**Atividade de SI**

**Grupo:** Rafael Lima**,** Rodrigo Antonio**,** Yuri Candido

**Turma B**

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

**R=** A informação é um ativo, que possui uma grande importância na organização, sendo um conjunto de dados, sendo muito valioso para a organização.

Podendo existir de diversas formas, tanto no papel, armazenada eletronicamente, enviada pelos correios ou meios eletrônicos.

Para a proteção da informação faz-se necessário uma série de regras e leis para garantir os principais princípios da segurança da informação, que são integridade, disponibilidade e confidencialidade.

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

**R=** A confidencialidade é a total garantia de que a informação seja acessível somente pelas pessoas autorizadas.

A integridade se refere salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Por fim a disponibilidade é a garantia de que os usuários autorizados, obtenham acesso à informação sempre que necessário.

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

**R=** Para se obter a segurança da informação é necessário a implementação de certos controles, políticas e práticas que garantam que os objetivos de integridade, confidencialidade e disponibilidade sejam atendidos.

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

**R=** Fraudes eletrônicas, espionagem, sabotagens, vandalismo. São tipos de ameaças que podem apresentar riscos a segurança da informação.

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

**R=** Para identificar os requisitos que uma empresa necessita,

A primeira se deriva da avaliação dos riscos ativos a está organização, identificando essas vulnerabilidades e riscos é estimado uma probabilidade da ocorrência de alguma ameaça.

A segunda é de acordo com a legislação, regulamentando cláusulas que as organizações precisam atender.

A terceira é um conjunto de princípios e objetivos para o processamento da informação que a organização tem a desenvolver.

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

**R=** Recomenda-se seguir as seguintes etapas:

1. Identificar as ameaças: as ameaças à segurança da informação devem ser identificadas, incluindo aquelas internas e externas, bem como as ameaças físicas e lógicas.
2. Avaliar os riscos: os riscos associados a cada ameaça identificada devem ser avaliados em termos de impacto e probabilidade.
3. Identificar os controles existentes: os controles existentes devem ser identificados, incluindo aqueles relacionados à prevenção, detecção e resposta a incidentes de segurança.
4. Avaliar a eficácia dos controles existentes: os controles existentes devem ser avaliados em relação à sua eficácia em mitigar os riscos identificados.
5. Identificar lacunas: quaisquer lacunas nos controles existentes devem ser identificadas, juntamente com quaisquer novos controles que possam ser necessários.
6. Planejar ações corretivas: as ações corretivas necessárias devem ser planejadas para abordar as lacunas identificadas e melhorar a eficácia dos controles existentes.
7. Implementar as ações corretivas: as ações corretivas devem ser implementadas e os controles atualizados conforme necessário.
8. Monitorar e revisar: os controles devem ser monitorados e revisados periodicamente para garantir sua eficácia contínua e abordar quaisquer novas ameaças ou riscos.

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

**R=** Os considerados essenciais:

1. Proteção de dados e privacidade de informações pessoais
2. Salvaguarda (medida de segurança) de registros organizacionais
3. Direitos de propriedade intelectual

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

**R=** Os considerados como melhores práticas:

1. Documento da política de segurança da informação
2. Definição das responsabilidades na segurança da informação
3. Educação e treinamento em segurança da informação
4. Relatório dos incidentes de segurança
5. Gestão da continuidade do negócio

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

**R=** A norma lista 8 fatores críticos para o sucesso da implementação, sendo alguns deles:

* Política de segurança (conjunto de diretrizes), 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;
* Proporcionar educação e treinamento adequados (aos colaboradores);

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

**R=** Sim. A norma estabelece que as empresas devem definir sua própria política de segurança, selecionar os controles de segurança adequados para suas necessidades e objetivos, e implementá-los de acordo com sua análise de riscos.

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

**R=** Avaliação de risco é uma avaliação de ameaças, impactos e vulnerabilidade da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência

Gerenciamento de risco é um processo de identificação, minimização e controle dos riscos da segurança que podem afetar os sistemas da informação, a um custo aceitável.

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

**R=** O objetivo de uma política de segurança da informação é dar apoio e uma direção para a segurança da informação. No documento deve ter contido:

uma definição para segurança da informação, a importância da segurança como um mecanismo que habilita o compartilhamento da informação e um resumo de metas e escopo

Declaração de comprometimento, dando apoio as metas e princípios da segurança da informação

Breve explanação de princípios, padrões, políticas e requisitos de conformidade de importância específica para a organização

definir as responsabilidades gerais e específicas na gestão da segurança da informação, tendo incluso o registro de segurança

Referência à documentação que possam apoiar a política.

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

**R=** Ela deve ser feita por um gestor que terá como responsabilidade realizar a manutenção e análise crítica da política, análise essa que teve ser feita com um processo já definido. Nesse processo terá o agendamento das seguintes análises críticas periódicas:

Efetividade da política

Custo e impacto dos controles de eficiência do negócio

Efeitos das mudanças na tecnologia

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

**R=** É importante sua criação pois ela é que tem como objetivo fazer o gerenciamento da segurança da informação dentro da organização, essa estrutura seja estabelecida para ser ter início e controle sobre a implementação da segurança da informação dentro da organização

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

R= Um gestor de um fórum tem como responsabilidade as atividades relacionadas à segurança, como 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.