Lista de Exercícios - Auditoria de Sistemas de Informação.

Nomes: Lucas Vieira, Mateus Vieira, Abner Bessi, Renato Cesar Garcia

1. Porque na atualidade é grande a necessidade de se utilizar melhores mecanismos para prover a segurança das transações e do armazenamento de informações?

R.: Atualmente, a quantidade de dados e informações trafegadas mundialmente atingiu níveis altíssimos, e a disponibilidade desses dados cresceu juntamente. Os serviços oferecidos pelas empresas dependem muito da integridade dessas informações, e a segurança das transações e do armazenamento virou parte essencial para garantia do negócio.

1. Como era feita a segurança antes da informatização e depois com uma informatização centralizada?

R.: A segurança da informação antes da informatização era basicamente física. Documentos eram registrados em papéis e posteriormente armazenados em locais de acesso restrito. Com a informatização, os dados receberam um tratamento de segurança mais pesado, mas a informatização centralizada não levava em conta agentes externos.

1. E nos dias atuais com o uso dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, o que mudou em termos de segurança?

R.: A informação foi descentralizada, então existe uma preocupação para garantir a origem e o destino das informações, além de prevenir as possibilidades de intercepção por algum agente malicioso. Contamos com várias opções de criptografia para garantir a integridade e segurança da informação.

1. Porque a segurança das informações deve ser absoluta?

R.: Muitos serviços fornecidos à população atualmente dependem de IT. A corrupção da informação pode resultar na falha ou total falta desses serviços básicos.

1. O que aconteceria se as informações adulteradas caíssem nas mãos da concorrência ou fossem corrompidas, apagadas ou adulteradas?

Isso representa um perigo para o negócio, gerando a possibilidade até de ocorrências de extorsão ou ameaças.

1. Quais seriam as consequências para a continuidade dos negócios da instituição?

R.: Pensando na continuidade do negócio, a empresa teria que ter um forte trabalho de reestruturação para possivelmente se reerguer após um ocorrência desse tipo.

1. O vazamento de informações sobre seus clientes comprometeria sua credibilidade e daria maiores oportunidades aos concorrentes?

R.: Com certeza. O vazamento de informações sobre os clientes provavelmente faria com que estes cortassem relações com a empresa e buscassem concorrentes.

1. Como é tratada a segurança em relação à Internet? Isso é ter as informações expostas a atacantes ou intrusos da Internet.

R.: Geralmente os usuários não se preocupam muito com suas informações na internet. É comum vermos golpes e outros crimes que se utilizam de informações em redes sociais, blogs, etc

1. Comente essa frase. A segurança não é só uma questão técnica, mas de política e educação empresarial.

R.: A segurança não se trata somente de algoritmos de criptografia, mas também de boas práticas e educação pessoal, principalmente em um ambiente empresarial onde as pessoas podem ser alvo de engenharia social

1. Para que a informação tenha o nível de segurança desejado, é necessária uma atuação sobre dois segmentos: acesso e integridade. O que são esses segmentos?

R.: Acesso: diz que somente as pessoas autorizadas podem ter acesso à informação

Integridade: a informação deve ser a mesma quando é recebida/transmitida, e deve ser confiável (ter o mesmo formato, íntegra)

1. O que são os níveis estratégico, tático e operacional?

R.: O nível estratégico é o de diretoria de uma empresa

Tático são os gerentes de área e coordenadores

Operacional é o nível técnico, chão de fábrica

1. Cite as três razões para que a administração deva preocupar-se com a segurança da informação.

R.: As organizações são dependentes do setor de TI; o setor de TI é vulnerável; deve existir um investimento na área de TI

1. Explique cada uma das razões citadas acima.

* Dependência dos sistemas de informação: sistemas com serviços adequados no devido tempo é a chave da sobrevivência das atuais organizações.
* Vulnerabilidade dos recursos de TI : esses sistemas exigem ambientes estáveis , sem fraquezas para desastres naturais (fogo, inundações, etc)
* Investimento em tecnologia das informações são caros, no desenvolvimento e na manutenção, sendo que a administração deve proteger os recursos para o investimento.

1. Quais são os pontos importantes determinar em termos de segurança sendo que a empresa deve sempre tê-los em mente?

* O que deve ser protegido?
* O que é necessário proteger?
* Como é feita a proteção?
* Importante avaliar o custo x benefício.

1. Apesar de reconhecer a necessidade de se estabelecer algum grau de segurança nos sistemas, a maioria das organizações tende a relegar o assunto para o final da sua lista de prioridades, até a ocorrência de um desastre. Porquê dessa atitude?

R.: Segurança é vista de forma negativa, pois reduz a capacidade operacional da organização, em vez de uma atividade que auxilia a organização a alcançar uma melhor qualidade do serviço com menos recurso.

1. O que é cada um dos termos a seguir? Análise de segurança. Definição e atualização das regras de segurança. Administração de segurança. Auditória.

R.: Análise de segurança: Analise da situação real, identificado o nível de risco a que a organização está exposta e quais providências a serem tomadas para cobrir eventuais vulnerabilidades.

Definição e atualização das regras de segurança: Baseado na análise de risco, as regras de segurança da informação são revisadas e atualizadas.

Implementação e divulgação das Regras de Segurança: Após a definição das regras de segurança, estas são implementadas e colocadas em prática nas diversas áreas da organização.

Administração de segurança: Efetua o monitoramento das regras de segurança por meio de ferramentas específicas e analisa os incidentes de segurança.

Auditória: Verificam o cumprimento das regras de segurança das informações nas diversas áreas da organização.

1. Comente a frase. Sempre existiram riscos. O que não se pode admitir é o descaso com a segurança.

R.: Concordo com essa frase, pois os riscos nunca deixaram de existir e não podemos ficar acomodados porque um dia pode ocorrer alguma situação de risco que possa prejudicar. Então nunca devemos descansar e sempre fazer uma análise e atualização continua.

1. Uma das maiores preocupações das organizações é o vazamento de informações. Em um processo de auditoria, quais são os principais pontos a serem focados para que isso seja evitado?

Auditar se os dados possuem criptografia, a forma de armazenamento, controle de log de quem acessou aquelas informações, ter um controle de quem pode acessar aquele tipo de informação.

1. O plano de continuidade de negócio descreve o enfoque para a continuidade do negócio, por exemplo, o enfoque para a disponibilidade e segurança em um sistema de informação. Em que o processo de auditoria pode auxiliar no plano de continuidade?

R.: A busca do aperfeiçoamento, analise e manutenção do sistema de segurança , para que possa sempre dar continuidade e evolução continua

20) Em relação aos aspectos da segurança física, quais os principais itens para o processo de auditoria serão identificados?

R.: Os principais aspectos que devem ser verificados são o controle de acesso e monitoramento das instalações por meio de sistemas de imagens.

O controle de acesso pode ser realizado com o uso de catracas, cartões de proximidades Smartcard, aliados a dispositivos biométricos. Disposições de câmeras em locais estratégicos.

1. Quais são os dois principais conceitos em se tratando da probabilidade de acontecimento de um problema?

R.: Rico é a probabilidade de ocorrência de um incidente e do grau de severidade que este causará.

Impacto é o grau de sensibilidade identificado quando da ocorrência de um evento de risco.

1. O que podemos citar como diferença entre recuperação convencional e alta disponibilidade ?

R.: Na **recuperação convencional** em caso de incidente a resposta é manual, os dados correntes precisam ser restaurados, a performance do serviço é degradada, tem uma duração de longo prazo para recuperação.

Para a **alta Disponibilidade,** a resposta é automática, a performance do serviço é equivalente, os dados correntes continuam disponíveis a partir do ponto de desastre.

Devido a utilização de base de dados redundante, o tempo de restauração é rápido gerando menos impacto para a continuidade do negócio.

1. O que é um processo de negócio ?

O que é um processo organizacional ?

São as mesmas coisas ?

1. Dentre os tipos de ameaças , cite dois tipos de ameaças humana e descreva-os.

Hacker

Indivíduo com profundos conhecimentos de sistemas operacionais, linguagens de programação, técnicas e ferramentas que potencializam as tentativas de acesso indevido. Comumente buscam mais conhecimento e evitam corromper informações intencionalmente.

Cracker

Indivíduo comumente dedicado a quebrar chaves de proteção de programas de computador e invadir sistemas, violando a integridade das informações com intenção maliciosa. Praticamente um Hacker profissionalmente perigoso

1. Quais são os tipos de impacto? Em sua opinião, qual o tipo de impacto mais complicado de solucionar?

Imagem, Administrativo,Financeiro e Mercado

No meu ponto de vista o impacto financeiro é o mais complicado de solucionar por que a empresa sem capital entre em falência e é extinta,

1. Quais são os benefícios do plano de contingência de negócios para uma empresa?

Redução do tempo de resposta, frente à indisponibilidade de componentes que suportam os principais processos de negócios

· Minimizar as perdas nos processos de negócios com paradas motivadas por múltiplos eventos

· Viabilização de site alternativo para continuidade de negócios

· Aumento de credibilidade com os integrantes da cadeia produtiva, acionistas e clientes

· Atendimento a normas regulatórias e legais relacionadas a continuidade de negócios.