Nome: Raíssa Bespalec Daloia

Segurança da Informação

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

A informação é um conjunto de dados e tem um valor fundamental para qualquer empresa, pois, caso houver alguma invasão, a empresa pode ser prejudicada tanto financeiramente, quanto legalmente. Existem diversos riscos para essa perda de informações, principalmente, para as informações fundamentais para o andamento da empresa.

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

Confidencialidade: proteção de dados; informação acessada somente com autorização do administrador.

Integridade: dados sem alteração.

Disponibilidade: sistema de fácil acesso da informação.

3-) Como podemos obter Segurança da Informação?

Por meio de estratégias, métodos, ferramentas, ações e ideias que visam a proteção de dados.

Exemplo:

- Profissionais na área;
- Sistema de segurança e de registros;
- Reforços e manutenções dos sistemas;
- Protocolos de segurança;
- LGPD (Lei Geral de Proteção de Dados).

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

As principais ameaças à segurança da informação são:

- Malware;
- Ransomware;
- Spyware;

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

Se atentando aos princípios:

- Confidencialidade;

- Integridade Disponibilidade (CID);
- Autenticidade;
- Irretratabilidade (Não-Repúdio).

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

Realizando avaliações sistemáticas, procurando potenciais falhas na segurança. Pode ser realizada na organização inteira ou apenas em uma parte do sistema.

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

É necessário identificar e gerenciar muitas atividades para funcionar efetivamente. Para implementar a Segurança da Informação em uma empresa, é necessário estabelecer uma estrutura para gerencia-la da maneira adequada. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes da organização, que devem ter responsabilidades bem definidas e proteger as informações de caráter sigiloso

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

Deve ser criado um documento sobre a política de segurança da informação da empresa, que deve conter os conceitos de segurança da informação, uma estrutura para estabelecer os objetivos e as formas de controle, o comprometimento da direção com a política, entre tantos outros fatores., processos e recursos.

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

Seguir os princípios sugeridos na normaISO/IEC27002é essencial para garantir a segurança da informação nas empresas. Neste sentido, é primordial ressaltar a importância de empresas possuírem profissionais certificados em seus times de segurança, dando maior respaldo ao processo de implantação das boas práticas relacionadas a norma, bem como a obtenção de certificação corporativaISO27001.

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

Se uma empresa optar por seguir um documento SGSI, deverá seguir os requisitos definidos nesta norma e pretende-se que seja aplicável a todas as organizações, independentemente do seu tipo, dimensão e natureza. Por outro lado, as empresas que não optarem por seguir essas normas poderão optar por criar sua própria documentação.

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

A avaliação de risco é a realização do processo paraidentificar fontes de risco e estimá-los. Já a gestão de riscos são as atividades programadas para gerenciar e controlar a organização numa situação de risco.

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

Tem como objetivo assegurar os controles de segurança para proteger e diminuir os riscos ou perdas de ativos. Tendo isso em mente, o documento deve "Prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)".

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

Verificar se os requisitos estabelecidos de um projeto foram alcançados, assegurar a sua pertinência, adequação e eficácia, e quais são as melhorias que possam agregar valor. Uma boa política de segurança deve estar diretamente ligada a cultura organizacional da empresa e deve ser coerente e alinhada com a sua missão, visão e valores e seu planejamento estratégico.

14-) Com relação a Segurança organizacional de uma empresa, por que é importante a criação de uma Infraestrutura da segurança da informação?

Tendo em vista que, o roubo e vazamento de dados exacerbado não compromete só a segurança da empresa, mas também a segurança de seus clientes, a criação de uma infraestrutura de segurança, permitiria um pouco mais de confiança da empresa contra esses tipos de ataques, eliminando a vulnerabilidade e protegendo os sistemas do negócio, sem contar que, também contribui para a longevidade da organização.

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

Sabemos que em um fórum de Segurança da informação, é discutido, orientado e apresentado diretrizes sobre a segurança da informação para todos os órgãos e ambientes do Poder Judiciário, refletindo a visão do mesmo diante da importância em proteger os seus ativos de informação. Os gestores desses fóruns, são responsáveis por:•Aprovar e Publicar a Política de Segurança da Informação e suas revisões;

•Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação