Segurança da Informação e Ética em TI

Nome: Fernanda Pinheiro Reis RA: 1110481823022

Segurança da Informação:

1- Qual a importância da Segurança da Informação para uma Organização Pública ou Privada aponte aspectos que você identifica importantes para tal (mínimo 5 linhas)?

A informação, nos tempos atuais, é um dos bens mais importantes para as empresas, sejam elas públicas ou privadas, afinal é natural que as empresas possuam sistemas de gerenciamento que lida com dados, ainda mais se a empresa oferecer algum serviço digital. A Segurança da Informação são todos os mecanismos de proteção que as empresas devem possuir para proteger os dados que possui. Uma empresa que possui boa segurança de informação, tem menor riscos em seu negócio e transmite mais confiança ao público.

2- Qual a importância da área de TI para uma Empresa e para os Negócios de uma empresa?

A Tecnologia da Informação está presente em diversas áreas (se não todas) das organizações. Boa parte das atividades de gestão são realizadas por meio de um computador, as empresas muitas vezes necessitam de uma rede de computadores, também necessitam de softwares, sites, aplicativos diversos.

Fora todas as questões administrativas de uma empresa, a TI também está presente na programação de máquinas das indústrias, algoritmos de inteligência artificial que identificam gostos dos usuários na internet, controle de dados e muitos outros serviços.

3- Quais os Três principais riscos pela falta de segurança em uma Organização, explique-os:

Indisponibilidade de recursos, faz com que a operação ou parte dela seja comprometida, fatores como falta de energia, problemas de hardware ou software, greves de funcionários ou desastres podem deixar servidores parados, ambientes computacionais sem profissionais para sua operação, perda de hardware e consequentemente dados armazenados nos mesmos (resultando por exemplo em indisponibilidade de serviços web, servidores tipo emails, arquivos, monitoramento dentre diversos outros sistemas que podem cair).

Falta de integridade de informações, o que pode acarretar em informações falsas e inconsistentes, causando erro na operação e gerando prejuízos ou tomada de

decisões incorretas devido o acesso de pessoas não autorizadas ou pela falta de controle de acesso a recursos computacionais.

Ausência de informações necessárias, gera resultados não confiáveis, impossibilita verificação de processos de troca de dados, dificulta a tomada de decisões.

4- Dentre as ameaças a Seg. da Informação podemos apontar:

a. Roubo
b. Perda
c. Sabotagem
d. Espionagem Industrial
e. Novas Tecnologias
f. Erros
g. Vírus
h. Pirataria

Aponte como cada uma dessas ameaças comprometem a Segurança da Informação de uma empresa:

A - Roubo → De equipamentos, informações, dinheiro ou estoques. Pode acarretar fraudes e prejuízos a instituição, através de vazamento de informações, fraude financeira eu prejuízo de equipamentos físicos.

B - Perda → Gera falhas de segurança em ausência de backups, falha de hardware vital sem plano de contingência, erro de persistência de dados.

C - Sabotagem → Indisponibilidade de serviços, perda de dados e alteração/invalidação e alterações.

D - Espionagem Industrial → Pode ocasionar roubo dados de negócios, estratégias, produtos e informações restritas aos produtos e serviços da instituição (dados patenteados e sigilosos por exemplo), segredos industriais.

E - Novas tecnologias → Furos e vazamentos de dados, quebra de segurança, invasões de área virtual (redes servidores, e mails, banco de dados).

F - Erros → Falhas humanas ou lógicas, erro de processos, falta de testes ou de treinamento adequado, pode gerar impactos como indisponibilidade de serviços, perda ou vazamento de dados.

G - Vírus → Contaminação por pirataria, quebra de protocolo de segurança, por utilização de softwares ou recursos proibidos no ambiente informatizado (softwares, pen drives, acesso a sites indevidos).

H - Pirataria → Penalização perante as leis de direitos autorais, perda de credibilidade junto a clientes e fornecedores, multas.

5- Quais os meios que as empresas podem se utilizar para mitigar os problemas relacionados a Segurança da Informação?

Através de políticas bem definidas de segurança, tanto em ambiente computacional quanto em regras de uso e manipulação de dados e equipamentos por parte dos funcionários. Análise de riscos atuais e futuros, treinamento específico aos funcionários, aplicando regras e as devidas penalidades quando infringidas, realizando auditoria de sistemas e manter-se atualizada quanto a novas tecnologias e ferramentas.

6- Dentre os elementos com necessidade proteção em uma organização estão:

a. Hardware
b. Software
c. Comunicações
d. Sistemas
e. Informações
f. Recursos Humanos

Quais os aspectos que envolvem cada um destes elementos voltados para segurança que devem ser observados?

A - Hardware → Acesso físico, condições do ambiente, Planos de contingência e manutenção.

B - Software → Atualizações, instalação e padronização/Homologação.

C - Comunicações → Criptografia, alternativas de rotas, uso de VPN para proteção.

D - Sistemas → Controle ao acessos, segregação de funções, Checagem de cálculos, relatórios de exceção, Log de atividades críticas.

E - Informações → Controle de acesso, armazenamento, Backup.

F - Recursos Humanos → Contratação, treinamento, Definição de funções.

7- Aborde quais são as medidas de segurança que devem ser inseridas pelas empresas/organizações para apoiar a Segurança da Informação?

Políticas bem definidas de regras de uso de dados, controle de acesso a recursos de software, hardware e acesso em ambientes críticos

Procedimentos de segurança e de operações que padronizam o script de trabalho e forma de uso de recursos computacionais, a fim de evitar quebra de segurança sobre dados e dispositivos e ambientes físicos.

Recursos físicos bem instalados, mantidos em ambiente adequado e constantemente avaliado. Controle de acesso de pessoal a estes recursos e plano de contingência em caso de catástrofes e acidentes.

Validação e teste de recursos lógicos, log de atividades para avaliação constante, controle de funções e acessos ao sistema e auditoria do mesmo.

Ética em T.I.

1- O que você entende por Ética e Ética Profissional:

Ética está relacionado com os princípios do comportamento humano, o que consideramos certo e errado, justo e injusto, como devemos conviver com outros seres e com o planeta.

Ética profissional está relacionado com o exercício correto da profissão. O profissional possui conhecimento adquirido e possui poder na área que se especializou. Sua profissão deve ser realizada como contribuição à população, que vise uma redução de problemas, sejam eles regionais ou globais. O profissional especializado tem a escolha de como deve realizar seus serviços e deve fazer isso da melhor forma.

2- Como a ética se encaixa na Computação (mínimo 5 linhas)?

A ética na computação é fator crucial para a alta adesão de uma aplicação. É importante considerar os seguintes passos:

Não invadir a conta de qualquer um, somente de pessoas nitidamente mal intencionadas;

Não aplicar golpes de qualquer natureza;

Não desenvolver virus;

Defender a liberdade individual nos sistemas digitais;

Não se vender para qualquer empresa, principalmente se for uma empresa ruim;

Pensar no usuário, que não costuma mexer bem no computador, portanto os sistemas devem ser funcionais e atraentes.

3- Independentemente da definição usada, podemos examinar tópicos típicos relacionados à ética, como cada um deles se encaixam no conceito ético?

a. Computadores no trabalho

De acordo com o seu uso, podem gerar ou tirar empregos. O que depende da forma como a organização trabalha e com as suas necessidades.Trazem facilidade e produtividade, mas em certos casos demandam alto nível de qualificação profissional e podem causar estresse e alguns tipos de doenças devido seu uso inadequado ou contínuo. Prejudicial ou benéfico de acordo com sua utilização.

b. Crime com computador

Quebra de protocolos de segurança, invasão de ambiente e captura de dados, fraudes e falhas operacionais, prejudicial a operação da organização sujeito a penalização perante a lei.

c. Privacidade e anonimato

Sigilo no acesso a grande volume de dados pessoais armazenados, anonimato em informações sigilosas. Forma de se manter o sigilo de dados que não devem ser expostos sem prévia autorização do usuário.

d. Propriedade intelectual

Diversos debates ocorrem sobre o que deve ou não ser protegido e quais as formas de proteção. Uma das implicações são em limitar a ciência e nível de

conhecimento por parte das pessoas, restringindo apenas a empresas com muito capital para acesso às informações.

e. Globalização

Impacto das grandes redes de dados sobre a população, como padronização da cultura, leis aplicadas a rede, práticas de negócios autorizadas criam debates e dúvidas sobre até quando a TI é benéfica.

f. Ética professional

Comportamento dos profissionais, suas responsabilidades quando exercidos promovem um trabalho íntegro e eficiente, sem riscos ou danos a organização ou a sociedade.

4- Quais são os Imperativos Morais de forma geral para quem atua na área de T.I?

- Devo contribuir para a sociedade e o bem-estar humano
- Devo evitar causar mal/danos a outros
- Devo ser honesto e digno de confiança
- Devo ser justo e agir para não discriminar
- Devo honrar direitos de propriedade, incluindo copyrights e patentes
- Devo dar crédito adequado à propriedade intelectual
- Devo respeitar a privacidade dos outros
- Devo honrar acordos de confiança