unis
Grupo Educacional

Guia de Estudo

SEGURANÇA E AUDITORIA DE SISTEMAS

unis
Centro Universitário
Grupo unis

Instituição credenciada pelo MEC
Centro Universitário do Sul de Minas

Instituição Credenciada Unis
Credenciado pelo MEC
Portaria 4.385/05

UNIS – Centro Universitário do Sul de Minas

Av. Cel. José Alves, 256 - Vila Pinto
Varginha - MG - 37010-540
Tele: (35) 3219-5204 - Fax - (35) 3219-5223

Instituição Credenciada pelo MEC – Portaria 4.385/05

Centro Universitário do Sul de Minas - UNIS
Unidade de Gestão da Educação a Distância – GEaD
Mantida pela

Fundação de Ensino e Pesquisa do Sul de Minas - FEPESMIG

Varginha/MG

PIURCOSKY, Fabrício Pelloso.
Guia de Estudo – Segurança e Auditoria de Sistemas. Fabrício Pelloso Piurcosky - Varginha: GEaD-UNIS, 2010.
87p.

1. Segurança 1. 2. Auditoria 1. 3. Sistemas de Informação 1. I. Título.

REITOR
Prof. Ms. Stefano Barra Gazzola

GESTOR
Prof. Ms. Wanderson Gomes de Souza

Supervisora Técnica
Profª. Ms. Simone de Paula Teodoro Moreira

Design Instrucional
Prof. Celso Augusto dos Santos Gomes
Jacqueline Aparecida Silva

Coord. do Núcleo de Comunicação
Renato de Brito

Coord. do Núcleo de Recursos Tecnológicos
Lúcio Henrique de Oliveira

Coordenadora do Núcleo Pedagógico
Terezinha Nunes Gomes Garcia

Equipe de Tecnologia Educacional
Danúbia Pinheiro Teixeira
Maria Carolina Silva Castro Oliveira

Revisão ortográfica / gramatical
Gisele Silva Ferreira

Autor
Fabrício Pelloso Piurcosky

MBA em Gestão de TI, Especialista em Redes de Computadores, Bacharel em Ciência da Computação e atualmente Mestrando em Engenharia Elétrica pela UFSJ. Leciona desde 2006 em cursos de graduação e pós-graduação do Unis, foi gestor de TI do Unis até 07/2009 e desde 2006 é Coordenador do Curso de Ciência da Computação do Unis.

ÍCONES

REALIZE. Determina a existência de atividade a ser realizada.
Este ícone indica que há um exercício, uma tarefa ou uma prática para ser realizada. Fique atento a ele.

PESQUISE. Indica a exigência de pesquisa a ser realizada na busca por mais informação.

PENSE. Indica que você deve refletir sobre o assunto abordado para responder a um questionamento.

CONCLUSÃO. Todas as conclusões, sejam de ideias, partes ou unidades do curso virão precedidas desse ícone.

IMPORTANTE. Aponta uma observação significativa. Pode ser encarado como um sinal de alerta que o orienta para prestar atenção à informação indicada.

HIPERLINK. Indica um link (ligação), seja ele para outra página do módulo impresso ou endereço de Internet.

EXEMPLO. Esse ícone será usado sempre que houver necessidade de exemplificar um caso, uma situação ou conceito que está sendo descrito ou estudado.

SUGESTÃO DE LEITURA. Indica textos de referência utilizados no curso e também faz sugestões para leitura complementar.

APLICAÇÃO PROFISSIONAL. Indica uma aplicação prática de uso profissional ligada ao que está sendo estudado.

CHECKLIST ou PROCEDIMENTO. Indica um conjunto de ações para fins de verificação de uma rotina ou um procedimento (passo a passo) para a realização de uma tarefa.

SAIBA MAIS. Apresenta informações adicionais sobre o tema abordado de forma a possibilitar a obtenção de novas informações ao que já foi referenciado.

REVENDO. Indica a necessidade de rever conceitos estudados anteriormente.

SUMÁRIO

EMENTA

Os conceitos e os tipos de ameaças, riscos e vulnerabilidades dos sistemas de informação. O conceito e os objetivos da segurança de informações. O planejamento, implementação e avaliação de políticas de segurança de informações. O conceito e os objetivos da auditoria de sistemas de informação. O planejamento, implementação e avaliação de auditorias de sistemas de informação.

APRESENTAÇÃO

Prezado aluno:

Vivemos na chamada Era da Informação, por isso, é vital sabermos utilizar o que ela tem de mais interessante e também estarmos preparados para ela.

Com o aumento do uso da tecnologia da informação, novos problemas e desafios surgem diariamente para a sociedade: *malwares*, *spam*, *crakers*, engenharias sociais e outros. Cada vez mais, os profissionais de computação necessitam saber como ter segurança em suas aplicações. Estaremos construindo nosso conhecimento por meio de fóruns, leitura de artigos, reportagens, exemplificações e discussões. Para isso, temos o apoio do nosso ambiente virtual de aprendizagem, com o qual, sem dúvida, todos já devem estar habituados.

O grande empresário J. Willard Marriott disse certa vez: "A boa madeira não cresce com sossego; quanto mais forte o vento, mais fortes as árvores".

Portanto, esperamos que “soprem fortes ventos” em nossa caminhada, pois, assim, todos se tornarão valorosos, quer profissionalmente, quer pessoalmente.

Contem comigo, forte abraço!

Professor Fabrício Pelloso Piurcosky

INTRODUÇÃO

Na disciplina de Segurança e Auditoria de Sistemas estudaremos os conceitos e os tipos de ameaças, riscos e vulnerabilidades dos sistemas. Conceituaremos o que é segurança e os objetivos de se manter uma política que cuide disso. Também conceituaremos auditoria de sistemas e veremos a importância de implementar e planejar ações assim.

Teremos quatro unidades: na Unidade I, estudaremos o que é Segurança da Informação, veremos seu conceito, classificação, aspectos humanos, segurança física e lógica e o contexto da mesma em relação à Governança de TI.

Na Unidade II, abordaremos a importância da segurança no desenvolvimento de softwares. Abordaremos modelos de especificação de segurança, ambiente de desenvolvimento, segurança da aplicação. Também veremos os conceitos e os tipos de ameaças, riscos e vulnerabilidades.

Na Unidade III, conceituaremos o que é auditoria, destacando as metodologias existentes, ferramentas, técnicas, melhores práticas e outros aspectos ligados ao tema.

E, finalmente, na Unidade IV, falaremos sobre política de segurança, apresentando exemplos de ciclo de vida de desenvolvimento seguro, NBR ISO/IEC e Planos de Segurança.

A Ementa de nossa disciplina é: Os conceitos e os tipos de ameaças, riscos e vulnerabilidades dos sistemas de informação. O conceito e os objetivos da segurança de informações. O planejamento, implementação e avaliação de políticas de segurança de informações. O conceito e os objetivos da auditoria de sistemas de informação. O planejamento, implementação e avaliação de auditorias de sistemas de informação.

DINÂMICA

Nossa disciplina terá atividades pelo ambiente virtual e encontros presenciais. As atividades serão publicadas com prazos de início e término (por meio da agenda da página principal). Ressalto que os prazos serão seguidos rigorosamente. Teremos como local de comunicação, exclusivamente, o ambiente, pois lá encontramos todas as ferramentas (correio, mural, fórum, portfólio e bate-papo) necessárias para tal. Assim o e-mail externo não será utilizado. Disponibilizarei um cronograma com todas as atividades que deverão ser cumpridas, além de uma sugestão de ritmo de leitura do nosso material.

AVALIAÇÃO

Na Etapa I (avaliação a distância), serão distribuídos 45 pontos nas atividades orientadas como: produção, interação, análise e aplicação dos conhecimentos adquiridos; auto-avaliação; fóruns; chats e portfólio. Na Etapa II (avaliação presencial), serão distribuídos 55 pontos, em avaliações que exigirão uma revisão do guia de estudo que será trabalhado durante o módulo. Poderão ser utilizadas provas individuais, em duplas, relatórios e grupos de discussão. As provas terão questões abertas e fechadas.

1 SEGURANÇA DA INFORMAÇÃO

META

Apresentar conceitos de Segurança, características da Informação e seu Ciclo de Vida, Segurança em Ambiente Físico e Lógico, Segurança no Contexto da Governança de TI

OBJETIVOS DA UNIDADE

Esperamos que, após o estudo do conteúdo desta unidade, você seja capaz de:

- conceituar segurança da informação;
- identificar as características da informação, seu ciclo de vida e a importância dela em ambientes físico e lógico;
- conceituar a segurança no contexto da governança de TI.

1.1 Conceitos e Princípios de Segurança da Informação

Com certeza um dos assuntos mais discutidos e importantes na atualidade é Segurança da Informação. Recentemente, a revista InformationWeek, publicou uma retrospectiva de alguns dos maiores acontecimentos mundiais ligados à tecnologia e olhe só o que temos:

Figura 1: Retrospectiva de Acontecimentos (Fonte: Revista InformationWeek, 2009)

Temos uma notícia que mostra a importância do tema que estamos estudando. Se não conseguiu observar, volte e olhe mais uma vez a figura. Notou agora? Isso mesmo! O ataque ao World Trade Center mudou a forma das empresas pensarem em segurança e contingência.

Pense um pouco no caso e com base no que leu a respeito, reflita um pouco agora na importância do tema que estudaremos.

Antes de passarmos diretamente ao tema de segurança, vamos relembrar alguns conceitos importantes.

De acordo com Filho (2008), informação é a forma final da transformação ou processamento dos dados originais, em algo com valor e significado para o usuário. Todo o dado trabalhado, útil, tratado com valor significativo atribuído ou agregado a ele e com um sentido natural e lógico para quem usa a informação.

Assim, estas têm importância fundamental nas empresas. Vivemos a chamada Sociedade da Informação e do Conhecimento (informação disponível e fluindo a toda velocidade), mercados globalizados (a informação é estratégia de competição). Filho (2008) destaca a importância da

informação para as empresas, evidenciando que é um ativo nas organizações e estas devem tratá-la como um bem, pois representa a inteligência competitiva. Dessa forma, para se montar uma estratégia ou um planejamento é vital ter total confiança nas informações que transitam nos sistemas de informação da empresa, afinal de contas, elas serão a base para a tomada de decisão.

Mas e quanto ao valor da informação? Você sempre lê que informação é o bem mais precioso, mas como quantificar? Não é difícil, analise comigo:

- Se uma informação de previsão de mercado é usada para produzir um novo produto que irá responder por um lucro X, neste caso, essa informação possui esse valor X.
- Se um novo sistema computadorizado de pedidos custa R$ 100.000,00, mas isto poderá gerar um adicional de R$ 150.000,00 nas vendas, o valor adicionado pelo novo sistema é de R$ 50.000,00

Vários autores já concordam que o valor econômico advindo da geração, do uso e da venda da informação está crescendo muito mais depressa que o valor agregado pela produção tradicional de bens e serviços. Por essa ideia, já consegue notar como esse tema vai ganhar importância cada vez mais?

Temos dois exemplos de como medir o valor de uma informação. Conseguiria realizar isso tendo como base algum sistema implantado em sua empresa ou que você tenha criado ou baseado em alguma pesquisa.
Vamos lá, mãos à obra! Tente mensurar o valor de uma informação. Faça isso em um documento *.doc* e poste em seu portfólio individual.

Lyra (2008) destaca que a segurança da informação tem vários aspectos importantes, mas sem dúvida três deles se destacam:

- Confidencialidade → capacidade de um sistema de permitir que

alguns usuários acessem determinadas informações ao mesmo tempo em que impede outros, não autorizados a veja.

- Integridade → a informação deve estar correta, ser verdadeira e não estar corrompida.
- Disponibilidade → a informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.

Estes três aspectos são os principais, muitos autores concordam que se a informação contiver todos eles podem tratá-la como uma informação segura.

No entanto, além destes três aspectos, ainda temos:

- Autenticação → garantir que um usuário é de fato quem alega ser;
- Não-Repúdio → capacidade do sistema de provar que um usuário executou uma determinada ação;
- Legalidade → garantir que o sistema esteja aderente à legislação pertinente;
- Privacidade → capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações;
- Auditoria → capacidade do sistema de auditar tudo que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

Um bom exemplo de um sistema com privacidade trata-se das urnas eletrônicas utilizadas pelo TSE. Utilizamos o sistema para realizar nosso voto não relacionando o usuário com a ação executada, garantindo assim que o nosso voto seja secreto.

1.2 A Segurança e o Ciclo de Vida da Informação

Quando realizamos um levantamento de informações para uma implantação ou um desenvolvimento de um sistema, é vital ter uma preocupação em como a informação irá fluir na organização. Assim, a identificação das necessidades e dos requisitos da informação é quem ditará o ciclo da mesma. Lyra (2008) destaca a sequência a que a informação é

submetida: obtenção, tratamento, armazenamento, distribuição, uso e descarte da informação. Analise a figura abaixo:

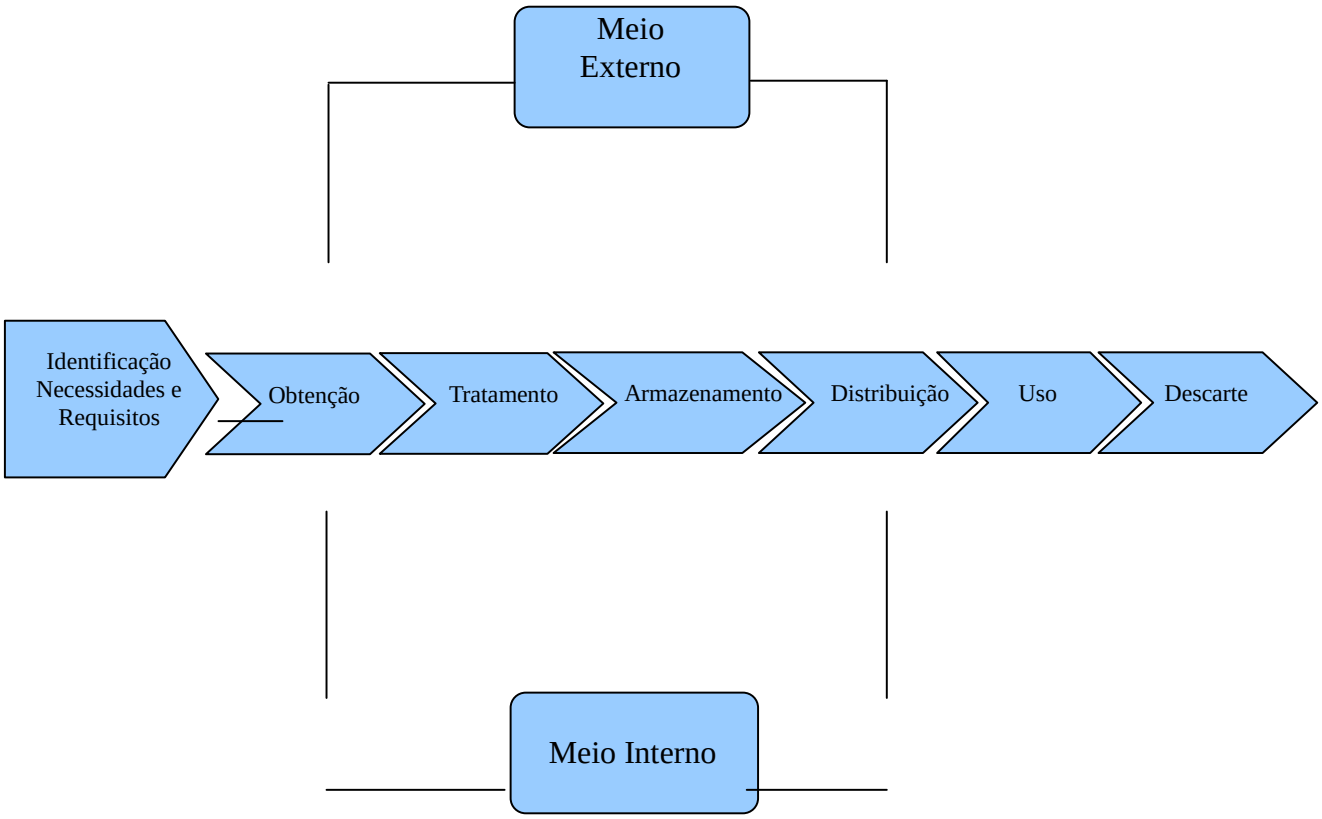

Figura 2: Ciclo de Vida da Informação. (Fonte: Lyra, 2008)

Conforme a Figura 2, a identificação das necessidades e requisitos é fundamental para que o restante do projeto consiga uma boa fluidez e sucesso. Você já deve ter lido, estudado ou praticado algumas das técnicas que auxiliam neste processo. Podemos até mesmo destacar algumas, tais como a observação pessoal, entrevistas e questionários. Não há uma "receita de bolo" que devemos seguir sempre que precisamos realizar um levantamento de informações. Isso dependerá da situação do ambiente, do tempo que temos e da possível reação dos usuários. A figura também serve para refletirmos um pouco em como é difícil darmos segurança à informação. Observem que tanto na Obtenção como na Distribuição há relacionamentos com o meio externo e com o meio interno. Estes são dificultadores que não podem ser restringidos, pois ao mesmo tempo em que podem trazer problemas, eles também podem ser importantes na obtenção e seleção da informação. Lyra (2008) explica cada componente deste ciclo de vida:

- Identificação das necessidades e dos Requisitos → geralmente dentro de uma organização nossa principal função é desenvolver produtos e serviços informacionais com especificidade. Isso pode ser desde um simples relatório, um produto ou um novo processo. Será que você conseguiria fazer isso sem conhecer as necessidades e as características que envolvem a situação? De forma alguma, por isso é importante gastar tempo nesta etapa.

- Obtenção → nesta etapa são desenvolvidos procedimentos para a captura e recepção da informação originária de uma fonte externa ou mesmo em como ela será criada. Para o primeiro caso (fonte externa), é necessário que você se preocupe com a integridade da informação, garantindo que ela é genuína, produzida por uma pessoa ou entidade autorizada e que, portanto, está completa e compatível com os requisitos que foram levantados anteriormente.

- Tratamento → antes da informação ser utilizada ou consumida, é imprescindível que ela seja classificada, formatada, organizada. Também é interessante torná-la mais acessível e de fácil utilização. Mas aqui vai um alerta! Depois de tratada, é preciso dar a garantia de que ela continue íntegra, bem como confidencial.

- Distribuição → esta etapa é um verdadeiro desafio! Mais à frente veremos o por quê. Consiste em levar a informação até quem será seu consumidor. Para isso quanto mais capilar for a rede de distribuição, melhor e mais seguro será.

- Uso → aqui é que veremos o quanto a informação será útil para gerar valor à organização. Devemos aplicar, portanto, os conceitos de disponibilidade, integridade e confidencialidade.

- Armazenamento → importante para que futuramente a informação possa ser utilizada novamente. Ela será mais onerosa se a informação estiver em vários formatos ou mídias. A preocupação com a integridade e a disponibilidade deve ser constante, bem como confidencialidade, se a mesma for sigilosa.

- Descarte → Beal (2005) diz que quando uma informação torna-se obsoleta ou perde a utilidade para a organização, ela deve ser objeto de processo de descarte obedecendo a normas legais, políticas operacionais e exigências internas. Isso ajudará no processo de gestão da informação.

O Descarte é uma etapa muito importante para as organizações, uma vez que auxilia a gestão da informação. Faça uma pesquisa sobre o tema e apresente quais são algumas das formas que as empresas utilizam para a realização dessa etapa e os cuidados necessários para tal.

1.3 Classificação e Controle dos Ativos de Informação

De acordo com Lyra (2008), a classificação da informação é o processo pelo qual estabelecemos o grau de importância das informações frente a seu impacto no negócio ou processo que elas suportam. Entendemos assim que, quanto mais ela for estratégica ou decisiva para o negócio mais importante ela será.

A figura 3 ilustra como os ativos da informação podem ser divididos em grupos:

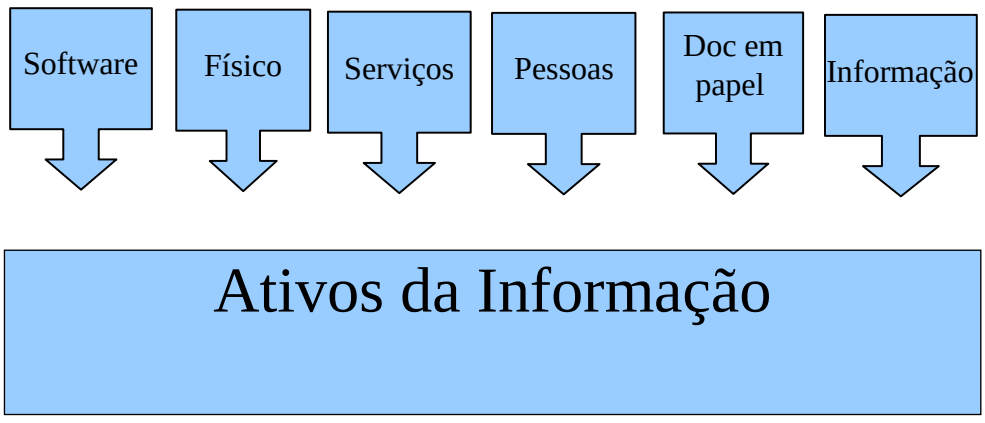

Figura 3: Ciclo de Vida da Informação. (Fonte: Lyra, 2008)

Você não consegue classificar os ativos da informação sem ter um bom conhecimento do negócio. Isso permitirá que você julgue o grau de importância de cada um. Outro ponto que é preciso levar em conta é a definição clara dos critérios de classificação que serão adotados, regras, exigências e normas corporativas.

O ideal seria que todos conseguissem ler a Norma ISO 17.799, no entanto, ela sai a mais de R$150,00 atualmente. Assim coloquei em nossa Midiateca um checklist de uma auditoria sobre os itens mais importantes. Assim você poderá ter uma ideia do que se trata. Vamos à leitura, pois citaremos várias vezes no decorrer do guia!

1.4 Classificação do Ativo da Informação

Lyra (2008) destaca que existem várias formas de classificar o ativo da informação, no entanto, esta não deve ser difícil de compreender e deve constar na política de segurança. Deve ter um número equilibrado de níveis de classificação e servir para demonstrar a diferenciação entre a importância dos ativos. Esta, então, deve estar centrada em quatro eixos: confidencialidade, disponibilidade, integridade e autenticidade. Vamos então tratar de cada um desses quatro eixos.

1.4.1 Quanto à Confidencialidade

Nível 1: Informação Pública → aqui devem estar os ativos públicos ou não classificados. Como entendemos isso? Ora, são informações que se forem divulgadas fora da organização não trarão impactos para o negócio. Não é vital a integridade e seu uso é livre.

Um bom exemplo de informação pública trata-se dos folders corporativos, brochuras, etc.

Nível 2: Informação Interna → ativos cujo acesso do público externo deve ser evitado, mas se por acaso estes venham a ter acesso, as consequências não são críticas ou preocupantes

Listas de Telefones e ramais, agendas dos executivos, planejamento semanal

Nível 3: Informação Confidencial → os ativos devem ter acesso restrito dentro da organização e protegidos do acesso externo. O acesso não autorizado pode trazer comprometimento às operações da organização e causar até mesmo perdas financeiras.

Dados de clientes, senhas de acesso, informações sobre vulnerabilidades da organização

Nível 4: Informação Secreta → nesse nível o acesso tanto interno como externo pode ser crítico para a organização. Deve-se controlar o número de pessoas que tem acesso a ela, a integridade das informações e criar regras restritas para o uso das mesmas.

Podemos citar informações de concorrentes, contratos confidenciais, informações estratégicas, etc.

1.4.2 Quanto à Disponibilidade

Geralmente sentimos falta ou avaliamos o quanto uma informação é importante quando precisamos dela e não conseguimos acessá-la.

Já aconteceu isso com você? Com todos nós. Quem já não precisou acessar um site que disponibilizaria o resultado de um processo de seleção ou de um concurso? Se a informação atrasa 10 minutos do horário proposto ficamos totalmente indignados. Nesse momento, quanto valeria essa informação? Valeria muito, não é mesmo?

Agora, pense em outra situação: você acessa uma informação nesse instante e em meia hora ela não está mais disponível. Qual a falta que a informação faz? Isso dependerá da importância dela. Mas imagine que você é administrador de um site de e-commerce e um cliente solicitou seu número de pedido de compra, mas ao entrar no site não consegue recuperar esse número. Isso poderia causar alguns problemas.

Dessa forma, podemos estabelecer uma ordem para recuperação de informações em casos de indisponibilidade, seria assim:

- Nível 1 → Informações que devem ser recuperadas em minutos
- Nível 2 → Informações que devem ser recuperadas em horas
- Nível 3 → Informações que devem ser recuperadas em dias
- Nível 4 → Informações que não são críticas

Não há dúvidas de que a classificação dos níveis de uma informação não deve ser feita apenas pela equipe de Tecnologia da organização. Esta deve ser feita por um comitê específico da empresa.

Faça uma pesquisa e aliste pelo menos duas formas de recuperação de informação existentes no mercado. Tente se possível, listar o custo dessas formas de recuperação.

1.4.3 Quanto à Integridade

A depender da decisão a ser tomada, se a informação estiver errada, isso pode significar transtornos e problemas sérios. Assim, conseguir realizar um trabalho de identificar as informações que são relevantes ao negócio fará com que você consiga direcionar seus esforços para os alvos corretos, permitindo controlar, prevenir, detectar e corrigir as informações que a empresa, de fato, precisará.

1.4.4 Quanto à Autenticidade

A ISO 17.799 recomenda que tanto dados como informações que serão acessadas por meios externos devem apresentar requisitos de verificação da autenticidade. Dessa forma, mais uma vez você deverá estabelecer em conjunto com a empresa quais as informações que serão tratadas neste contexto.

1.4.5 Monitoramento Contínuo

Lyra (2008) argumenta que após a classificação dos ativos da informação, é necessário elaborar e manter procedimentos de reavaliação periódica dos mesmos. Como fazer isso? Tanto a área de segurança como os proprietários da informação, deve reavaliar a pertinência da categoria atribuída a cada ativo para assegurar que os mesmos estão adequadamente classificados.

Vamos fazer uma avaliação das informações em nosso ambiente?

Tarefa 1: Divida os ativos da Informação

Tarefa 2: Classifique o ativo software quanto à Confidencialidade

Tarefa 3: Classifique o ativo software quanto à Disponibilidade em todos os níveis

1.5 Aspectos Humanos da Segurança da Informação

Filho (2008) destaca que a segurança da informação se preocupa com os objetivos de garantir a continuidade do negócio, minimizar as perdas do negócio pela prevenção e redução do impacto de incidentes de segurança, habilitar as informações a serem compartilhadas enquanto estabelece a proteção da informação e do acesso aos Sistemas de Informações.

Isso se torna cada vez mais difícil porque o cenário da tecnologia é mutante e evolutivo. Há algumas décadas a realidade de tecnologia e as preocupações trazidas por ela eram totalmente diferentes das principais atenções que precisamos ter hoje. Analise que na maioria das casas já existe uma rede de Computadores, a Evolução da Internet é algo mundial e a diversidade de sistemas.

Assim, dizemos que a informação é segura e que cumpre seu propósito quando informação certa é comunicada às pessoas certas (na hora certa).

Pessoas são os elementos centrais para que a segurança da informação aconteça. Todos os incidentes sempre envolverão pessoas, seja pelas vulnerabilidades que foram exploradas, seja pelas ameaças que exploram as vulnerabilidades.

É muito comum a ideia de que manter a informação segura é papel obrigatório da equipe de tecnologia. Além disso, muitos ainda acham que somente eles devem se preocupar com isso. Na verdade, essa preocupação deve ser de toda a organização. Se isso não estiver claro em um ambiente corporativo, pode-se investir milhões em segurança que o retorno não será o esperado.

Acesse o site do CERT.BR (http://www.cert.br/stats/incidentes/) e analise os incidentes de segurança registrados no ano de 2009. Compare com os incidentes reportados nos últimos 5 anos. Analise que ataques tem crescido mais e veja como cada dia que passa é mais difícil manter a informação segura.

Com o crescimento dos números de vírus e de casos de invasão, cada vez mais veremos a figura de um novo profissional nas empresas: *Security Officer* ou *CSO (Chief Security Officer).* Este tem o papel de coordenar, planejar, implementar, monitorar e melhorar o Sistema de Segurança da Informação. Ele deve ter as seguintes atribuições:

- Coordenar área de segurança e de infraestrutura organizacional
- Planejar investimentos de segurança
- Definir índices e indicadores para segurança da corporação
- Definir, elaborar, divulgar, treinar, implementar e administrar a política de segurança, plano de continuidade de negócios e de contingência
- Investigar incidentes de segurança
- Analisar riscos envolvendo segurança

Pense nas atribuições que falamos para o profissional de segurança. Quais delas você já fez na empresa em que atua? Qual delas considera mais importante? Que ação prática envolvendo os usuários da empresa que você atua poderia ser implementada?

O *SANS Institute* define Engenharia Social como "a arte de utilizar o comportamento humano para quebrar a segurança sem que a vítima sequer perceba que foi manipulada." O *CERT.BR* define como "um método de ataque 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 aos ativos da informação".

Esta prática acaba fazendo com que pessoas desavisadas passem informações importantes, pois confiam demais no seu atacante. Ela pode ser dividida em duas categorias: física e psicológica.

Lyra (2008) apresenta as ações relacionadas à categoria física como sendo: procura de informações no lixo, presença física, observação do comportamento, escuta de conversa telefônica, busca de papéis e relatórios

sobre as mesas da organização, uso de portas USB e roubo de pen drives.

Nas questões psicológicas o problema está relacionado ao comportamento humano e à tendência do ser humano em ser prestativo, cortês e de não ver maldade nas pessoas. Dessa forma, o atacante consegue informações para preparar o seu ataque.

Você recebe um telefonema de um pesquisador que é muito educado e fala muito bem, aos poucos ele pode extrair informações tais como tipo de rede, sistema operacional utilizados, etc.

Não há dúvidas de que o elo mais fraco do sistema é quando este interage com humanos. Dessa maneira, é preciso desenvolver interfaces que façam a segurança de forma menos inoportuna e intrusiva.

Quando se fala sobre pessoas, devemos também lembrar que os problemas de comportamento acontecem em qualquer nível, desde os que estão no topo até os que nem mesmo utilizam computador. Nesse aspecto, pense no zelador que vai abrir a sala de servidores para limpeza do chão e que por descuido deixa a porta aberta enquanto vai buscar a vassoura em outro lugar do prédio. Nestes poucos minutos é como se a empresa estivesse totalmente desprotegida ou escancarada.

Em nossa Midiateca, temos um artigo chamado Engenharia Social. Ele traz informações importantes sobre as formas de ataque mais comuns e outras informações sobre essa prática cada vez mais comum.

A figura 4 retrata um ambiente que em alguns aspectos podemos até ver em nosso dia a dia. Poste no portfólio individual o que está sendo pedido e tente apontar 5 ações urgentes a serem tomadas neste ambiente que não envolveria custos para a empresa na sua implantação.

1.5.1 Segurança nos Termos, Condições e Responsabilidades de Trabalho

É necessário precaver-se para que exista um mínimo de garantia de responsabilidade daqueles que utilizarão a informação da empresa. Deve ser claro que é responsabilidade de todos a segurança da informação e que as ações dos funcionários devem ser de acordo com a política de segurança. Lyra (2008) destaca que os termos e condições de trabalho devem conter o que está relacionado ao cargo, as obrigações, cuidados e condutas relativas à segurança da informação. Tais itens devem estar registrados no contrato de trabalho. A isso, pode ser adicionado ainda um termo de confidencialidade por ocasião da admissão do colaborador.

1.5.2 Segurança no Processo de Seleção de Pessoal e Treinamento de Usuários

O processo de seleção deve ser alvo de atenção da segurança da informação uma vez que é a porta de entrada da organização. Nem sempre referências, cópias de documentos e currículo é suficiente para ter confiança no entrevistado. É preciso ações de checagem de informações, confirmação

de dados, entrar em contato com as pessoas e empresas citadas, confirmar diplomas nas instituições de ensino alistadas, verificar conduta, etc.

Não podemos falar em segurança da informação sem mencionar algo fundamental que é treinar, educar e conscientizar os usuários. Todos os colaboradores (internos e/ou externos) devem conhecer a política de segurança da empresa, diretrizes, entender os conceitos de confidencialidade, integridade e disponibilidade e os desdobramentos das mesmas. Somente assim pode-se cobrar uma conduta compatível com as boas práticas de segurança. Um erro bastante comum é o de fornecer treinamento num determinado período e não repetir os mesmos. Ora, as pessoas mudam, as formas de ataque mudam, os sistemas mudam. Isso implica então, em treinamentos periódicos e sistemáticos, desenvolvendo a cultura da segurança da informação.

Entrevista de Kevin Mitnick à CNN:
http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html

Um bom mercado de atuação é o de fornecer treinamentos e capacitações de segurança para as empresas. Não são raras as empresas e órgãos que não detém nenhum tipo de cuidado com as suas informações. Recentemente fui convidado para ministrar uma palestra sobre Segurança e a grande maioria dos funcionários não tinha nenhum tipo de cuidado com as senhas pessoais do sistema. Algo que encaramos como premissa básica de segurança. Eram vários os casos de funcionários que acessavam o sistema com o usuário e senha do colega.

No ano passado convidei um ex-aluno do curso de Ciência da Computação do Unis para ministrar uma palestra. Na oportunidade ele falava como Gerente de uma Unidade Bradesco de São Paulo e nos falou um pouco sobre as políticas de segurança da entidade. Entre as ações citadas, ele nos mostrou que se o funcionário se levantar para buscar uma água ou um café é norma da empresa ele bloquear o computador, se não o fizer ele é advertido. Isso é uma norma imposta pela política de segurança.

1.6 Segurança do Ambiente Físico

Um problema comum que deve ser evitado é o de preocupar-se somente com a segurança lógica. Muitas vezes são esquecidas as medidas de prevenção, detecção e reação a possíveis incidentes de segurança física dos ativos.

Sobre isso a ISO 17.799 chama de barreira de segurança qualquer medida preventiva que sirva para impedir um ataque a algum ativo da informação. Mas o que poderia ser encarado como barreira de segurança ou medida preventiva? Estas podem ser de três tipos:

- Físicas – muros, cercas, trancas
- Lógicas – senhas de *logon*
- Combinação das Anteriores - *token*

Além de tais cuidados é importante definir um perímetro de segurança. Mas o que vem a ser isso? Trata-se de um contorno ou linha imaginária que delimita uma área ou região separada de outros espaços físicos por um conjunto de barreiras de segurança. E aqui vai uma dica: quanto mais clara for a definição desse perímetro mais acertados serão os investimentos e as barreiras a serem implementadas. Surge outra pergunta: Que perímetros podem ser protegidos? Bem, isso dependerá de cada situação, mas podemos citar prédios, geradores, cofres, etc. Mas, se pensarmos somente na informação e sua segurança, teremos os perímetros que seguem nos próximos itens do guia.

1.6.1 Segurança em Escritórios, Salas e Instalações de Processamento de Dados

A ISO 17.799 recomenda a elaboração de um projeto de áreas de segurança. Este deve contemplar escritórios fechados ou com várias salas dentro de um perímetro seguro que considere as ameaças de fogo, poeira,

fumaça, vibração, vazamento de água, explosão, manifestações civis ou desastres naturais.

É necessário ainda um cuidado especial com equipamentos instalados em áreas comuns. Nesses casos é muito útil aplicar medidas específicas de proteção contra acesso não autorizado, dano ou furto. A norma sugere, inclusive, mecanismos de bloqueio, como *time-out* e treinamento específico para prestadores de serviços de limpeza e manutenção.

Não é difícil encontrarmos empresas em que a impressora fica numa área de livre circulação. Conseguem perceber o perigo que isso tem? Alguém manda imprimir um documento importante, alguém passa uma ligação importante. Enquanto atende essa ligação, que pode ser demorada pode passar alguém e levar a informação impressa. E grandes problemas podem surgir.

1.6.2 Segurança de Equipamentos

Um medo mórbido que todos nós temos é o de falha de energia. Geralmente isso acontece quando menos esperamos, e, detalhe, quando a energia retorna ela traz consigo uma série de problemas. A norma ISO mais uma vez fornece auxílio. Ela aponta algumas opções para garantir a continuidade do fornecimento elétrico, veja:

- Alimentação com múltiplas fontes
- Uso de *nobreaks*
- Geradores de reserva

Outro aspecto que você não pode esquecer é o *hardware.* Estes são defeitos inerentes, podem estar funcionando muito bem e podem não estar no minuto seguinte. Assim, algumas medidas podem ser tomadas, como por exemplo:

- Planejamento de manutenções periódicas
- Treinamento de melhores práticas de utilização dos equipamentos

1.6.3 Segurança de Documentos em Papel e Eletrônicos

Geralmente quando se fala em segurança da informação, instantaneamente pensamos na segurança através do computador. No entanto, de nada adianta termos um perfeito esquema de segurança para os meios eletrônicos ou que geram a informação se não há nenhuma estrutura segura para a guarda das informações físicas.

Lyra (2008) propõe a adoção de procedimentos de tratamento das cópias, armazenamento, transmissão e descarte seguros. É necessário preocupar-se com umidade, acidez do papel, técnicas de restauração, etc. É lógico que de acordo com o negócio da organização será decidido que papéis devem ser guardados e existe uma lei que rege sobre o tempo de guarda de cada documento. Se a organização precisar guardar documentos ela então precisa dispor de controles, que podem ser:

- Uso de rótulos para identificar documentos
- Política de armazenamento de papéis em local adequado
- Procedimentos especiais para impressão, cópia e transmissão
- Recepção e envio de correspondências sigilosas

É interessante ainda criar procedimentos especiais para armazenamento e manipulação de papéis sensíveis à luz e ambiente como cheques e notas fiscais.

Um bom mercado de atuação hoje em dia é o de digitalização de documentos. Há empresas especializadas nisso. Pense em uma instituição de ensino como o Unis. Existe há mais de 40 anos. Imagine que amanhã apareça um aluno que perdeu o seu diploma e necessite de uma cópia ou

> uma nova emissão. Detalhe: ele formou em Engenharia Mecânica em 1975, por exemplo. Para terem uma ideia, entrei como aluno no Unis em 2000 e atuo profissionalmente lá desde 2003. De 2000 para cá, o Unis trocou de Sistema de Informação 3 vezes. Perceberam a importância de manter em segurança os documentos impressos? No exemplo que citei a instituição na oportunidade não possuía nem mesmo sistema computacional. Uma boa saída para garantir essas informações seria a digitalização de todos os documentos que a instituição possui. Agora imaginem quanto mercado este tipo de ação tem.

Mas e quanto aos documentos salvos na rede da empresa ou mesmo nos computadores?Estes documentos eletrônicos trazem três preocupações:

- dispor de um aparato de tecnologia que os deixe visíveis e compreensíveis aos seus usuários;
- manter a integridade da informação, pois o documento eletrônico pode ser mais facilmente alterado que o documento em papel;
- não esquecer das evoluções tecnológicas (migrar documentos armazenados em disquetes e fitas);
- estabelecer procedimentos de *backup.*

Sobre o último item, é essencial criar como isso vai funcionar e controlar também o acesso a essas informações e quando e como devem ser descartadas.

1.6.4 Segurança no Cabeamento

Mais uma vez a norma ISO nos auxilia, ela recomenda controles para cabeamento elétrico e de telecomunicações:

- sempre que possível utilizar linhas subterrâneas;
- proteger cabeamento de rede contra interceptações não autorizadas ou danos;
- separar cabos elétricos dos cabos de comunicação;
- uso de conduites blindados e salas trancadas para os sistemas críticos.

1.7 Segurança do Ambiente Lógico

1.7.1 Segurança em Redes

Lyra (2008) destaca que as preocupações neste aspecto passam pelos problemas de autenticação de usuários e equipamentos e de restrição de acesso os usuários aos serviços autorizados, buscando com isso estabelecer interfaces seguras entre a rede interna e a rede pública ou de outra organização. A norma mais uma vez nos ajuda. Ela menciona diversos mecanismos de proteção de redes, tais como criptografia, *tokens*, VPN's, antivírus, *gateways* e *firewalls*, que podem controlar o tráfego, estabelecer rotas de redes obrigatórias e dividir grandes redes em domínios lógicos separados, sendo que com isso pode-se dar proteção por perímetros de segurança específicos.

Embora alguns dos mecanismos de proteção você já conheça, convém que o apresentemos para relembrar alguns conceitos.

Quando a norma cita *firewall*, isso representa recursos de segurança com objetivo de controlar o acesso às redes. Serve como uma barreira de proteção entre um computador e seu ambiente externo. Com isso, é possível examinar e bloquear o tráfego. Mas que desvantagem esse mecanismo traz? Se você respondeu gargalo na rede, acertou. Pelo fato de todo tráfego passar por ele, é necessário dimensionar de forma correta o seu serviço, senão fatalmente ocorrerá lentidão na rede.

Já os perímetros lógicos ou zonas desmilitarizadas (DMZ), protegem o computador ou segmento da rede que fica entre uma rede interna e a

Internet. Assim, podemos entender que ela atua como intermediária tanto para o tráfego de entrada quanto para o de saída. As VPN's é outra alternativa para racionalizar os custos de redes corporativas, dando confidencialidade e integridade no transporte de informações por meio das redes públicas. Há vários exemplos de softwares de VPN's que criam túneis virtuais criptografados entre os pontos autorizados para a transferência das informações.

Em grupo vocês deverão fazer uma pesquisa sobre as outras formas de mecanismos de segurança abaixo:

1 – Criptografia
2 – Esteganografia
3 – Assinatura e Certificado Digital
4 – Sistemas de Detecção de Intrusos

Pense que vocês foram designados responsáveis pela empresa para realizar um curso sobre segurança da informação. Para isso vocês deverão preparar uma apostila que será lida por todos os funcionários, abordando os quatro itens acima.
Mãos à obra! Ao final poste no portfólio de grupo

1.8 Controle de Acesso

Se não houver um controle de acesso à informação, é impossível garantir os três princípios básicos de segurança. Porém, este controle não pode "engessar" a organização, não deve impedir os processos de negócio da mesma.

O item 11 da norma citada é todo dedicado a esse assunto. Recomenda que nada deve ser permitido, tudo deve ser proibido, a menos que se tenha permissão expressa para tal.

1.8.1 Controle de Acesso Lógico

Para esse controle é preciso que você preste atenção a recursos comumente usados como arquivo-fonte, sistema operacional, bancos de dados, utilitários, etc. Para estes ativos temos de estabelecer, de acordo com Lyra (2008), os seguintes controles:

- Identificação e Autenticação do Usuário → a identificação se faz através da criação de contas de usuários com uma identificação única. Dessa forma, é possível autenticar o usuário através da senha de acesso que o próprio usuário sabe. As melhores práticas recomendam troca periódica de senhas, identificação de senhas fáceis, bloqueio de acesso após certo número de tentativas erradas. Se possível, é muito interessante que você agregue autenticação baseada em algo que o usuário tem (*token*, *smart card*, cartão com *chip).* Além disso, cada vez mais comum será a utilização do que o usuário é. Características físicas como impressão digital, reconhecimento facial, voz, íris, etc. são cada vez mais comuns.
- Administração dos Privilégios de Usuários → é importante realizar uma administração adequada dos privilégios concedidos. O uso de perfis e grupos de usuários com diferentes necessidades e permissões permite o gerenciamento de forma mais eficiente dos privilégios e os acessos aos ativos. Deve-se revisar frequentemente os perfis e os componentes dos grupos, uma vez que pessoas são trocadas de cargos e responsabilidades, são demitidas e nem sempre o departamento de tecnologia é comunicado.
- Monitoração do Uso e Acesso ao Sistema → é imprescindível que os sistemas possuam registros das atividades de cada usuário. Embora isso represente uma carga de informações a mais no servidor, afetando sua *performance*, esses mecanismos, ou *log's*,devem registrar data e hora, tipo de atividade e eventuais alterações de dados. Isso será importante para a comprovação de uma futura auditoria em caso de violação da integridade da informação. Hoje há sistemas que

permitem o cadastro do intervalo de tempo em que o usuário está autorizado a utilizar o sistema.

1.8.2 Controle de Acesso Físico

É necessário controles de entrada apropriados para evitar que pessoas não autorizadas obtenham acesso aos recursos de informação. Estes precisam ser proporcionais à importância da informação ou à criticidade da mesma. Como exemplo, temos crachás de identificação, cartão com PIN, dispositivos de senha nas portas de acesso, etc.

1.9 A Organização da Segurança

Sêmola (2003) propõe um modelo de gestão corporativa de segurança da informação cíclico e encadeado, este prevê que cada etapa gera resultados que serão importantes para a próxima. Ele é formado pelas etapas que seguem:

- Comitê Corporativo de Segurança da Informação → papel de orientar as ações corporativas, medindo os resultados parciais e finais; alinhar o plano de ação às diretrizes estratégicas do negócio; coordenar os agentes de segurança em seus Comitês Interdepartamentais; e garantir o sucesso de implantação, pois dará autonomia na gestão dos seus associados e promover a consolidação do modelo como um processo auto-gerido
- Mapeamento de Segurança → identificar o grau de relevância e as relações diretas e indiretas entre os diversos processos de negócio, perímetros e infraestruturas; inventariar os ativos físicos, tecnológicos e humanos que sustentam a operação da empresa; identificar o cenário atual – ameaças, vulnerabilidades e impactos – e especular a projeção do cenário desejado de segurança; e mapear as necessidades e as relações da empresa associadas ao manuseio, armazenamento,

transporte e descarte de informações.

- Estratégia de Segurança → definir um plano de ação, geralmente plurianual, considerando todas as particularidades estratégicas, táticas e operacionais do negócio, bem como aspectos de risco físicos, tecnológicos e humanos; e criar sinergia entre o cenário atual e desejado, buscando apoio explícito dos executivos às medidas propostas.
- Planejamento de Segurança → organizar os Comitês Interdepartamentais, deixando claro as responsabilidades, escopo de atuação; iniciar ações preliminares de capacitação dos executivos e técnicos, com objetivo de direcionar para os desafios; elaborar Política de Segurança de Informação sólida, considerando as características de cada processo de negócio perímetro e infraestrutura, procurando criar diretrizes, normas, procedimentos e instruções que oficializarão o posicionamento da empresa destacando as melhores práticas; e realizar ações corretivas emergenciais de acordo com o que foi levantado no mapeamento.
- Implementação de Segurança → divulgar para toda a corporação a Política de Segurança, com vistas a torná-la um instrumento oficial; capacitar e conscientizar os usuários em relação ao comportamento; e implementar mecanismos de controle físicos, tecnológicos e humanos.
- Administração da Segurança → monitorar os controles que foram implantados, medindo eficiência e mostrando as possíveis mudanças que interferem no negócio; projetar a situação do Retorno sobre o Investimento (ROI), identificando os resultados alcançados; garantir a adequação e a conformidade do negócio com normas associadas, padrões e legislação; e manter planos estratégicos para contingência e recuperação de desastres.
- Segurança na Cadeia Produtiva → equalizar as medidas de segurança adotadas pela empresa aos processos de negócio comuns, mantidos junto aos parceiros da cadeia produtiva: fornecedores, clientes,

governo, etc. Isso deve ser com objetivo de nivelar o fator de risco sem que uma das partes exponha suas informações compartilhadas.

1.10 A Segurança no Contexto da Governança de TI

O Control Objectives for Information and Related Technology (COBIT) trata-se de um guia dirigido para a gestão de Tecnologia da Informação. Este é recomendado pelo *Information Systems Audit and Control Fundation* (ISACA) e possui uma série de recursos que podem servir como modelo de referência para a gestão. Inclui ainda controle de objetivos, mapas de auditoria, ferramentas para a sua implementação e técnicas de gerenciamento. É um meio de otimizar os investimentos, melhorar o ROI percebido com métricas para avaliação de resultados.

COBIT abrange quatro domínios:

- Planejar e Organizar → cobre o uso de informação e tecnologia e como isso pode ser usado para que a empresa atinja seus objetivos e metas. Como objetivos de alto nível para esse domínio estão: Definir um Plano Estratégico de TI e orientações; Definir Arquitetura de informação; Determinar o gerenciamento tecnológico; Definir os processos de TI; Gerenciar o investimento em TI; Comunicar os objetivos de gerenciamento e orientar; Gerenciar os recursos humanos de TI; Gerenciar a qualidade; Estimar e gerenciar os riscos de TI e Gerenciar projetos.
- Adquirir e Implementar → este domínio cobre os requisitos de TI, aquisição de tecnologia e sua implementação dentro dos processos de negócios da empresa. Foca ainda o desenvolvimento do plano de manutenção. Como objetivos de alto nível temos: Identificar soluções automatizadas; Adquirir e manter *software* de aplicação; Habilitar operação e uso; Obter recursos de TI; Gerenciar mudanças; Instalar e credenciar soluções e mudanças.

- Entregar e Dar Suporte → foca a execução de aplicações dentro do sistema de TI e seus resultados, além do suporte dos processos. Pode-se incluir questões de segurança e treinamento. Para esse domínio temos os seguintes objetivos de controle: Definir e gerenciar níveis de serviço; Gerenciar serviços de terceiros; Gerenciar *performance* e capacidade; Assegurar serviço contínuo; Assegurar segurança de sistema; Identificar e alocar recursos; Treinar usuários; Gerenciar serviços de escritório e incidentes; Gerenciar a configuração; Gerenciar problemas; Gerenciar dados; Gerenciar o ambiente físico e Gerenciar operações.
- Monitora e Avaliar → este domínio lida com a estimativa estratégica das necessidades da organização e avalia se o atual sistema atinge os objetivos que foram especificados para tal. Cobre ainda questões de estimativa independente da efetividade do sistema de TI e sua capacidade de estar alinhado às estratégias. Essa avaliação ainda é feita por auditorias internas e externas. Tem por objetivos de alto nível: Monitorar processos; Assegurar avaliação dos controles internos; Obter avaliação independente e Prover auditoria independente.

Em nossa Midiateca temos o texto COBIT. Apresenta de forma sucinta e muito clara essa ferramenta. Leitura Obrigatória.

Para mais detalhes sobre COBIT:
http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Outro modelo de referência para gerenciamento de TI é o ITIL.

Você deverá montar uma apresentação em *.ppt* sobre o tema acima e postar em seu portfólio individual. Ao final da

apresentação, não esqueça da bibliografia e um último slide comentando se em seu departamento você desempenha alguma ação parecida e se seria difícil implementar esse modelo.

CONCLUSÃO

A base de todos esse conceitos que vimos e revimos, pode-se observar como cada vez mais com a evolução dos dispositivos, a globalização e o contínuo aumento de uso da tecnologia vai ser ainda mais desafiador manter a informação segura. Nos Estados Unidos, os dados sobre roubo de identidade são cada vez mais alarmantes, a privacidade é cada vez menor. Assim, se as empresas não levarem a sério os investimentos em segurança e os departamentos de tecnologia não forem criativos grandes perdas acontecerão.

Vimos ainda que existe várias formas, e muitas delas são simples, de fornecer um nível melhor de segurança. Daqui para frente, veremos uma nova figura dentro das empresas, que é o profissonal responsável somente pela segurança da informação. Também é importante ressaltar o quanto a norma ISO 17.799 nos ajudou nas definições.

Mais à frente notamos que pessoas é o elo fundamental para ter segurança. Não basta apenas investimentos em segurança lógica, cada vez mais os incidente acontecem no meio físico, envolvendo pessoas. O alerta foi até mesmo envolvendo a contratação de pessoas.

O COBIT e o ITIL são os modelos mais amplamente usados no mundo. Muitas das ações propostas são práticas de nosso dia a dia, no entanto, precisamos colocar isso no papel, tentando tangibilizar nossas ações e criar um escopo de aplicação dessas práticas.

Enfim, concluímos que tanto as organizações como as pessoas não podem ignorar as normas de segurança e as boas práticas de uso da tecnologia. O preço pode ser altíssimo!

APONTAMENTOS SOBRE A PRÓXIMA UNIDADE

Em nossa próxima unidade veremos a importância de desenvolver software com técnicas de segurança. Veremos modelos de especificação de segurança para a aplicação, para o ambiente de desenvolvimento e no ciclo de vida da aplicação.

2 SEGURANÇA NO DESENVOLVIMETO DE SOFTWARES

META

Apresentar a importância da segurança no desenvolvimento de softwares. Modelos de especificação de segurança, ambiente de desenvolvimento, segurança da aplicação. Também veremos os conceitos e os tipos de ameaças, riscos e vulnerabilidades.

OBJETIVOS DA UNIDADE

Esperamos que, após o estudo do conteúdo desta unidade, você seja capaz de:

- construir um software através de um modelo de segurança;
- conceituar e identificar as maiores ameaças e riscos quanto à segurança

2.1 Modelos de Especificação da Segurança

Common Criteria é nome do padrão de mercado que deu origem à Norma ISO/IEC 15.408. Seu objetivo é fornecer um conjunto de critérios para especificar a segurança de uma aplicação de forma clara, estabelecendo características para o ambiente de aplicação e definindo formas de garantir a segurança da aplicação para o cliente final. Em suma, ele pode ser usado para desenvolver um sistema seguro ou ainda, realizar a avaliação de um já existente.

Mas aí você pergunta: o que faz com que um sistema seja seguro?

Este padrão nos dá resposta. Ele estabelece que qualquer sistema para ser seguro, precisa ter seu *Security Target* (objetivo ou alvo de segurança) elaborado. Este deve indicar quais aspectos de segurança foram considerados importantes para o sistema em questão.

Ele define ainda sete níveis de garantia de segurança. A cada nível há um maior rigor nos testes. Esses são chamados de EAL (do inglês Evalution Assurance Level, ou nível de garantia da avaliação) e são classificados entre os níveis 1 a 7, sendo o nível 7 o mais alto. Atingir este último nível não é fácil, envolve tempo e dinheiro. Podemos afirmar que atingir o nível 3 já seria bastante interessante para a maioria dos aplicativos comerciais.

É preciso dizer que aplicar a norma em questão em sua totalidade seria bastante oneroso. Embora seja muito interessante, é possível atingir um bom nível de segurança não sendo necessário aplicar a norma totalmente.

Albuquerque & Ribeiro (2002) apresenta um modelo mais simples, e, portanto, mais interessante e plausível de aplicação. Se for iniciar uma aplicação do zero, ele apresenta quatro passos, quais são:

- Especificar a segurança na fase de análise → gerar um documento de especificação utilizando a ISO/IEC 15.408 como guia. Não é necessário aqui seguir o padrão imposto por ela no que tange ao Security Target;
- Manter ambiente de desenvolvimento e testes seguros e capazes de

atender ao EAL3;

- Desenvolver aplicação utilizando boas práticas de programação e fazer uso dos requisitos de segurança → criar processo de desenvolvimento definido e planejar implantação dos requisitos especificados, e
- Testar sistema internamente → gerar as evidências para verificar aderência às especificações realizadas anteriormente, como EAL3.

Será que são os mesmos passos se a aplicação já estiver desenvolvida? Não, é necessário realizar algumas adaptações, que seguem:

- Especificar a segurança para a aplicação usando ISO/IEC 15.408;
- Levantar quais requisitos de segurança a aplicação possui e quais estão presentes em seu ambiente de desenvolvimento;
- Verificar se os requisitos implementados atendem à necessidade de segurança verificada na especificação inicial, e
- Escolher um nível de garantia de segurança (somente até EAL3, pois níveis 4 a 7 exigem testes e procedimentos durante a implementação e portanto inviáveis para aplicações prontas) e fazer os testes para garantir a segurança da aplicação.

2.2 Especificação da Segurança Desejada

Assim como na análise de sistemas, em segurança é também necessário conhecer as necessidades do cliente, bem como do usuário.

Essa preocupação com segurança é válida tendo em vista as legislações e políticas de segurança estabelecidas e as ameaças ao negócio. Dessa maneira, a primeira ação a ser feita é levantar as necessidades legais e as políticas de segurança que vertem sobre a aplicação. Também deve ser realizado um levantamento dos tipos de ameaças.

Com tais levantamentos em mãos, é hora de consolidar os objetivos de segurança. Cada um deles deve estar ligado a pelo menos uma ameaça ou a uma legislação ou norma.

2.3 Especificação da Segurança da Aplicação

Para conseguir realizar esta especificação é primordial identificar as ameaças, pontos críticos, os ativos valiosos, legislação aplicável e as medidas de contingência existentes no ambiente. (LYRA, 2008)

Como realizar isso?

Mais uma vez a norma ISO/IEC 15.408 nos auxilia. Ela sugere a realização de uma busca extensiva, passando por quatro aspectos:

- Política de segurança → documento de normatização, sendo importante levantar os motivos dos requisitos existirem;
- Ameaças → levantar somente as que são significativas, que podem ocorrer com maior probabilidade e com impacto;
- Objetivos de segurança → trata-se da segurança que será implementada;
- Premissas → ambiente esperado para a construção do sistema, lembrando que deve ser autorizado pelo usuário;
- Estratégia → procurar atender cada objetivo de segurança anterior.

2.4 Segurança do Ambiente de Desenvolvimento

Lyra (2008) diz que não é possível desenvolver uma aplicação segura em um ambiente não seguro. Abaixo temos um modelo esquemático de como seria esse ambiente, tendo por base as normas:

Gerência de Configuração	
Objetivo	Preservar Integridade do Sistema
Como?	Prevenindo mudanças, acréscimos e exclusões sem autorização na documentação do sistema
Distribuição	
Objetivo	Não comprometer a transição entre desenvolvimento e a produção
Como?	Assegurar versão com especificações de segurança

Desenvolvimento	
Objetivo	Representar as funcionalidades de segurança em todas as fases de desenvolvimento
Como?	Particionar as especificações de segurança

Documentação	
Objetivo	Operação segura do sistema
Como?	Manual com orientações de configuração, manutenção e administração do sistema

Suporte ao Ciclo de Vida	
Objetivo	Atingir requisitos funcionais de segurança
Como?	Utilização de modelos como CMMI, RUP

Testes de Segurança	
Objetivo	Garantir que sistema está atendendo aos requisitos de segurança
Como?	Testes de unidade, integração, sistema, instalação e aceitação

Avaliação de Vulnerabilidades	
Objetivo	Analisar ameaças que podem ser exploradas
Como?	Procurar por possibilidades de falhas, quer nos mecanismos de segurança, quer na documentação, quer no uso do sistema

Muitas ferramentas CASE oferecem suporte automatizado ao processo de teste.

Há também boas ferramentas para auxiliar na documentação de softwares

Escolha um dos dois itens acima e faça uma pesquisa apresentando as principais ferramentas de mercado. Escolha uma delas e procure utilizar de alguma forma. Ao final apresente um relatório sobre a ferramenta que você utilizou, evidenciando pontos positivos e negativos

2.5 Segurança no Ciclo de Vida de Desenvolvimento da Aplicação

Lyra (2008) aconselha a escolha de uma metodologia de desenvolvimento. No entanto, além disso, ele cita as boas práticas de programação:

- criar funções intrinsecamente seguras;
- usar funções intrinsecamente seguras;
- testar o retorno de funções;
- documentar funções corretamente;
- tratar as entradas de dados;
- ter uma política de versão consistente;
- usar componentes e bibliotecas confiáveis;
- evitar informações sensíveis em arquivos temporários;
- não armazenar senhas e chaves criptográficas no código;
- operar com o privilégio necessário, e
- tratar todas as entradas do sistema como não seguras.

Temos um Fórum chamado "Boas Práticas de Programação". Antes de postar sua participação você deverá escolher duas boas práticas e pesquisar o que de fato elas significam e comentar se você tem o costume de utilizá-la.

Para finalizar nossa unidade, disponibilizei em nossa Midiateca, uma monografia com o tema: "Um Guia para Implantação de Segurança Básica em Sistemas". Vocês deverão ler da página 12 a 48, em que são apresentados os principais problemas e aspectos de segurança. Após a leitura deverá ser construída uma resenha com metodologia científica (vide manual de normatização do Unis páginas 79 e 80 disponível em www.unis.edu.br, portal do aluno).

CONCLUSÃO

Nesta unidade vimos a importância de construir aplicações com segurança, ou mesmo verificar em aplicações já implantadas. Importante ressaltar que nada disso pode ser feito do nada, existem ferramentas, metodologias, práticas e normas para nos auxiliar neste aspecto. Dessa forma, é responsabilidade nossa cada vez mais cuidar disso. Percebe que não basta simplesmente ser um bom programador, ter uma boa lógica se não há cuidado nenhum com a segurança. Vimos que é importante começar a tratar do assunto ainda nas primeiras fases de levantamento de requisitos.

APONTAMENTOS SOBRE A PRÓXIMA UNIDADE

Em nossa próxima unidade veremos os conceitos de auditoria, fudamentos, metodologias, ferramentas e práticas. Veremos que ela é importante em várias fases como: aquisição, desenvolvimento, documentação e manutenção de sistemas

3 AUDITORIA EM SISTEMAS DE INFORMAÇÃO

META

Apresentar conceitos de auditoria, destacando as metodologias existentes, ferramentas, técnicas, melhores práticas e outros aspectos ligados ao tema.

OBJETIVOS DA UNIDADE

Esperamos que, após o estudo do conteúdo desta unidade, você seja capaz de:

- Conceituar Auditoria de Sistemas
- Entender o objetivo e importância das Auditorias
- Aprender sobre as melhores práticas e ferramentas

3.1 Fundamentos em Auditoria

O objetivo de realizar uma Auditoria de um Sistema de Informação é o de conseguir adequar, revisar, avaliar e recomendar alterações positivas nos processos internos, bem como avaliar a utilização dos recursos humanos, materiais e tecnológicos envolvidos (LYRA, 2008).

Gil (2000) destaca que a Auditoria de Sistemas é importante tendo em vista os recentes altos investimentos das organizações em sistemas, a necessidade de segurança dos computadores e seus sistemas e a garantia do alcance da qualidade dos sistemas computadorizados.

Podemos resumir que a Auditoria de Sistemas de Informação possui alguns objetivos principais, quais são:

- Integridade → ter confiança nas transações processadas pelo sistema. Isso permite que os usuários tomem decisões sem receio, sem desconfiança. Muitas vezes dentro de empresas ao extrair um relatório ninguém se compromete em assiná-lo ou em tomar uma decisão tendo somente ele por base de informações.
- Confidencialidade → informações reveladas somente às pessoas que de fato precisam delas. É muito comum em empresas, um funcionário assumir outra função ou não ter mais uma função anterior e continuar com acesso às informações do cargo anterior.
- Privacidade → enxergar apenas as informações que lhe são cabíveis para execução de suas atividades.
- Acuidade → validar as transações realizadas. Evitar que dados incompatíveis populem o sistema, gerando transações indevidas ou inválidas.
- Disponibilidade → sistema disponível para realizar as tarefas. Queda ou problemas no sistema podem gerar despesas ou prejuízos incontáveis. Lembram da queda de serviço do Speed?

- Auditabilidade → documentar *logs* operacionais. Embora isso possa trazer um pouco de lentidão ao sistema, maiores gastos em infraestrutura computacional, é extremamente vantajoso.
- Versatilidade → sistema deve ser amigável, adaptável e ter condições de uso para exportar e importar dados. Nos dias atuais é extremamente importante não ter ações de digitação nos sistemas, quanto mais se conseguir automatizar as tarefas, menos erros ocorrerão.
- Manutenibilidade → os procedimentos devem conter controles. Estes devem incluir testes, conversões e documentação.

Em nossa Midiateca temos um Glossário com termos utilizados em Auditoria. A Leitura ajudará na compreensão mais fácil dos termos. Leitura Obrigatória.

3.2 Tipos de Auditoria

Há várias modalidades de Auditoria, porém tendo em vista o assunto que discutimos e de acordo com Lyra (2008), destacamos:

- Auditoria Durante o Desenvolvimento de Sistemas: auditar todo o processo de construção do sistema, desde a fase de requisitos até a implantação, passando ainda pela metodologia de desenvolvimento.
- Auditoria de Sistemas em Produção: auditar os procedimentos e resultados dos sistemas já implantados.
- Auditoria no Ambiente Tecnológico: auditar o ambiente de informática, no que tange a estrutura organizacional, contratos, normas técnicas, custos, planos, etc.
- Auditoria em Eventos Específicos: auditar eventos novos ou eventos não detectados por auditorias anteriores.

3.3 Metodologia de Auditoria de Sistemas de Informação

Quando falamos em metodologia é necessários uma palavra de cautela. Nem sempre podemos seguir à risca, com os olhos fechados uma metodologia do início ao fim. Cada empresas, cada época, cada situação tem as suas particularidades. No entanto, estabelecer um norte de atuação é sempre útil, mas não se deve deixar de lado o chamado "jogo de cintura", pois assim o trabalho torna-se peculiar e mais interessante. A metologia proposta por Lyra (2008) está descrita abaixo e dividido em fases, conforme poderá ver:

3.3.1 Planejamento e Controle do Projeto de Auditoria de Sistemas de Informação

Para isso é interessante levar em consideração a abrangência das ações, o enfoque desejado, além de um levantamento do quantitativo de sistemas que serão auditados. Este será então o planejamento inicial das ações e dos recursos necessários para executar a auditoria.

Mas aí você pergunta, como vou fazer isso de forma correta? Aí vão algumas dicas ou recomendações:

- forme uma Equipe de Trabalho;
- divida essa Equipe em dois grupos: Coordenação e Execução;
- coordenação: composto pelo gerente de auditoria, gerente da área usuária responsável pelo sistema de informação, gerente da área de TI e gerente ou responsável técnico do sistema;
- execução: composto por auditores e técnicos da área de informática e da área usuária;
- o grupo Coordenação deverá: definir procedimentos a serem

utilizados durante o trabalho de auditoria, escolher alternativas para acompanhar trabalhos, acompanhar e controlar resultados obtidos;

- o grupo Execução realizará a Auditoria;
- utilizar ferramentas e métodos consagrados como PMBoK para auxiliar no planejamento das atividades.

3.3.2 Levantamento do Sistema de Informação a ser Auditado

Após essa primeira fase é necessário levantar as informações relevantes sobre o sistema. Este deve ser o mais abrangente possível, para que assim exista um entendimento das características do sistema. Neste ponto você deve aplicar o que aprendeu em Análise e Projetos de Sistemas. Isso mesmo! É hora de entrevistas, analisar documentações existentes, criar diagramas, gráficos, etc. Lembra de algumas ferramentas para auxiliar nisso? Se você lembrou de DFD, MER, dicionário de dados, casos de uso, diagramas de classe, sequenciais você acertou. É hora de utilizar esses conceitos e ferramentas. Ajudarão a explicar o comportamento do sistema e como ele figura nos processos da empresa.

Não esqueça de que nessa fase o mais importante é conseguir determinar o escopo. Com isso você poderá determinar a abrangência da auditoria e o seu possível alcance.

3.3.3 Identificação e Inventário dos Pontos de Controle

O objetivo desta etapa é você conseguir determinar os pontos de controle que precisam ser validados. Isso é o inventário de pontos de controle. Eles podem ser encontrados em documentos de entrada do sistema, relatórios de saída, telas, arquivos, pontos de integração, bancos de dados. Cada ponto deve estar relacionado e seus objetivos também devem ser conhecidos. O resultado deste levantamento deve ser enviado ao Grupo Coordenação para uma validação de pertinência.

3.3.4 Priorização e Seleção dos Pontos de Controle do Sistema Auditado

Essa etapa seleciona e prioriza os pontos de controle inventariados anteriormente. Mas como selecionar esses pontos? Essa seleção deve ser baseada no Grau de Risco existente no ponto, na existência de ameaças e na disponibilidade de recursos.

Quando se fala em Grau de Risco isso consiste em verificar os prejuízos que poderão ser acarretados pelo sistema a curto, médio e longo prazo. Prevê as ameças prováveis de um ponto. Sobre a existência de ameaças, consiste em classificar os pontos e dar atenção primeiro aos que possuem forte ameaça. Finalmente, sobre Disponibilidade de Recursos inclui dar atenção aos pontos que podem ser atendidos dentro do que foi levantado como recursos para a auditoria.

Levando em conta essas três características pode-se conseguir elencar os pontos de controle que deverão ser revisados e auditados com maior prioridade.

3.3.5 Avaliação dos Pontos de Controle

Somente nesta fase começa a Auditoria realmente. É aqui que os testes dos pontos de controle selecionados serão feitos. As técnicas aplicadas deverão procurar falhas e pontos que podem ser melhorados. Para isso é interessante aplicar ferramentas e técnicas para um melhor resultado. Apresentaremos algumas destas um pouco mais à frente.

3.3.6 Conclusão da Auditoria

Ao término da execução dos testes, você deverá elaborar um relatório contendo o resultado encontrado. Detalhe: o resultado deve ser o encontrado, independente se for ruim ou bom.

O que você acha que deve conter um relatório assim?

Ele deve conter o diagnóstico da situação atual dos pontos de controle, e se existir, as falhas ou fraquezas dos controles internos.

Se encontrar um ponto de controle que possui fraqueza ou falha este se transforma em Ponto de Auditoria. Você poderá então apontar melhorias ou soluções para este ponto.

Estes Pontos de Auditoria deverão periodicamente sofrer avaliações ou revisões para verificar se a falha ou fraqueza foi sanada. Esta análise pode ser feita por analistas ou usuários responsáveis.

3.3.7 Acompanhamento da Auditoria

O Acompanhamento da Auditoria ou *follow-up*, deve ser feito até que todas as recomendações tenham sido atendidas em um nível satisfatório. Este deve verificar se os Pontos de Auditoria estão sendo revistos e avaliados e o comportamento referente aos mesmos.

Temos um Fórum chamado “Auditoria”. Poste qualquer experiência que tenha tido com Auditoria. Não se esqueça de mencionar técnicas utilizadas, melhorias apontadas, ferramentas, etc.

Se você não passou por uma experiência assim, pesquise sobre o tema e poste algo relacionado.

3.4 Ferramentas de Auditoria de Sistemas de Informação

Imagine extrair, sortear, selecionar dados e transações sem o apoio de ferramentas computacionais. Seria muito exaustivo. Há uma grande variedade de ferramentas para auxiliar neste aspecto.

Entre essas ferramentas há *softwares* de uso em ambiente *batch* que podem processar, simular, analisar amostras, gerar dados, apontar duplicidade, entre outros. Entre as vantagens da utilização de uma ferramenta podemos destacar o fato de um aplicativo conseguir processar vários arquivos ao mesmo tempo, processar vários arquivos de diferentes formatos, integrar sistemicamente com vários tipos de estruturas diferentes, reduzir a dependência do auditor em relação ao pessoa da TI da empresa. Este tipo de sistema é chamado de ferramentas generalistas. Abaixo temos exemplos:

- *Audit Command Language* (ACL) → extração e análise de dados
- *Interactive Data Extraction & Analisys* (IDEA) → extração e análise de dados
- Audimation → extração e análise de dados
- Galileo → gestão de auditoria, incluindo gestão de risco, documentação e emissão de relatórios;
- Pentana → permite a elaboração de um planejamento estratégico de auditoria, com planejamento e monitoramento de recursos, controle de horas, registro de checagens e desenho e gerenciamento de plano de ação.

Surge uma dúvida: a utilização de ferramentas como as que vimos apresentam somente vantagens? Não. Há algumas desvantagens como a não utlização das mesmas em ambiente *online* e quando se torna necessário a execução de cálculos mais complexos que não podem ser resolvidos por ferramentas generalistas.

Em vista disso, existem as chamadas ferramentas especializadas. Trata-se de sistemas desenvolvidos para execução de tarefas em cirscuntância definida. Estas podem ser desenvolvidas pelo auditor, pelo especialista da empresa ou por outros. A vantagem desse tipo de ferramenta está no fato de conseguir atender necessidades específicas. As desvantagens estão em custo e em problemas de atualização de sistema.

Há ainda os programas utilitários que realizam tarefas comuns como ordenar um arquivo, concatenar textos, sumarizar, etc. Estes são verdadeiros

"quebra-galhos" para algumas ações que poderá economizar principalmente tempo e esforço.

Este espaço abaixo é para você complementar este guia. Pesquise, converse com colegas, entreviste auditores e liste outras ferramentas de auditoria utilizadas hoje em dia. Procure alistar vantagens e desvantagens das mesmas.

3.5 Técnicas de Auditoria de Sistemas de Informação

Lyra (2008) afirma que as varidas metodologias de auditoria podem ser chamadas de técnicas. Em vista disso, selecionamos algumas delas que poderão orientar sobretudo se for ter uma primeira experiência neste âmbito. Lyra (2008) afirma que as varidas metodologias de auditoria podem ser chamadas de técnicas. Em vista disso, selecionamos algumas delas que poderão orientar sobretudo se for ter uma primeira experiência neste âmbito.

- DADOS DE TESTE → envolvem o uso de um conjunto de dados especialmente projetados e preparados com o objetivo de testar as funcionalidades de entrada de dados no sistema. É interessante realizar uma entrada com os mesmos e verificar os resultados obtidos. Será que este resultado era o esperado ou existe alguma discrepância? Quanto mais combinações de transações puderem ser feitas no arquivo de carga, maior será a cobertura do teste.
- FACILIDADE DE TESTE INTEGRADO → melhor aplicada em ambientes *online e real time*. Os dados de teste são introduzidos nos ambientes reais de processamento, formando assim uma linha de produção. Envolve aplicar situações inusitadas e novas ao sistema para avaliar seu comportamento e consistência. Pode-se confrontar dados reais com os dados fictícios lançados.
- SIMULAÇÃO PARALELA → envolve utilizar um programa desenvolvido de forma especial que simule as funcionalidades do

programa em produção. São realizadas transações em ambos e compara-se os resultados. Este é interessante principalmente para rotinas que apresentam inconstância em seus resultados.

- LÓGICA DE AUDITORIA EMBUTIDA NOS SISTEMAS → inclusão da lógica de auditoria nos sistemas em fase de desenvolvimento. Criar relatórios de auditoria para acompanhamento dos procedimentos.
- RASTREAMENTO E MAPEAMENTO → elaborar e implementar uma trilha de auditoria para acompanhar os principais pontos de lógica do processamento das transações críticas, registrando seu comportamento e resultados para uma análise a ser feita futuramente. Essas trilhas, na verdade, são rotinas de controle para permitir o alcance da informação tanto após o processamento como antes.
- ANÁLISE DA LÓGICA DE PROGRAMAÇÃO → certificação de que as instruções construídas para execução pelo computador estão de acordo com as regras de negócio da empresa e de acordo com o que foi passado para a Auditoria.

3.6 Melhores Práticas de Auditoria de Sistemas de Informação

Ainda não há uma convenção de padrão para Auditoria de Sistemas de Informação. Lyra (2008) informa que várias associações apresentam regras do exercício da profissão que servem para nortear a atuação de seus membros.

3.6.1 Comitê de Padrões da Associação de Controle e Auditoria de Tecnologia da Informação

Trata-se de uma associação norte-americana que dá recomendações para quem trabalha com auditoria de tecnologia da informação. (LYRA, 2008). Entre as recomendações temos:

- Responsabilidade, Autoridade e Prestação de Contas: estas devem estar documentadas em uma carta proposta ou de aderência ao escopo.
- Independência Profissional: auditor deve ser independente em atitude e aparência. Ele deve ser independente inclusive da área auditada para que assim seu trabalho tenha uma conclusão objetiva.
- Ética Profissional e Padrões: o zelo profissional e a observância dos padrões profissionais de auditoria devem ser exercidos em todos os aspectos do trabalho do auditor.
- Competência: deve possuir habilidades e conhecimento necessários para a execução do seu trabalho. Deve manter a competência técnica por estar sempre se aprimorando.
- Planejamento: deve ter um bom planejamento que permita atingir seus objetivos. Deve supervisionar sua equipe e ter capacidade de analisar e interpretar informações permitindo uma conclusão lógica.
- Emissão de Relatório: na conclusão de seu trabalho deve ser elaborado um relatório contendo escopo, objetivos, período de abrangência, natureza e extensão do trabalho. Deve ainda elaborar observações, conclusões, recomendações e possíveis soluções para as situações encontradas durante a auditoria.
- Atividades de *Follow-up:* deve requisitar e avaliar as informações apropriadas sobre pontos, conclusões e recomendações anteriores. Assim tem condições de avaliar se foi conseguido solucionar os pontos em tempo satisfatório.

3.6.2 Associação de Auditores de Sistemas e Controles (ISACA)

Ela criou um código de ética profissional com objetivo de guiar as atividades de seus membros. Entre as ações que eles devem fazer, estão:

- apoiar a implantação e encorajar o cumprimento com os padrões sugeridos dos procedimentos e controles dos sistemas de informações;

- exercer suas funções com objetividade, diligência e zelo profissional, de acordo com os padrões profissionais e as melhores práticas;
- servir aos interesses dos *stakeholders* de forma legal e honesta, atentando para a manutenção de alto padrão de conduta e caráter profissional, e não encorajar atos de descrédito à profissão;
- manter privacidade e confidencialidade das informações obtidas no decurso de suas funções, exceto quando exigido legalmente. Tais informações não devem ser utilizadas em vantagem própria ou entregue a pessoas dasautorizadas;
- manter competência nas respectivas especialidades e assegurar que nos seus exercícios somente atua nas atividades em que tenha razoável habilidade para competir profissionalmente.

Imagine que você foi chamado para participar de uma Auditoria de Sistemas de Informação. Você então deverá tentar montar esse processo. Para isso você deverá montar inicialmente quatro fases, quais são: Planejamento da Auditoria, Definição da Equipe, Documentação do Trabalho e Produtos Gerados pela Auditoria. Monte esse processo com detalhes em cada fase.

CONCLUSÃO

Nesta unidade vimos a importância que as Auditorias tem dentro das organizações. Embora possam existir dificuldades para a sua realização, tais como defasagem tecnológica, falta de bons profissionais, falta de cultura da empresa e tecnologia variada e abrangente ela ganha força a cada dia. Isso porque, conforme vimos, os resultados são tangíveis, expressos em relatórios e de fácil verificação de seus resultados. Vimos ainda a variedade de ferramentas existentes e também um passo a passo para uma primeira auditoria. Tente realizar isso internamente, prove o que a Auditoria pode fazer por você e seu departamento. Os resultados podem surpreender!

APONTAMENTOS SOBRE A PRÓXIMA UNIDADE

Em nossa próxima unidade veremos política de segurança, apresentando exemplos de ciclo de vida de desenvolvimento seguro e Planos de Segurança.

4 POLÍTICA E SEGURANÇA

META

Apresentar importância do estabelecimento de uma política de segurança, destacando exemplos de ciclo de vida de desenvolvimento seguro e Planos de Segurança

OBJETIVOS DA UNIDADE

Esperamos que, após o estudo do conteúdo desta unidade, você seja capaz de:

- elaborar uma política de segurança;
- entender o objetivo e importância de um plano de segurança;
- conhecer um ciclo de vida de desenvolvimento seguro.

4.1 Os Planos de Segurança

Uma Política de Segurança não pode ser criada da noite para o dia. Trata-se de um processo cultural. Para tal é necessário que todos os que compõem a empresa, mais os parceiros ou terceiros estejam interessados em tal. Wanderley e Moura (2000), abordam a importância de utilizar boas tecnologias para isso.

A necessidade e o medo são tantos que muitas vezes pensamos em construir algo como demonstra a figura 5. Em muitas empresas, há resistência por parte da gerência no que tange a investir em programas ou políticas de segurança. Isso se deve muitas vezes ao fato de economizar recursos, manter satisfação dos funcionários em não ser vigiados ou dar "liberdade" na utilização dos equipamentos. Porém, a conta pode sair muito cara. É muito melhor iniciar um investimento de conscientização, criação de uma política a ser estabelecida, criar normas que perder dados ou não ter segurança nas informações transacionadas internamente.

Figura 5: Segurança.
(Fonte:www.gta.ufrj.br/.../images/antispam_2.png)

O uso de Certificados Digitais, bem como criptografia não é apenas uma opção para quem vai construir um Plano de Segurança. Antes, trata-se de uma necessidade. A figura abaixo nos mostra uma visão geral de uma política de segurança, de acordo com Wanderley e Moura (2000).

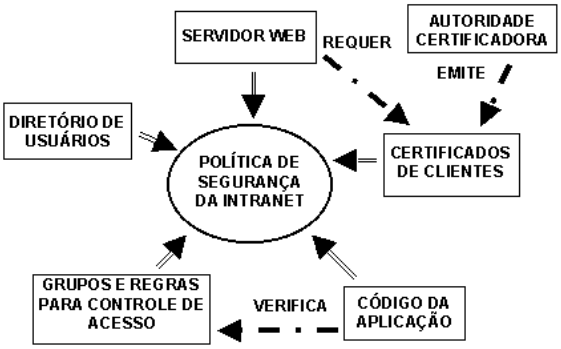

Figura 6: Política de Segurança (Fonte: Wanderley e Moura, 2000)

A figura mostra o que é necessário em uma política de segurança para estabelecer ações para autenticação e autorização:

- Servidor Web → configurar para requerer certificados dos clientes;
- Certificados de clientes → obtidos pelos usuários e instalados em seus navegadores Web;
- Diretório de usuário → projetado para armazenar chaves públicas e informações sobre usuários;
- Definições de grupos e regras → dar ou negar acesso aos recursos;
- Código fonte da aplicação → checando o acesso e regras de controle.

4.1.1 Plano Diretor de Segurança

O primeiro passo para quem quer dar segurança à sua informação é criar um plano diretor de Segurança. Ele não deve ser algo muito rígido, antes, deve ser flexível e pronto para se ajustar às necessidades de segurança da organização.

Este plano deve objetivar o fornecimento de orientações sobre como

será o comportamento da organização em relação à segurança. Assim, não é possível estabelecer um plano e dizer que ele serve para todo e qualquer ambiente corporativo. Há determinadas ações que para uma empresa seria um risco elevado de segurança e para outras um risco moderado. Assim cada uma pode estabelecer como agir de acordo com sua realidade. Ele também deve, de acordo com Lyra (2008),

montar um mapa de relacionamento e dependência entre processos de negócio, aplicações e infraestrutura física, tecnológica e humana.

Embora não exista uma "receita de bolo" para guiar a construção deste plano, Sêmola (2003) propõe uma metodologia para elaborar este plano.

Em nossa Midiateca temos um arquivo *pds.ppt* que contém as seis etapas distintas proposta por Sêmola (2003) para a criação de um Plano Diretor de Segurança. Leia, Confira!

Nesta proposta identifica-se claramente que as ações de segurança devem ter foco no negócio da empresa e nas informações que sustentam esse negócio. Assim é primordial conseguir levantar quais são os processos mais vitais. Quem deve participar desse levantamento obrigatoriamente é a alta gerência, pois ela conhece quais processos são essenciais para sua tomada de decisão.

Após esse mapeamento deve-se estabelecer a relevância de cada um realizando uma classificação dos mesmos. Isso também deve ser feito junto com gestores que conhecem a organização como um todo. Para isso pode-se criar uma escala de 1 a 5 para realizar a pontuação (1 menos relevante e 5 mais relevante). Depois de descobrir quais processos são mais importantes é hora de relacioná-los com incidentes de segurança. Para este estudo de impacto pode ser feita uma análise CIDAL (conceitos de confidencialidade, integridade, disponibilidade, autenticidade, legalidade). Nesse ponto não se leva em conta o todo e sim uma visão mais pontual do processo. Deve-se

então analisar o processo e verificar o que poderia acontecer se ocorresse uma quebra em um dos três aspectos de segurança (CID) ou nos aspectos de segurança (AL). O próximo passo seria estabelecer uma prioridade para cada processo sob ameaça. Esta prioridade pode ser montada através de uma matriz GUT (Gravidade, Urgência, Tendência). Vide arquivo pds.ppt na MIDIATECA. Depois de todas estas atividades é importante identificar os ativos (infraestrutura, tecnologia, aplicações, informações e pessoas). Estes ativos são os que fazem os processos de negócio existir e acontecer. Eles possuem falhar e fraquezas em relação à segurança. E somente as pessoas que trabalham nesse ambiente saberão exatamente os pontos que devem ser melhorados. Agora, portanto, é hora de esquecer alta gestão e trabalhar com o pessoal técnico. Por último, é a montagem do plano. Que soluções são mais interessantes? Que projetos poderão já ser implantados? Que ações ocorrerão em ambientes e perímetros distintos e isolados? Portanto, é nessa fase que são indicadas as atividades e/ou projetos juntamente com um cronograma.

4.1.2 Plano de Continuidade de Negócios

Lyra (2008) aborda este tipo de plano como tendo por objetivo assegurar a continuidade das atividades exercidas por cada processo dentro da organização. Entre seus objetivos, destaca-se:

- garantir segurança dos empregados e visitantes;
- minimizar danos imediatos e perdas numa situação de emergência;
- assegurar a restauração das atividades, instalações e equipamentos o mais rápido possível;
- assegurar a rápida ativação dos processos de negócio críticos;
- fornecer conscientização e treinamento para as pessoas-chave encarregadas desta atividade.

Lyra (2008) cita o Disaster Recovery Institute (DRI International) que

elaborou uma proposta de um padrão de desenvolvimento de um Plano de Continuidade de Negócios. As etapas devem ser feitas na ordem em que aparecem, sendo sucessivas:

1 - Início e Administração do Projeto → definir o escopo/necessidade para o PCN, incluindo questões sobre patrocínio, organização e gerenciamento de projeto

2 - Avaliação e Controle dos Riscos → definir os possíveis e prováveis cenários que fazem parte da organização e que podem afetar o ambiente. Determinar os dados que podem vir a existir e que medidas podem ser tomadas para reduzir o problema. Uma boa alternativa é uma análise ROI (*Return of Investment*) para justificar o investimento em segurança ou no plano.

3 - Análise de Impacto nos Negócios → identificar e avaliar os impactos de uma possível interrupção e dos cenários pessimistas. Definir a criticidade dos processos, prioridades de recuperação e interdependência.

4 - Desenvolvimento de Estratégias de Continuidade de Negócio → definir as estratégias operacionais para a recuperação dos processos e dos componentes de negócios dentro dos prazos de recuperação esperados. Pode-se dividir os procedimentos em Plano de Recuperação de Desastres que seria um plano para atividades relacionadas à recuperação ou substituição de componentes e Plano de Contingência que é a manutenção dos processos de negócios.

5 - Respostas e Operações de Emergência → desenvolver e implementar procedimentos de resposta e estabilização de situações por meio de um incidente ou evento. Pode-se criar um Centro

Operacional de Emergência (COE) que servirá como central durante uma crise.

6 - Desenvolvimento e Implantação do PCN → integrar todos os componentes elaborados e planejados.

7 - Implantação dos Programas de Treinamento → desenvolver programa para incrementar a cultura corporativa, incentivar as habilidades necessárias,

executar Plano. O Treinamento das Equipes pode acontecer de várias formas, mas um primeiro passo começa por distribuir o plano para conhecimento de todos.

8 - Manter e Exercitar os PCN's → elaborar um pré-plano para coordenar exercícios do PCN, buscando avaliar os resultados obtidos. Deve-se analisar e atualizar constantemente o PCN para que o mesmo seja válido. Procedimentos devem ser inclusos. Deve ser testado regularmente para garantir eficácia.

9 - Gerenciamento de Crise → desenvolver, coordenar, avaliar e exercitar o manuseio de mídias e documentos. Assegurar o fornecimento de informações para investidores.

10 - Parcerias com Entidades Públicas → estabelecer procedimentos e políticas de coordenação de respostas, atividades de continuidade e restauração de negócios, buscando ajuda de órgãos públicos e cumprindo normas e leis.

11 - Parcerias com Entidades Privadas → estabelecer diretrizes e coordenação de resposta, atividades de continuidade e restauração de negócios, com ajuda de organizações privadas.

Ufa! O assunto é bem extenso e dá ampla margem para discussão e conversa. Mas, perceberam que na etapa quatro falamos sobre Plano de Contingência. Este tipo de plano é um dos mais falados hoje em dia. Por isso é interessante explorar um pouco mais o tema. Quais seriam algumas das estratégias de contingência? Já precisou estabelecer alguma?

Lyra (2008) destaca que uma das estratégias de contingência é o *HOT-SITE*. Trata-se de uma iniciativa pronta para entrar em operação assim que uma situação de risco acontecer. O seu tempo de operacionalização está diretamente ligada ao tempo de tolerância a falhas do objeto. Outra estratégia é o *WARM-SITE*, que se aplica a objetos com maior tolerância à falha ou paralisação, podendo ficar mais tempo indisponível. A *BUREAU* DE SERVIÇOS possibilita a transferência da atividade atingida para um ambiente terceirizado, fora da empresa, ou seja, não pertencente a ela. O ACORDO DE RECIPROCIDADE propõe a aproximação e um acordo

formal com empresas que mantém características físicas, tecnológicas ou humanas semelhantes. Dessa forma, concordam em estabelecer um conjunto de situações de contingência em que compartilhariam recursos. *COLD-SITE* propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, mas sem processamento de dados. Assim, torna-se interessante quando há tolerância para as falhas. A AUTO-SUFICIÊNCIA é muitas vezes, a melhor ou a única estratégia possível para determinada atividade. Isso acontece quando nenhuma outra estratégia é aplicável, quando os impactos possíveis não são altos ou inviáveis em vários aspectos.

O que você aprendeu ao ler sobre as estratégias?

Um aspecto muito importante é sempre se lembrar de que a escolha de qualquer estratégia depende diretamente do nível de tolerância que a empresa consegue suportar e o nível de risco que a alta gestão está disposta a correr.

Dê exemplos de situações em que poderia aplicar as estratégias citadas acima: HOT-SITE, WARM-SITE, REALOCAÇÃO DE OPERAÇÃO BUREAU DE SERVIÇOS, ACORDO DE RECIPROCIDADE E COLD-SITE

4.1.3 Plano de Administração de Crise

De acordo com Lyra (2008), trata-se de um documento que tem a finalidade de definir como funcionará as equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência de um incidente. Define ainda, procedimentos a serem executados quando tudo está normal. Uma ação que também é tratada por esse documento é como comunicar o incidente, sua solução e seus possíveis transtornos à imprensa.

É muito comum, além desse tipo de ação, criar um Grupo de Respostas a Incidentes de Segurança.

No site do CERT existe um documento traduzido com permissão especial do Software Engineering Institute, que citaremos a partir de agora.

De acordo com o CERT (2010), manter a segurança da informação se torna mais difícil à medida que são lançados novos produtos para a Internet e novas ferramentas de ataque são desenvolvidas.

Assim, você deve concordar que é impossível criar uma solução única, como um *be-a-bá* de segurança. Mas o que fazer?

O CERT (2010) fala sobre a necessidade de ter uma estratégia de segurança composta de várias camadas. Uma dessas camadas trata-se do Grupo de Resposta a Incidentes de Segurança em Computadores, conhecido como CSIRT (do inglês "Computer Security Incident Response Team").

Os motivos para essa ação estão em:

- aumento na quantidade de incidentes de segurança sendo reportados (vide site do *cert.br*)
- aumento na quantidade e na variedade de organizações afetadas por incidentes de segurança em computadores
- uma maior consciência da necessidade de políticas e práticas de segurança
- novas leis e regulamentos que afetam a maneira como as organizações precisam proteger as suas informações
- a percepção de que administradores de redes e sistemas não podem proteger sozinhos os sistemas e as informações da organização

Assim, o objetivo de criar um CSIRTs é o de buscar respostas para a construção de um mecanismo de auxílio para os incidentes. Porém, isso não é tarefa fácil, o CERT (2010) lista as dificuldades e questionamentos para tal:

- Quais são os requisitos básicos para se estabelecer um CSIRT?
- Que tipo de CSIRT será necessário?

- Que tipos de serviços devem ser oferecidos?
- Qual deve ser o tamanho de um CSIRT?
- Onde o CSIRT deve estar localizado na organização?
- Qual o custo para implementar e manter um CSIRT?
- Quais são os passos iniciais que devem ser seguidos para criar um CSIRT?

Se você está esperando uma resposta objetiva para cada pergunta acima, sinto em dizer que não existe. Cada CSIRT é singular como a sua organização. Assim, se hoje você estabelece uma estrutura dessas em uma empresa e amanhã está em outra empresa, o CSIRT da segunda não será igual ao da primeira. Após implementar o CSIRT você terá as respostas para os questionamentos acima.

Embora não seja uma "receita de bolo", o artigo supracitado considera alguns passos para a criação de um CSIRT:

- Obter o Apoio e a Aprovação da Administração Superior → sem a aprovação e o apoio da alta administração fica muito difícil a criação de um CSIRT. Quando se fala em apoio isso significa recursos materiais e financeiros, e de tempo para trabalhar (tanto para a pessoa como para a equipe). Outro aspecto importante é ouvir o que a administração espera do CSIRT. Também, eles podem confirmar o compromisso de sustentar as operações e a autoridade do CSIRT em longo prazo.
- Determinar o Plano de Desenvolvimento Estratégico do CSIRT → esta ação deve procurar gerenciar o desenvolvimento do CSIRT. Para que isso seja feito de forma correta são recomendadas algumas questões: Quais questões administrativas e de gerência do projeto devem ser consideradas? Existem prazos específicos a cumprir? Estes prazos são realistas? Se não, eles podem ser alterados?Existe um grupo de projeto? Qual a origem dos membros do grupo? Um bom

procedimento para fazer isso á aplicar práticas em gerência de projetos, teoria do comportamento organizacional e teoria da comunicação. Essas práticas poderão fornecer um maior embasamento às ações que se queira realizar, bem como garantir sucesso na implantação. Outra dica é criar um ambiente online em que todos os componentes do grupo podem se comunicar e acessar documentos importantes e relevantes ao projeto.

- Coletar as Informações Relevantes → Este passo é muito importante, pois permite que se saiba exatamente quais são as necessidades da organização. É vital coletar informações de departamentos estratégicos ao CSIRT e saber ouvir aqueles que podem contribuir. Para isso é importante aplicar técnicas de coleta de informações. Isso vai ajudar a determinar que estratégias deverão ser aplicadas primeiro, que alvos são mais necessários ou que precisam de mais atenção.

Dê exemplos de Técnicas de Coleta de Informações e tente levantar as vantagens e desvantagens de cada técnica.

Quase todos os dias as organizações lidam com incidentes de segurança.

Tente montar uma situação hipotética ou que seja comum e apresente como você montaria uma resposta a esse incidente. Para isso tente utilizar o espaço abaixo.

Um exemplo de resposta à atividade proposta acima é dada pelo CERT(2010):

- Imagine que uma organização foi vítima de um vírus ou “worm”, incidentes muito comuns. Serão necessários procedimentos de busca, eliminação e recuperação de vírus com ferramentas antivírus. Talvez será necessário treinamentos e produzir documentação para ajudar a desenvolver programas de conscientização dos usuários.

- Conceber a Visão do seu CSIRT → o passo anterior ajuda a definir uma visão do CSIRT e seus objetivos e funções. Assim, é vital alcançar um entendimento da definição e das expectativas para o CSIRT. Não se pode esquecer que o foco principal é prevenir e responder a incidentes. Assim o CERT (2010) cita que deve existir as seguintes preocupações ao criar a visão: Identificar a comunidade a ser atendida – Definir a missão e os objetivos do seu CSIRT – Selecionar os serviços a serem prestados à comunidade (ou a outros) – Determinar o modelo organizacional – Identificar os recursos necessários – Determinar o modelo de financiamento do seu CSIRT.
- Comunicar a Visão do CSIRT → Comunicar a visão criada no passo anterior é fundamental. E isso deve ser feito a todos, da alta gerência a toda a comunidade. Outro aspecto importante é lembrar que ajustes são permitidos e devem ser feitos.
- Iniciar a Implementação do CSIRT → Para implementar é importante treinar o pessoal inicial do CSIRT, comprar os equipamentos e montar a infraestrutura de rede necessária para dar suporte ao grupo, desenvolver um conjunto inicial de políticas e procedimentos para o CSIRT, definir as especificações para o sistema de acompanhamento de incidentes e implementar e, por fim, desenvolver recomendações e formulários para que todos possam reportar incidentes. Este aspecto é muito importante, pois um incidente reportado de forma errada pode gerar esforços desnecessários.

4.1.4 Plano de Continuidade Operacional

Objetivo de definir os procedimentos para contingência dos ativos que suportam cada processo de negócio, com objetivo de reduzir o tempo de indisponibilidade e os possíveis impactos. Além disso, deve orientar as ações para que o serviço da empresa não fique indisponível por muito tempo. Um clássico exemplo disso seria uma queda da conexão à Internet. Que ações deveriam ser feitas? Este plano traçaria exatamente que ações deveriam ser feitas. (LYRA, 2008)

4.2 Ciclo de Vida de Desenvolvimento Seguro

Lyra (2008) apresenta um processo chamado SDL, sigla do inglês, que significa *Trustworthy Computing Software Development Lifecycle.*

O processo citado acima é utilizado pela Microsoft e está disponível no link abaixo:
http://msdn.microsoft.com/pt-br/library/ms995349.aspx

Acesse o link citado e elabore um resumo detalhando como funciona o processo utilizado pela Microsoft.

4.3 Forense Computacional

Cada vez mais os crimes tornam-se mais invasivos e fortuitos. Isso tem obrigado as autoridades a estabelecer formas cada vez mais inteligentes de combate. Guimarães et. al (2001) destaca que a eliminação de fronteiras realizada pela Internet gerou um grande problema para as instituições de combate ao crime. Ele aborda que os crimes eletrônicos passaram a ter vítima e criminoso em países distintos. Com isso, nota-se uma obrigatoriedade de troca de informações e evidências eletrônicas entre as agências de combate ao crime. No entanto, ainda não há padrões internacionais, o que faz com que o valor jurídico de uma prova eletrônica seja contestável.

Você então se pergunta: como é realizada uma verificação em um computador?

Uma perícia envolve uma série de conhecimentos técnicos e a utilização de ferramentas. Para isso é necessário um conhecimento de alto nível em relação aos sistemas operacionais. (GUIMARÃES, 2001).

As ferramentas precisam ser específicas para o caso e não podem afetar ou perturbar o que está sendo analisado ou o alvo da perícia. Uma das

atividades, por exemplo, é análise dos arquivos (MAC times). A ferramenta utilizada não pode perturbar estes arquivos, pois poderia facilmente "rasurar" as utilizações recentes do computador.

No Brasil não existem normas para a forense computacional, porém há leis que podem ser usadas ou citadas para este tipo de perícia. Guimarães et. al.(2001) fala que no caso de uma perícia criminal existe a figura do Perito Oficial (dois para cada exame), onde o seu trabalho deve servir para todas as partes interessadas (Polícia, Justiça, Ministério Público, Advogados, etc.). Para desempenhar seu papel é necessário nível universitário e prestar concurso público específico.

Guimarães et. al (2001) cita as principais entidades:

- IOCE (*International Organization on Computer Evidence*): estabelecida em 1995 com o objetivo de facilitar a troca de informações entre as diversas agências. Investiga crimes envolvendo computadores ou outros assuntos relacionados ao meio eletrônico. Formula padrões para evidências computacionais e desenvolve serviços de comunicação entre as agências e organiza conferências.
- SWGDE (Scientific Working Group on Digital Evidence): Criado em 1998 nos Estados Unidos se esforça em padronizar os conceitos sugeridos e conduzidos pela IOCE.
- HTCIA (High Technology Crime Investigation Association): Discute e promove a troca de informações para auxiliar no combate ao crime eletrônico.
- IACIS (International Association of Computer Investigatibe Specialists): Composta por voluntários com objetivo de treinar novos peritos em forense computacional.
- SACC (Seção de Apuração de Crimes por Computador): Age no âmbito do Instituto Nacional de Criminalística/Polícia Federal, dando suporte em crimes ou incidente em que há presença de computadores.

Tente encontrar técnicas utilizadas pelos peritos forenses.

Descreva abaixo algumas técnicas que você encontrou e tente até mesmo realizá-las em seu computador.

4.4 Segurança da Informação – uma necessidade latente

Fernandes (2007) destaca que a Segurança da Informação é uma prática antiga. Já no passado existiam práticas de criptografia.

No entanto, foi a partir da década de 90, com a popularização da Internet, que a Segurança ganhou outro enfoque.

Assim, é importante analisar neste último capítulo o contexto atual de Segurança da Informação. Os dados apresentados abaixo são de uma pesquisa anual realizada pela PricewaterhouseCoopers. (FERNANDES, 2007)

- 60 por cento das empresas possuem uma área de segurança da informação com até quatro empregados;
- 30 por cento das empresas consideram sua estratégia de segurança alinhada ao negócio;
- 65 por cento das empresas já sofreram incidentes de segurança;
- 40 por cento das empresas já ficaram mais do que 4 horas com as operações paralisadas em virtude de incidentes;
- 70 por cento das empresas identificam como interna a origem dos ataques e incidentes de segurança da informação, e
- 27 por cento das empresas possuem um processo único e automatizado de gestão de identidades de usuários.

O que achou dos dados da pesquisa?

Concorda que ficou evidente que a maioria das empresas ainda não possui uma estrutura encorpada de segurança?

Ao analisar a pesquisa, Fernandes (2007) aborda que a minoria das empresas considera suas estratégias de segurança alinhadas ao negócio. Isso demonstra uma evolução por parte das organizações. Evidência disso está em outro dado, em que 70 por cento das empresas entendem que a origem dos incidentes de segurança é interna, mas apenas 27 por cento aplicam seus investimentos em soluções relacionadas à gestão de usuários e identidades digitais.

Com tais aspectos considerados, concorda que é necessário cada vez mais ter uma visão holística? Para tal, é preciso considerar Processos, Tecnologia e Pessoas. Fernandes (2007) destaca que quando os esforços são direcionados para tratar das pessoas e da influência das mesmas sobre o nível de segurança, o desafio é grande. A conscientização pode ser desenvolvida de várias formas, mas deve ser desenvolvida. Deve servir de suporte legal à Política de Segurança da Informação.

É interessante observar que à medida que o tempo passa, a segurança da informação começa a ser incorporada em outras áreas, pois com o avanço da tecnologia essas tornaram-se automatizadas.

O site Universo Jurídico (www.uj.com.br) aborda sobre essa necessidade de segurança. Em um artigo sobre o assunto, o Mestre em Direito José Carlos de Araújo Almeida Filho analisa a necessidade da proteção de dados no sistema da informatização judicial do processo, recém implantada pela Lei nº. 11.419/2006.

Esta fala sobre a transmissão de peças processuais através de meios eletrônicos

Assim, o autor aborda a questão do GED – gerenciamento eletrônico de documento, a questão da segurança da informação e a necessidade de normas previamente estipuladas e sempre de acordo com a ABNT27001.

Em nosso país, privacidade de dados se encontra regulamentada pelo Decreto 3505/2000, que institui a Política de Segurança da Informação nos

órgãos e entidades da Administração Pública Federal. Entre seus atributos encontramos garantias como assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição; uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais; criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

Notaram como muitos aspectos tratados pela Lei foram discutidos no decorrer do nosso Guia?

Esta Lei foi construída e se refere apenas à Administração Pública Federal.

O autor aborda que a preocupação se justifica quanto à possibilidade que as pessoas têm de consultar a Internet. Ele destaca, por exemplo, que a Internet não permite o esquecimento de dados. Estes ficam, permanentemente, alocados nos servidores e possíveis de serem analisados a qualquer momento.

Exemplo dessa preocupação é dado pela invasão de privacidade das comunidades de natureza virtual, como o *Orkut* e, agora, o *Youtube*, que violam, diariamente, os direitos mais sagrados do ser humano. Ele cita a obra do jornalista Heródoto Barbeiro:

"Hoje, usuários de microcomputador têm mais capacidade na ponta de seus dedos do que a NASA tinha como os computadores que usou na primeira viagem do homem à Lua. A tendência de uma capacidade, velocidade, redução de preços e mobilidade cada vez maior terá enorme implicação política: milhares de pessoas e de pequenos grupos – muitos dos quais nunca tiveram tanta capacidade – não apenas de conectarão com os outros, mas também planejarão, mobilizarão e cumprirão tarefas com resultados potencialmente mais satisfatórios e eficientes do que seus governos poderiam imaginar. Isso certamente afetará o relacionamento entre indivíduos, seus governos e diretrizes governamentais, bem como gerará pressão em alguns governos para que respondam de maneira mais ágil."

Podemos concluir que trata-se de uma realidade impensada a tempos atrás e que seus efeitos ainda serão sentidos futuramente.

A seguir o autor do artigo destaca que um sistema seguro deve obrigatoriamente ter uma certificação digital. Ainda, destacando este aspecto, ele destaca os requisitos mínimos: adoção de portais com criptografia e sistema ssl; adoção de *string* a fim de restringir a busca através dos motores na Internet, como *Google, Yahoo!*, dentre outros; a necessidade de adoção de certificação digital, dentro da hierarquia ICP-Brasil, nos termos da Medida Provisória 2.200-2/2001; adoção das normas ABNT 27001/2006; adoção do GED com filtros informáticos que impeçam a visualização do documento a não ser através de pessoas cadastradas.

Em outro artigo, intitulado "Necessidade de uma Política de Proteção à Informação para o Legislativo Federal", Alexandre Bento Hilgenberg destaca a necessidade de segurança, sobretudo para as Comissões Parlamentares de Inquérito – CPI's. Em seu artigo ele focaliza vários casos em que houve vazamentos de informações e isso prejudicou em muito o andamento das investigações. Destaca ainda que isso desmoraliza o Parlamento, gerando desconfiança por parte da população. Também apresenta ações necessárias para segurança, como:

- o treinamento do recurso humano;
- a preparação dos ambientes destinados a produção;
- análise e arquivamento dessas informações;
- a execução de contra-medidas, ou seja, medidas de detecção das falhas de segurança e a conscientização quanto a responsabilidade em preservar as informações sigilosas.

Essas informações que nos consideramos leva à uma boa reflexão.

Notem que os órgãos públicos estão preocupados com a questão de segurança. Isso, sem dúvida é um aspecto interessante, pois demonstra que investimentos serão feitos e conseqüentemente aportes para pesquisa nesse ramo serão destinados.

Além disso, percebemos que cada vez mais, os serviços estão sendo convergidos para o meio digital. O primeiro artigo destacou a sistematização computacional na área jurídica, o segundo destacou a

necessidade de segurança no Parlamento.

Observem que estamos falando de aspectos profundamente importantes para um país. Assim, se as camadas mais altas da república estão preocupadas com isso, quanto mais as empresas devem estar.

Dessa forma, é imperativo que a preocupação exista. Caminhamos para um mundo em que utilizaremos menos dinheiro (papel-moeda), este será cada vez mais virtual (cartões de débito, crédito) e com isso melhoramos a segurança física, mas precisaremos ainda mais da segurança lógica.

Não precisaremos sair de casa para realizar uma compra, mas precisaremos de investimentos para que a loja saiba que o cliente que está comprando trata-se do cliente real mesmo, e não alguém se passando por ele.

Além disso transações virtuais de negócios são realizados aos trilhões em todo mundo, sem nem mesmo às vezes ter um encontro formal de negócios. Julgamentos já podem ser realizados pelo Juiz via videoconferência. O voto também é eletrônico.

Tais exemplos, apenas demonstram que a área de segurança estará em crescente expansão sempre, pois sempre teremos novas tecnologias, novos serviços e aspectos de segurança sendo quebrados e a necessidade, portanto, de se criar novas formas – criativas e até certo ponto simples – para garantir os níveis aceitáveis do mundo virtual para o real.

Lembro que há 8 anos atrás quando se falava em compras pela Internet, não raro as pessoas “torciam o nariz”. Hoje, já comprovamos que é mais seguro fornecer o número de seu cartão pela Web – logicamente em um site com um bom nível de segurança – a dar seu cartão nas mãos do atendente da loja ou do mercado.

Tudo isso que falamos somente nos mostra a necessidade enorme que teremos de ter pessoas para pensar em como prover melhor segurança aos dados que lhe interessa.

Já conversaram com alguém que teve sua conta de e-mail ou da comunidade virtual invadida? Ou que comprou e não recebeu? Creio que todos nós já conhecemos alguém. Com isso percebemos que realmente falta

bons e melhores métodos de segurança tanto no nível empresarial como no nível pessoal.

Isso é importante destacar tendo em vista que os alvos são desde grandes corporações reconhecidas por investir milhões em segurança até o mais simples usuário de Internet.

Interessante isso não é?

Isso somente reforça o que estamos falando, pois se há ataques a todo o momento em instituições de grande porte, isso evidencia que o nível de segurança não é alto. Senão, os ataques seriam menores e certo desânimo em quebrar a barreira de segurança.

Notem que não estou dizendo que as técnicas de segurança são todas ruins.

Estamos vivendo esse mundo agora, estamos construindo as barreiras de segurança a muito pouco tempo.

Podemos comparar nossas seguranças atuais às armas que existiam nos períodos feudais. Mesmo grandes fortalezas eram invadidas. Um dia, alguém descobria um ponto fraco.

A segurança de sistemas é igual. Por mais investimentos que se faça, por mais técnicas que existam hoje, um dia alguém descobre um ponto fraco.

Mas notem que, a cada ano, surgem novos sistemas operacionais e novos aplicativos, que apresentam, por conseqüência, novos desafios para prover segurança.

Mais um exemplo disso é o artigo publicado na Revista InformationWeek de Edgar D'Andrea. Ele cita um estudo da Symantec que revelou que a Copa do Mundo é o evento mais atrativo do ano para os autores de *malwares e spams*. Isso levou a empresas a monitorar e analisar o tráfego de rede na África do sul, com o objetivo de alertar o mercado sobre ameaças de segurança relacionadas ao evento.

Até aqui nenhuma novidade, mas o autor cita as técnicas esperadas para os ataques, quais são:

- Uso tradicionais técnicas de spam
- Phising
- Roubo de identidade
- Venda de ingressos falsos
- Vírus, denial-of-service e cavalos de troia.

Além do próprio evento ser alvo, as possibilidades do país-sede também ser alvo de ataques de hackers é muito grande. Estes objetivam propagar o terrorismo, desmoralizar a organização da Copa e manchar a imagem da nação.

O artigo cita outra empresa, a McAffe. Segundo a revista, esta empresa menciona que o aumento das atividades de phising relacionadas ao Mundial e reforça o ativismo político de hackers fora do eixo EUA-China, destacando atividades recentes de terrorismo via web em países como Irã, Dinamarca, Suécia e Polônia.

No entanto, o interessante é o desfecho do autor. Ele nos cita – como país – um alvo enorme durante a Copa. Por quê?

Por causa da nossa paixão pelo futebol. Seria muito fácil conseguir com que usuários no Brasil abrissem mensagens maliciosas ou com conteúdo invasivo com desculpa de ser informações sobre nossa Seleção.

Recentemente, o portal Terra trouxe uma reportagem com números interessantes – números citados no artigo acima. Apresentou dados da Symantec realizado em cerca de 20 mil sensores do DeepSight Threat Management System, instalados em mais de 180 países.

A avaliação mostra que 64% dos novos ataques visam vulnerabilidades com menos de um ano. Além disso, 66% das invasões detectadas no primeiro semestre deste ano usaram brechas de segurança classificadas como altamente críticas. O estudo ainda recomendou aos usuários e administradores de rede a adoção das seguintes práticas para melhorar a segurança da Internet:

- desligue e remova serviços desnecessários;

- mantenha os sistemas atualizados com os patches de correção, especialmente em computadores que hospedam serviços públicos e são acessíveis por meio de um firewall, como serviços de HTTP, FTP, e-mail e DNS;
- reforce a política de senhas;
- configure os servidores de e-mail para bloquearem ou removerem as mensagens que contenham arquivos anexados usados normalmente para disseminar vírus, como os arquivos .vbs, .bat, .exe, .pif e .scr;
- isole rapidamente os computadores infectados para prevenir futuros comprometimentos na empresa.
- realize uma análise detalhada e restaure os computadores por meio de soluções confiáveis;
- treine os funcionários para abrir arquivos anexados somente se forem documentos solicitados pelo usuário. Oriente-os também para não fazerem download de software pela Internet, a não ser que tenha sido verificado por um antivírus;
- certifique-se de que os procedimentos de respostas a emergências foram implementados;
- teste a segurança para garantir que os controles adequados foram adotados.

O que são essas ações acima? Como implementá-las?

Política de Segurança. Cada vez mais vital para sobrevivência das organizações. Não há saída.

Interessante que essa reportagem citada acima foi de 2004. Ela cita o Brasil em 15º lugar como alvo de ataques.

No entanto, notem no dia 20 de abril o site da Revista Info publicou uma pesquisa realizada em 2009, em que coloca nosso país em 3º lugar no ranking mundial.

Um salto enorme em pouco tempo. A reportagem mostrou os Estados Unidos em primeiro, com 19%, a China em segundo, 8%, e o Brasil, terceiro,

com 6%. De acordo com o estudo, software de segurança falso foi o maior problema de segurança online para os usuários de computadores em 2009.

Ressaltou ainda como novidade os grandes e fortes ataques aos sites de grandes empresas, como o *Google.*

Apontou como forma mais comum de crime de computação o falso software de segurança. Isso seria um alerta que surge em na tela do usuário dizendo que o computador está infectado. Junto com isso há um link para um software ser baixado, mediante pagamento. O usuário, no entanto, em lugar de receber software de segurança recebe um vírus.

Assim, mais uma vez comprovamos a necessidade urgente de cada vez mais pesquisa e desenvolvimento na área de segurança.

Abaixo, reservei um espaço para que você aliste algumas ideias inovadoras sobre segurança. Pense nas já existentes e tente moldá-las para novas realidades, pensando em novas tecnologias.

Bom trabalho!

CONCLUSÃO

Esta unidade objetivou evidenciar a importância de estabelecer uma política de segurança. Um incidente pode acontecer a qualquer momento e, portanto, é necessário conseguir estabelecer um passo a passo de ações que deverão nortear a recuperação ao incidente. Do contrário, as ações serão desordenadas e não conseguirão estabelecer um plano inteligente e lógico. Embora não seja algo relativamente simples, é importante estabelecer planos mesmo para pequenos incidentes, isso gera confiança e experiência tanto para solução de problemas como para prever situações mais críticas.

Nesse aspecto, vimos ainda como é importante incluir o corpo diretivo da organização e conscientizá-lo de que não serão despesas, mas sim investimentos em segurança. É primordial conseguir explicar a importância disso e sempre que possível tentar tangibilizar a solução de incidentes. Isso implica em estabelecer valor para os serviços e mostrar o quanto economizou ou o quanto de lucro foi gerado com a manutenção do serviço.

BIBLIOGRAFIA

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. Segurança no desenvolvimento de Software. Rio de Janeiro: Campus, 2002.

BEAL, Adriana. Segurança da Informação. São Paulo: Atlas, 2005.

CERT. <http://www.cert.br/certcc/csirts/Creating-A-CSIRT-br.html> Acessado em 10/01/2010.

ESPODE, Elton Régis. Auditoria e Segurança de Sistemas. Santa Maria: 2008. (Notas de Aula da disciplina de Segurança e Auditoria de Sistemas, Curso de Sistemas de Informação, Unifra)

FERNANDES, Marcelo Lemos. Tecnologia da Informação e da Comunicação – A Busca de uma Visão Ampla e Estruturada. São Paulo: Editora Pearson, 2007

FILHO, Hélio Alano. Segurança e Auditoria de Sistemas. Salvador: 2008. (Apostila da disciplina de Segurança e Auditoria de Sistemas, Curso de Sistemas de Informação, Faculdade Hélio Rocha)

GIL, Antônio de Loureiro. Auditoria de Computadores, 2000, Atlas, 5ª Edição

GUIMARÃES, Celio Cardoso, et al. Forense Computacional: Aspectos Legais e Padronização. 2001:Unicamp

LYRA, Maurício Rocha. Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008

SÊMOLA, Marcos. Gestão de segurança da informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

WANDERLEY, Euricélia Viana. MOURA, Maria Teresa. A Integração de LDAP e Certificados Digitais em uma Política de Segurança. Boletim RNP: 2000