Lista de Exercícios - Auditoria de Sistemas de Informação.

Nomes: Artur P. Ferreira, Murilo Pucci, André Neves, Yuri Ramos, Igor Queiros

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: Pois assim garantimos mais eficiência na realização de tais operações.

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

R: Antes, a segurança da informação era feita auditando-se todos os papéis necessários, após a informatização, audita-se apenas o processo a ser realizado com as informações.

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: Ficou muito mais fácil de se realizar ataques cibernéticos a informação, portanto, o controle de acesso a informação deve ser muito mais rigoroso.

1. Porque a segurança das informações deve ser absoluta?

R: Para garantir que não haja vazamentos de informação, que causam perca de monopólio ou patentes, por exemplo.

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

R: Os concorrentes teriam informações potencialmente valiosas, tendo a oportunidade de prejudicar sua empresa e seus clientes.

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

R: Os negócios seriam prejudicados pois qualquer perda de informação causa grande prejuízo, principalmente se forem informações confidenciais.

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

R: Com certeza, pois possibilitaria aos concorrentes propor o mesmo serviço com preços mais baratos para que haja quebra de contrato, prejudicando os negócios da empresa.

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

R: A questão de segurança é também bastante enfatizada quando se imagina a possibilidade de se ter suas informações expostas a atacantes ou intrusos da Internet, verdadeiras ameaças aos ambientes computacionais que estão em constante evolução, seja em número ou em forma, surgindo com meios cada vez mais sofisticados para violar a privacidade e a segurança das comunicações. Devido a essas preocupações, a proteção da informação tem se tornado um dos interesses primários dos administradores de sistemas, pois uma falha de segurança, vazamento ou perda de informações pode determinar grandes prejuízos.

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

R: É claro que as medidas de segurança não asseguram 100% de proteção contra todas as ameaças, mas a definição das expectativas da organização com relação ao comportamento e os procedimentos necessários no manuseio dos seus bens/ativos deverá estar, mais do que nunca, enraizada na cultura da empresa, pois segurança não é só uma questão técnica, mas de política e educação empresarial.

Não adianta um grande investimento em equipamentos e softwares se os funcionários que lidam com as informações não estiverem cientes das normas e funções que devem cumprir para não comprometer a segurança das informações.

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: O acesso às informações sensíveis de uma empresa deve estar protegido por sistemáticas que garantam que apenas as pessoas autorizadas possam obter essas informações. Já a garantia de integridade deve garantir tanto a exatidão dos dados (confiabilidade) quanto à proteção no que tange à perda.

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

R: Estratégico: Nível em que as políticas da organização são definidas. Descreve o que deve ser feito. Tático: Nível em que as normas da organização são descritas conforme as políticas definidas no nível superior. Operacional: Nível onde os procedimentos são estabelecidos com base nas normas definidas no nível acima. Descreve como são implementadas as regras.

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

R: 1ª Dependência dos sistemas de informação, 2ª vulnerabilidade dos recursos de TI e 3ª investimento em tecnologia da informação.

1. Explique cada uma das razões citadas acima.

R: 1ª Dependência dos sistemas de informação: sistemas que ofereçam serviços adequados e no tempo certo são a chave para a sobrevivência da maioria das organizações atuais. 2ª Vulnerabilidade dos recursos de TI: esses sistemas exigem um ambiente estável, podendo ser danificados por desastres naturais, como fogo, inundação ou terremotos, falhas no controle da temperatura ou no suprimento da energia elétrica, bombas, acidentes ou sabotagens. 3ª Investimento em Tecnologia da Informação: os sistemas de informação são caros, tanto no desenvolvimento quanto na manutenção e a administração deve proteger esse investimento como qualquer outro recurso valioso.

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

R: Alguns pontos são importantes determinar e a empresa deve sempre tê-los em mente:

* O que deve ser protegido?
* Contra o quê será necessário proteger?
* Como será feita a proteção?

Além disso, será necessário determinar que nível de segurança é necessário, bem como avaliar a questão ‘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. Porque dessa atitude?

R: Os dirigentes costumam ver a segurança da informação sob uma perspectiva negativa, como fatores inibidores, responsáveis pela redução da capacidade operacional da organização, em vez de uma atividade que auxilia a organização a alcançar uma melhor qualidade do serviço com menos recursos.

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: Diagnósticos da situação real, com identificação do 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: Com base na análise de risco e/ou outras avaliações, as regras de segurança da informação são revisadas e atualizadas periodicamente.

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 plenamente, pois é impossível existir um sistema impenetrável. E o pensamento leviano de que não há riscos pode nos levar a ataques inesperados.

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?

R: Para evitar o vazamento de informações, é importante realizar a utilização de termos de responsabilidade, existir uma política clara de uso de e-mails, realização de treinamentos, campanhas de divulgação, fiscalização constante, e testes periódicos de verificação de vulnerabilidade.

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 auditoria pode auxiliar ao sugerir novos processos e modelos que assegurem a disponibilidade e segurança dos sistemas utilizados na empresa, além de verificar se o atual modelo é eficiente e cumpre seu papel.

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

R: São realizadas verificações sobre os dispositivos físicos da empresa, não se restringindo a computadores e HDs, mas também a locais de armazenamento, cabeamento, estrutura física dos patrimônios, e também às políticas de proteção às informações não digitais.

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

R: Confidencialidade e disponibilidade

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

R: Alta disponibilidade realiza a criação de processos com a finalidade de realizar a recuperação mais rápida possível em situação de crise, gerando disponibilidade mais rapidamente em relação à recuperação convencional, o que pode gerar benefícios para o negócio.

1. O que é um processo de negócio ?

O que é um processo organizacional ?

São as mesmas coisas ?

R: São as mesmas coisas, pois um processo de negócio, processo organizacional ou método de negócio é um conjunto de atividades ou tarefas estruturadas relacionadas que produzem um serviço ou produto específico (fornece uma meta particular) para seus clientes ou para um cliente particular.

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

R: Engenharia social é uma ameaça humana, sendo o caso onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Outro tipo é o ex-funcionário infeliz, o qual possui informações confidenciais por ter trabalhado na empresa anteriormente, e pode utilizá-las para prejudicar a empresa.

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

R: São impactos na confidencialidade, integridade e disponibilidade, sendo o mais complicado de solucionar a confidencialidade, pois a partir do momento que suas informações se tornam publicas, os danos são imensuráveis.

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

R: Os benefícios são a mais rápida disponibilidade e integridade dos seus dados.