da informação;
  d) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança;
  e) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informações específicos ou regras de segurança que convém que os usuários sigam.

- Como deve ser feita a análise crítica e avaliação da Política de Segurança de uma empresa?
  R:Como já dissemos, a análise crítica deve ser realizada pela alta direção, que deve analisar criticamente o sistema de gestão da qualidade da organização em intervalos planejados para garantir sua relevância, adequação e eficácia.

- Com relação à Segurança organizacional de uma empresa, porque é importante a criação de uma Infraestrutura da segurança da informação?
  R:Além de eliminar vulnerabilidades e proteger sistemas do negócio contra ataques, a segurança da informação também contribui para a longevidade da organização.

- Quais são as responsabilidades dos gestores de um fórum de segurança da informação?
  R: É responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem.