Nomes: **3ºC;Turma B**

Kewyn Torres

Laura Esther

Luiz Lima

Mateus Moraes

Richard Dutra

1. **O que é a informação e como ela pode existir dentro de uma organização? Por que é importante protegê-la?**

Informação é um conjunto de informações e existe dentro de uma organização como ativo principal, sendo de tamanha importância para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado. Ela pode pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas.

A proteção da informação é importante para garantir que a organização não esteja exposta a vulnerabilidades, visando impedir acessos que representem ameaças, para sempre preservar o valor do dado.

2. **Quando falamos de segurança da informação o que significa os termos: confidencialidade, integridade e disponibilidade?**

Confidencialidade: a garantia de que as informações serão divulgadas e acessadas sem autorização

Integridade: garante a completude e exatidão das informações sem que elas sofram alteração ou sejam violadas

Disponibilidade: garante acesso à informação quando necessário.

3. **Como podemos obter Segurança da Informação?**

Os primeiros passos para obter Segurança da Informação, é começar fazendo a avaliação de riscos da empresa, para avaliar supostas ameaças e vulnerabilidade, e com qual frequência isso pode ocorrer. Logo após, realizar a análise da legislação, ou seja, verificar estatutos e cláusulas contratuais da organização. Depois de realizar os primeiros passos, é essencial definir os objetivos, princípios e requisitos da empresa para começar a desenvolver os controles de segurança.

4. **Quais são os principais tipos de ameaças à segurança da informação?**

Dentre os principais tipos de ameaças à segurança da informação, estão fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou inundação.

5. **Como uma organização pode identificar os seus requisitos de segurança?**

Para identificar os seus requisitos de segurança, uma organização necessita de três principais fontes: Avaliação de riscos e seus impactos, uso da legislação vigente e um conjunto particular de princípios, objetivos e requisitos para o processamento da informação que a organização tem que desenvolver para apoiar suas operações.

6. **Como realizar análises críticas periódicas dos riscos de segurança e dos controles?**

Ao realizar análises críticas periódicas dos riscos de segurança e dos controles deve-se levar em conta: os impactos que serão causados no caso de incidentes com esse tipo de ameaça, a eficiência e balanço de gastos dos controles e os efeitos após as devidas alterações na tecnologia de segurança.

7. **Quais são os controles considerados essenciais para uma organização?**

Os controles essenciais são:

- Proteção de dados e privacidade de informações pessoais
- Salvaguarda de registros organizacionais
- Direitos de propriedade intelectual

8. **Quais são os controles considerados como melhores práticas para a segurança da informação?**

Os controles considerados como melhores práticas para a informação são:

- Documento da política de segurança da informação
- Definição das responsabilidades na segurança da informação
- Educação e treinamento em segurança da informação
- Relatório dos incidentes de segurança
- Gestão da continuidade do negócio

9. **Quais são os fatores críticos para o sucesso da implementação da segurança da informação dentro de uma organização?**

   Os fatores críticos para o sucesso da implementação da segurança em uma organização, são:

   - política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;
   - um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;
   - comprometimento e apoio visível da direção;
   - um bom entendimento dos requisitos de segurança, avaliação de risco e gerenciamento de risco;
   - divulgação eficiente da segurança para todos os gestores e funcionários;

10. **As empresas podem criar suas próprias recomendações de segurança?**

    Sim, pois as normas podem ser consideradas como ponto de partida para o desenvolvimento de recomendações específicas para a empresas, além disso um controle adicional que não estão incluídos nas normas podem ser necessários .

11. **Qual a diferença entre avaliação de risco e gerenciamento de risco?**

    Avaliação de riscos é o estudo das ameaças e nos impactos nas instalações de processamentos da informação já o gerenciamento de risco é o estudo de brechas para possíveis ameaças

12. **Qual o objetivo de uma Política de segurança da informação e o que deve conter este documento?**

Promover uma direção e apoio para segurança da informação e deve conter a definição de segurança, resumo das metas e escopo, declaração de alto comprometimento da alta direção apoiando as metas e princípios da informação, explanação das políticas mostrando a importância de cada uma delas, definição das responsabilidades gerais da gestão da segurança da informação e referência a documentação que possam apoiar a política.

13. **Como deve ser feita a análise crítica e avaliação da Política de Segurança de uma empresa?**

A análise deve ser feita por um gestor responsável, de acordo com o processo de análise crítica definido. Este processo deve garantir que a análise crítica ocorra após qualquer mudança significativa que afete a segurança, como um incidente de segurança, vulnerabilidades ou mudanças na infra-estrutura técnica.

14. **Com relação à Segurança organizacional de uma empresa, porque é importante a criação de uma Infraestrutura da segurança da informação?**

O objetivo é gerenciar a segurança da informação na organização. Uma estrutura de gerenciamento deve ser estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Deve ser mantido contato com especialistas de segurança, uma fonte especializada em segurança da informação deve ser estabelecida e disponibilizada dentro da organização. Tudo isso garante que a empresa tenha condições e preparo para uma eventual falha na segurança.

15. **Quais são as responsabilidades dos gestores de um fórum de segurança da informação?**

- análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;
- monitoração das principais mudanças na exposição dos ativos das informações às principais ameaças;
- análise crítica e monitoração de incidentes de segurança da informação;
- aprovação das principais iniciativas para aumentar o nível da segurança da informação