Neste documento constam a prova A (1a. Página) e a prova B (2a. Página) da 2a. prova presencial da disciplina Segurança e Auditoria de Sistemas.

PROVA A

Questão 1) (9 pontos)

A classificação das informações é um dos primeiros passos para se elaborar um plano de segurança. Uma classificação adotada amplamente define quatro níveis, dois deles são: pública e interna. Quando uma informação é classificada de acordo com cada nível citado anteriormente ?

Uma informação **pública** é aquela que pode ser divulgada para qualquer pessoa sem que haja implicações para a instituição. Uma informação **interna** é uma informação que não devem sair do âmbito da instituição. Entretanto, caso isso vem a ocorrer, as consequências não serão críticas.

Questão 2) (9 pontos)

Objetivos da segurança devem ser tratados cuidadosamente pela equipe de informática e pelos usuários de sistemas. Explique os objetivos indicados abaixo.

Privacidade: proteger informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação;**Integridade dos dados**: evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação; **Isolamento**: certificar que de que nada importante do sistema foi alterado ou adulterado em caso de acesso indevido.

Questão 2) (9 pontos)

Qual o objetivo da análise de riscos no contexto de segurança da informação ? Qual a sua relação com a Análise de Ameaças e Vulnerabilidades ?

O objetivo da análise de riscos é medir ameaças, vulnerabilidades e impactos em um determinado ambiente, de forma a proporcionar a adoção de medidas apropriadas tanto às necessidades de negócio de uma instituição, ao proteger seus recursos de informação, como aos usuários que necessitam utilizar esses recursos, levando em consideração justificativas de custos, nível de proteção e facilidade de uso.

A análise de riscos, então, engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, a qual identifica os componentes críticos e o custo potencial ao usuário do sistema.

Questão 3) (8 pontos)

Quais são as responsabilidades e a importância de um modelo de governança da segurança da informação para uma organização?

O modelo de governança de segurança da informação é responsável para que as organizações tenham proteção contra os riscos inerentes ao uso da infraestrutura de TIC ao mesmo tempo que obtenham indicadores dos benefícios de ter essa infra- estrutura segura e confiável. Em função do grande número de dados provenientes das mais diversas fontes da infraestrutura de TIC no cenário atual, é importante que boa parte das decisões seja tomada de forma estruturada e científica e não mais de forma sistêmica. No enfoque organizacional, de forma científica, o gestor pode utilizar modelos de governança organizacional apoiados por ferramentas disponíveis na teoria da decisão.

PROVA B

Questão 1) (9 pontos)

A classificação das informações é um dos primeiros passos para se elaborar um plano de segurança. Uma classificação adotada amplamente define quatro níveis, dois deles são: confidencial e secreta. Quando uma informação é classificada de acordo com cada nível citado anteriormente ?

Uma informação confidencial é aquela cujo acesso é realizado de acordo com estrita necessidade, isto é, os usuários só podem acessá-las se forem fundamentais para o desempenho de suas funções na instituição. O funcionamento da organização pode ficar seriamente comprometido, danos financeiros podem ocorrer ou perda de mercado para a concorrência se essas informações forem acessadas de forma não autorizadas. Uma informação secreta é aquela cujo acesso interno ou externo de pessoas não autorizadas é extremamente crítico para a organização.

Questão 2) (9 pontos)

Objetivos da segurança devem ser tratados cuidadosamente pela equipe de informática e pelos usuários de sistemas. Explique os objetivos indicados abaixo.

Confidencialidade: proteger informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação; **Disponibilidade**: proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização; **Confiabilidade**: garantir que, mesmo em condições adversas, o sistema atuará conforme o esperado.

Questão 3) (9 pontos)

O que se entende por controle de acesso lógico, controle de acesso físico e controle de acesso ambiental? Lista também duas verificações para cada um dos controles citados anteriormente.

O controle de acesso lógico tem como objetivo proteger dados e aplicações de software contra acesso indevido e malicioso. Verificações (Duas das listadas abaixo):

1. Conceder acesso, aos usuários, apenas aos recursos realmente necessários;
2. Restringir e monitorar o acesso a recursos críticos;
3. Utilizar softwares de controle de acesso lógico;
4. Utilizar criptografia
5. Revisar periodicamente as listas de controle de acesso;
6. Bloquear a conta do usuário após um certo número de tentativas frustadas de logon;
7. Restringir acesso a determinados periféricos.

O controle de acesso físico trata das medidas de proteção contra acesso físico não autorizado(Duas das listadas abaixo):

1. Instituir formas de identificação capazes de distinguir um funcionário de um visitante e categorias diferentes de funcionários, se for necessário;
2. Exigir devolução de bens de propriedade da instituição quando o funcionário é desligado ou demitido;
3. Controlar a entrada e a saída de equipamentos, registrando data, horário e responsável;
4. Controlar a entrada e saída de visitantes, registrando data, horários e local de visita, e dependendo do grau de segurança necessário, acompanhá-los até o local de destino;
5. Instituir vigilância no prédio, 24 horas por dia, 7 dias por semana.

O controle de acesso ambiental visa proteger os recursos computacionais contra danos provocados por desastres naturais, falhas na rede de fornecimento de energia, ou no sistema de ar condicionado dentre outros(Duas das listadas abaixo).

1. Instituir procedimentos de prevenção contra incêndios de acordo com as normas vigentes;
2. Na construção do prédio, usar materiais resistentes à ação do fogo e instalar para-raios;
3. Planejar a disposição dos equipamentos e móveis de forma a facilitar a circulação das pessoas, principalmente nas áreas próximas às saídas de emergência;
4. Adotar política anti-fumo nas dependências da organização;
5. Proibir o consumo de comidas e bebidas próximo aos equipamentos;
6. Manter as salas limpas, sem acúmulo de papéis ou outros materiais de fácil combustão.

Questão 3) (8 pontos)
Como o autor do artigo "Algumas recomendações para um modelo de governança da segurança da informação" define governança da Tecnologia da Informação e Comunicação (TIC) ?

Uma estrutura de relacionamentos entre processos para direcionar e controlar uma empresa para atingir seus objetivos corporativos, por meio da agregação de valor e controle dos riscos pelo uso da TIC e seus processos; ou

Capacidade organizacional exercida pela mesa diretora, gerente executivo e gerente ; de TIC, de controlar o planejamento e a implementação das estratégias de TIC e, dessa forma, permitir a fusão da TIC ao negócio ;ou

Especificação das decisões corretas em um modelo que encoraje o comportamento desejável no uso de TIC, nas organizações ; ou