**QUESTÕES S.I.**

**INTEGRANTES:** Gabriel Oliveira Sampaio, Gustavo Silvério Firmino Sotelo de Oliveira, Breno Cardozo Fagundes, Gustavo Rodrigues Martins, Julia Granado Ferri Barbosa.

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 que tem um valor para a organização. É importante protegê-la pois cada vez mais as organizações têm seus sistemas de informação e redes de computadores expostos à prova por diversos tipos de ameaças à segurança da informação de uma variedade de fontes.

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

**R:** Confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso; Integridade é como uma salvaguarda da exatidão e completeza da informação e dos métodos de processamento; Disponibilidade é a garantia de que os usuários com autorização obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Como podemos obter Segurança da Informação?

**R:** Implementando uma sucessão de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software.

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

**R:** Fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou inundação.

Como uma organização pode identificar os seus requisitos de segurança?

**R)** É essencial que uma organização identifique os seus requisitos de segurança. 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 aos ativos, as vulnerabilidades e sua probabilidade de ocorrência é avaliada, bem como o impacto potencial é estimado, sendo assim, após essa verificação da integridade e bem estar dos ativos, é feita a eliminação das possíveis ameaças e brechas de segurança.
* A segunda fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender.
* A terceira fonte é o conjunto particular 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)** De princípio, é necessário agendar as seguintes análises críticas periódicas para verificar a integridade da organização:

* Efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados;
* Custo e impacto dos controles na eficiência do negócio;
* 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: 

* Proteção de dados e privacidade de informações pessoais;

* Salvaguarda de registros organizacionais;
* Direitos de propriedade intelectual.

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:

* 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.

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

**R:** Para ter uma boa implementação de segurança em uma organização, é necessário encontrar vulnerabilidades nos servidores, networking e aplicações. Também criar políticas de proteção com o uso de processo.

As empresas podem criar suas próprias recomendações de segurança?

**R:** Sim, mas é necessário que as recomendações estejam bem estabelecidas.

Qual a diferença entre avaliação de risco e gerenciamento de risco?

**R:** A análise e gerenciamento de risco é o processo de planejamento dos recursos de uma organização, com o objetivo de reduzir e eliminar a ocorrência de determinados riscos, além de minimizar os efeitos dos que venham acontecer.

Durante a fase de planejamento de um projeto, ela torna-se fundamental para prevenção de falhas. Já ao longo do seu desenvolvimento, ela aparece como meio de correção do processo para as demais falhas que surgiram ao longo de seu funcionamento.

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

**R:** O objetivo é prover à direção uma orientação e apoio para a segurança da informação. Deve-se encontrar nesse documento a definição de segurança da informação, declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação, definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança.

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

**R:** As análises críticas são executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações de risco feitas anteriormente e das mudanças nos níveis de risco que a direção considera a um nível aceitável para os negócios. Uma vez tendo sido identificados os requisitos de segurança, convém que os controles sejam selecionados e implementados para assegurar que os riscos são reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta Norma ou de outro conjunto de controles, ou novos controles podem ser desenvolvidos para atender às necessidades específicas, quando apropriado. Existem diversas maneiras de gerenciar os riscos e esta Norma fornece exemplos para as situações mais comuns

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

**R:** Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Convém que fóruns apropriados de gerenciamento com liderança da direção sejam estabelecidos para aprovar a política de segurança da informação, atribuir as funções da segurança e coordenar a implementação da segurança através da organização. Se necessário, convém que uma fonte especializada em segurança da informação seja estabelecida e disponibilizada dentro da organização. Convém que contatos com especialistas de segurança externos sejam feitos para se manter atualizado com as tendências do mercado, monitorar normas e métodos de avaliação, além de fornecer o principal apoio durante os incidentes de segurança. Convém que um enfoque multidisciplinar na segurança da informação seja incentivado, tais como o envolvimento, cooperação e colaboração de gestores, usuários, administradores, projetistas de aplicações, auditores, equipes de segurança e especialistas em áreas como seguro e gerenciamento de risco.

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

**R:**  As responsabilidades dos gestores são as seguintes: 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 de informação e a aprovação das principais iniciativas para aumentar o nível da segurança da informação.