Segurança da Informação

Nélia O. Campo Fernandes

Cuiabá-MT
2013

Presidência da República Federativa do Brasil
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Diretoria de Integração das Redes de Educação Profissional e Tecnológica

©Este caderno foi elaborado pelo Instituto Federal de Educação, Ciência e Tecnologia de Rondônia/RO para a Rede e-Tec Brasil, do Ministério da Educação em parceria com a Universidade Federal do Mato Grosso.

Equipe de Revisão
Universidade Federal de Mato Grosso – UFMT

Coordenação Institucional
Carlos Rinaldi

Coordenação de Produção de Material Didático Impresso
Pedro Roberto Piloni

Designer Educacional
Neusa Blasques

Designer Master
Marta Magnusson Solyszko

Diagramação
Tatiane Hirata

Revisão de Língua Portuguesa
Marta Maria Covezzi

Revisor Final
Marta Magnusson Solyszko

Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO
Campus Porto Velho Zona Norte

Direção-Geral
Miguel Fabrício Zamberlan

Direção de Administração e Planejamento
Gilberto Laske

Departamento de Produção de EaD
Ariádne Joseane Felix Quintela

Coordenação de Design Visual e Ambientes de Aprendizagem
Rafael Nink de Carvalho

Coordenação da Rede E-Tec
Ruth Aparecida Viana da Silva

Projeto Gráfico
Rede e-Tec Brasil / UFMT

Dados Internacionais de Catalogação na publicação

Apresentação Rede e-Tec Brasil

Prezado(a) estudante,

Bem-vindo(a) à Rede e-Tec Brasil!

Você faz parte de uma rede nacional de ensino que, por sua vez, constitui uma das ações do Pronatec - Programa Nacional de Acesso ao Ensino Técnico e Emprego. O Pronatec, instituído pela Lei nº 12.513/2011, tem como objetivo principal expandir, interiorizar e democratizar a oferta de cursos de Educação Profissional e Tecnológica (EPT) para a população brasileira propiciando caminho de acesso mais rápido ao emprego.

É neste âmbito que as ações da Rede e-Tec Brasil promovem a parceria entre a Secretaria de Educação Profissional e Tecnológica (Setec) e as instâncias promotoras de ensino técnico, como os institutos federais, as secretarias de educação dos estados, as universidades, as escolas e colégios tecnológicos e o Sistema S.

A educação a distância no nosso país, de dimensões continentais e grande diversidade regional e cultural, longe de distanciar, aproxima as pessoas ao garantir acesso à educação de qualidade e ao promover o fortalecimento da formação de jovens moradores de regiões distantes, geograficamente ou economicamente, dos grandes centros.

A Rede e-Tec Brasil leva diversos cursos técnicos a todas as regiões do país, incentivando os estudantes a concluir o ensino médio e a realizar uma formação e atualização contínuas. Os cursos são ofertados pelas instituições de educação profissional e o atendimento ao estudante é realizado tanto nas sedes das instituições quanto em suas unidades remotas, os polos.

Os parceiros da Rede e-Tec Brasil acreditam em uma educação profissional qualificada – integradora do ensino médio e da educação técnica – capaz de promover o cidadão com capacidades para produzir, mas também com autonomia diante das diferentes dimensões da realidade: cultural, social, familiar, esportiva, política e ética.

Nós acreditamos em você!
Desejamos sucesso na sua formação profissional!

Ministério da Educação
Janeiro de 2014

Nosso contato
etecbrasil@mec.gov.br

Indicação de ícones

Os ícones são elementos gráficos utilizados para ampliar as formas de linguagem e facilitar a organização e a leitura hipertextual.

Atenção: indica pontos de maior relevância no texto.

Saiba mais: oferece novas informações que enriquecem o assunto ou "curiosidades" e notícias recentes relacionadas ao tema estudado.

Glossário: indica a definição de um termo, palavra ou expressão utilizada no texto.

Mídias integradas: remete o tema para outras fontes: livros, filmes, músicas, *sites*, programas de TV.

Atividades de aprendizagem: apresenta atividades em diferentes níveis de aprendizagem para que o estudante possa realizá-las e conferir o seu domínio do tema estudado.

Reflita: momento de uma pausa na leitura para refletir/escrever sobre pontos importantes e/ou questionamentos.

Palavra da Professora-autora

Prezado(a)estudante,

É com grande satisfação que estamos lhe recebendo nessa nova empreitada. Estudar esta disciplina significa que você irá dar um passo em direção ao aperfeiçoamento da sua carreira profissional e pessoal. Para isso, vamos precisar de seu esforço e dedicação na realização desse empreendimento.

Para atingirmos nossas metas com êxito, orientamos você a utilizar todos os recursos que disponibilizamos para melhor aproveitamento e rendimento nas atividades propostas.

Este caderno será o seu guia de estudos, apresentando um roteiro dos assuntos a serem abordados e direcionando a outros espaços para o seu aperfeiçoamento.

É importante, você reservar sempre um tempo para seus estudos complementares, além da realização das atividades propostas no ambiente virtual, sendo mais um momento para refletir sobre o conteúdo das aulas, rever conceitos e sanar dúvidas que normalmente ocorrem quando estamos enfrentando novos desafios. Para isso, poderá contar com seu professor-tutor para orientá-lo nessa jornada, além, é claro, do ambiente virtual, dos grupos de discussões, enfim, com os vários recursos disponibilizados que servirão de suporte em seu processo de aprendizagem.

Apresentação da Disciplina

Prezado(a) estudante,

Atualmente, vivemos num mundo totalmente interligado pelas redes de computadores, as quais nos permitem interagir com pessoas do outro lado do mundo, bastando apenas acessar a Internet no seu celular, tablet, notebook... Nesse mundo maravilhoso, podemos nos divertir, aprender, ensinar ou simplesmente passar o tempo.

Contudo, todas essas facilidades têm um preço. Os cuidados que devemos ter ao acessar a Internet devem ser muitos, pois uma vez que você se conecta, pode ser entendido como: olá, estou aqui, venham me visitar! Nesse caso, você poderá receber a visita de qualquer pessoa, com boas intenções ou não.

É justamente aí que devermos ter cuidado com a segurança das informações que guardamos em nossas máquinas, seja uma simples fotografia de aniversário, ou até mesmo um trabalho da escola, senhas de acesso a bancos, tudo deve estar bem protegido, para que somente pessoas autorizadas possam visualizar essas informações.

O objetivo da disciplina Segurança da Informação no curso técnico é o de tratar dos mecanismos de segurança das informações, pois atualmente esse tema vem assumindo posição de destaque nas discussões nacionais e internacionais por tratar-se de um patrimônio empresarial ou pessoal bem relevante.

Com o passar dos anos, novos modelos de segurança foram surgindo, emergindo desse processo a formação de uma nova sociedade, em função da popularização da informação em massa.

Diversos eventos mundiais foram promovidos com o objetivo de discutir sobre as mais eficientes maneiras de proteger as informações. A conclusão foi uma só: proteger um dos ativos mais importantes contra ataques é uma tarefa difícil que requer implementação de novas técnicas de segurança e constantes modificações, de forma a acompanhar essa evolução acelerada.

Diante desse quadro, a disciplina Segurança da Informação foi inserida no curso de Técnico em Informática para Internet com o intuito de apresentar e discutir temas que auxiliarão você a enfrentar os problemas de segurança da informação que porventura possam surgir na empresa onde atuará.

Para efeitos didáticos, a disciplina Segurança da Informação possui uma carga horária de 60 horas, cujo caderno aqui apresentado está dividido em oito aulas. Nas duas primeiras aulas, faremos uma Introdução à Segurança da Informação; na aula três, abordaremos os Mecanismos e Tecnologias de Segurança. A seguir, trataremos dos conceitos de segurança em rede e, finalmente, nas três últimas aulas, veremos Controles de Segurança da Informação.

Este caderno procura ofertar uma instrumentalização teórica que possa ampliar a compreensão acerca do tema segurança da informação, da qual todos nós participamos, na criação e distribuição, assim como nos possibilitará uma atuação profissional transformadora.

Além deste material didático, você conta com recursos técnico-pedagógicos que facilitarão sua aprendizagem, como a biblioteca física e virtual, o ambiente virtual, os fóruns de discussão, assim como o acompanhamento do professor tutor a distância e do tutor presencial.

Também pode contar com a autoavaliação, uma ferramenta importante para averiguar o seu desempenho. Lembre-se de que, no Ensino a Dis¬tância, a construção do conhecimento ocorre de forma cooperati¬va e colaborativa; compartilhe, portanto, as suas descobertas com seus colegas.

O curso inclui momentos de aprendizagem a distância e de encontros presenciais, que são importantes para interagir com seus colegas e tutores presenciais, propiciando atividades práticas e avaliação.

Nesta disciplina, seguindo as orientações do professor responsável e do tutor, você terá a oportunidade de aprender conceitos sobre segurança da informação, mecanismos existentes e controles que devem assegurar o patrimônio de uma empresa.

Bons estudos!

Sumário

Aula 1. Conceitos básicos de segurança da informação 15

1.1 Sociedade da Informação: a informação e sua importância 15

1.2 Segurança da informação 18

1.3 Função do departamento de segurança de Informação de uma empresa 19

1.4 Princípios da segurança da informação 20

Aula 2. Problemas de segurança da informação 23

2.1 Principais problemas de segurança 23

Aula 3. Mecanismos e tecnologias de segurança 29

3.1 Controles de pessoal 29

3.2 Controles físicos 30

3.3 Segurança de equipamentos 30

3.4 Controles de acesso lógicos 31

3.5 Outros mecanismos de segurança 31

Aula 4. Conceitos de segurança em rede: criptografia, assinatura e certificado digital 39

4.1 Criptografia, fases e classificação 39

4.2 Assinatura digital 43

4.3 Certificado digital 44

Aula 5. Conceitos de segurança em rede: Autoridade Certificadora – AC, autenticação e firewall 49

5.1 Autoridade Certificadora – AC 49

5.2 Autenticação 51

5.3 Firewall 51

5.4 Tipos de firewall 52

5.5 Localização do firewall 53

AULA 6. Controles de segurança da informação: política de segurança da informação **57**

6.1 Política de segurança da informação 57

6.2 Criação de aplicações seguras: características de uma política de segurança 59

6.3 Política de uso aceitável (AUP – acceptable use policy) 61

6.4 Plano de contingência 61

6.5 Plano de recuperação de desastre 63

Aula 7. Controles de segurança da informação: criação de aplicações seguras **65**

7.1 Criação de aplicações seguras 65

7.2 Características de um ambiente seguro 66

7.3 Etapas para segurança no ambiente de desenvolvimento 67

7.4 Segurança no ciclo de vida de desenvolvimento da aplicação 69

Aula 8. Controles de segurança da informação: auditoria em sistemas computacionais **73**

8.1 Auditoria em sistemas computacionais 73

8.2 Conceito de auditoria 74

8.3 Padrões 74

8.4 Formas de auditoria em sistemas de informação 77

8.5 Etapas de uma auditoria 79

Palavras finais **83**

Guia de Soluções **84**

Referências **102**

Obras Consultadas **104**

Currículo da Professora-autora **105**

Aula 1. Conceitos básicos de segurança da informação

Objetivos:

- reconhecer a importância da informação;
- identificar conceitos básicos de informação, segurança e segurança da informação; e
- apontar as funções de um de departamento de tecnologia da informação.

Prezado(a) estudante,

Nesta primeira aula, você terá uma visão geral do que será es¬tudado no decorrer da disciplina. Aqui, você entrará em contato com os principais assuntos de forma breve e geral e terá a oportunidade de aprofundar essas questões nas próximas aulas. Desse modo, essa abordagem geral visa fornecer-lhe o conhecimento básico necessário a partir do qual você possa cons¬truir um referencial teórico com bases sólidas para que, no futuro exercício de sua profissão, você a exerça com competência, ética e responsabilidade social. Vamos co¬meçar nossa aventura pela apresentação das ideias de Sociedade da Informação, segurança e dos princí¬pios básicos que fundamentam esta disciplina.

1.1 Sociedade da Informação: a informação e sua importância

O termo "Sociedade da Informação" também é conhecido como "Globalização", a qual se apresenta ainda em formação e em plena expansão, pois é caracterizada pelo seu dinamismo, uma vez que as tecnologias existentes são as fontes desse processo de mudança.

Essas transformações implicam diretamente no comportamento social, econômico e cultural de uma sociedade, pois as novas tecnologias são uma fonte de poder inesgotável de produção de novos conhecimentos e estão enraizadas nessa nova sociedade, a chamada "Sociedade do Conhecimento".

A-Z

Paradigma:
Algo utilizado como padrão a ser seguido, modelo, exemplo.>

Fonte: Disponível em: <**http://www.dicio.com.br/paradigma/** > Acesso em: 8 Abr 2013. >

Esse novo **paradigma** de organização da sociedade, é caracterizado pela contínua geração de informação, estabelecendo um novo padrão de produção de novas riquezas visando acima de tudo o bem-estar dos cidadãos.

Esse grau de exigência requer um maior desempenho profissional, pois o mercado de trabalho pede profissionais mais bem preparados, em virtude de as informações serem mais complexas e em grande quantidade, resultado das facilidades ofertadas pelas tecnologias.

São nítidos os aspectos favoráveis ao uso das tecnologias em nossas vidas. Esse fato pode ser observado na medicina, por exemplo, possibilitando fazer cirurgias a distância; outro exemplo são as viagens espaciais, enfim, basta olhar para o lado e observar que as tecnologias estão introduzidas no seu cotidiano.

As máquinas estão substituindo o homem em tarefas repetitivas que muitas vezes requerem apenas força bruta, precisão ou mesmo adentrar em locais de difícil acesso e perigosos, oportunizando ao homem desempenhar um papel de detentor do conhecimento, e a máquina, mera coadjuvante, um apoio na tomada de decisões.

A seguir traremos alguns conceitos de informação,

1.1.1 Conceitos fundamentais

Muitas mudanças ocorreram com a introdução da Internet em nosso cotidiano, a informação, por exemplo, não era um ativo muito importante nas organizações há certo tempo; o importante eram os equipamentos, considerados o maior patrimônio de uma empresa. Com o passar dos tempos e a modernização das estruturas de trabalho, novos modelos de gestão foram surgindo e alguns ativos, anteriormente sem importância, assumiram a primeira posição.

- **Informação**

Atualmente, a informação é um ativo importantíssimo, que requer cuida-

dos especiais e restrições de acessos, por ser um ativo intangível e abstrato, podendo facilmente sair da empresa em uma lata de lixo, na memória de alguém, em meio magnético, impressa em papel, enfim, é um ativo muito vulnerável, logo, demanda cuidados.

Mas o que exatamente entendemos por Informação? Bem, entende-se por Informação, "ativos que, como qualquer outro ativo importante para os negócios, possuem valor para uma organização e consequentemente precisam ser protegidos adequadamente", conforme ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) nº 17799.

Fontes (2006, p.2) afirma que, "Informação é um recurso que move o mundo, além de nos dar conhecimento de como o universo está caminhando [...] É um recurso crítico para realização do negócio e execução da missão organizacional".

Fontes também acrescenta que:

> A informação é um recurso que tem valor para a organização e deve ser bem gerenciado e utilizado [...] é necessário garantir que ela esteja sendo disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais. (2006, p. 2)

Podemos dizer então que informação é um conjunto de dados que, por sua vez, poderá gerar novas informações, consistindo em um ativo valioso para a organização.

Exemplo: Ao nascermos, somos registrados em cartório, esse documento é conhecido como Certidão de Nascimento, imagine que cada campo que foi digitado na certidão seja um dado. Preenchidos todos os campos, você tem um conjunto de dados, esse conjunto de dados gera uma informação que conhecemos como Certidão de Nascimento. Com o passar dos anos, você tem a necessidade de obter outros documentos, como por exemplo, a Cédula de Identidade, conhecida como RG. (Registro Geral). Para obtenção desse documento você deverá apresentar a Certidão de Nascimento para gerar outra informação, intitulada RG, e assim por diante.

1.2 Segurança da informação

A Segurança da Informação é um tema bastante discutido não somente em salas de aula, como também nas redes sociais e em outros meios de comunicação, por tratar-se de assegurar informações tanto pessoais como corporativos, que uma vez lidos ou até mesmo distribuídos, poderão ocasionar transtornos diretos e/ou indiretos à vítima.

Há inúmeras definições de Segurança da Informação, pois há vários autores que discorrem a respeito do assunto, vamos então citar algumas:

Para Alves (2006, p. 15), a Segurança da Informação "visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios".

Há também um sistema especializado para padronização mundial, formado pela ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) e definem Segurança da Informação "como uma proteção das informações contra uma ampla gama de ameaças para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidade comerciais".

Sêmola (2003, p. 9) define Segurança da Informação como "uma Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Para Ferreira, a Segurança da Informação:

> Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades. (2003, p.162)

Nesse contexto, a informação é um Ativo muito desejado e valioso tanto para uma pessoa como para uma organização, devendo obrigatoriamente estar protegido de acessos não autorizados. Na aula dois, trataremos sobre ativo com mais detalhes.

Se voltarmos na história, na época da Revolução Industrial, pouco se pensava em segurança da informação e, se pensavam, o problema era facilmente

solucionado, porque as informações que circulavam em uma empresa eram feitas em formulários, apresentadas em papel, e eram arquivadas em armários com chaves.

Com o passar do tempo, já no século XX, foram introduzidas em pequenos bancos de dados e armazenadas no próprio computador com acesso bastante restrito, porque pouquíssimas pessoas manipulavam a máquina. Mais tarde, com o advento da Internet, é que esse quadro foi mudando, no final do século XX o processo intitulado Globalização trouxe drásticas mudanças na administração dos negócios, as informações já não podiam circular facilmente pelos computadores em discos flexíveis sem maiores preocupações, pois os sistemas caminhavam pelas redes de computadores, sendo possíveis acessos não autorizados.

Hoje, a dependência pelos sistemas informatizados é gigante, a sobrevivência de muitas organizações depende exclusivamente desses ambientes, tornando esses ativos ainda mais valiosos e cobiçados, pois passaram a integrar todos os processos da empresa, ou seja, nesses sistemas armazenam-se, processam-se e transmitem-se dados corporativos, tornando os processos mais rápidos e eficientes, contudo, se usado inadequadamente, tem o poder de inviabilizar resultados satisfatórios.

Atividades de aprendizagem

1. Qual a importância da informação para a sociedade?

2. Conceitue Informação.

3. Elabore um conceito de Segurança da Informação.

1.3 Função do departamento de segurança de Informação de uma empresa

Basicamente, as atividades pertinentes a esse setor envolvem a criação, implementação, controle e monitoramento de políticas que almejam assegurar os ativos de informação de uma empresa ou pessoa.

As áreas de negócios são seu foco, principalmente os setores que utilizam as tecnologias para o desenvolvimento dos trabalhos, sendo um recurso indispensável aos processos de produção atualmente.

A-Z

Sinergia:
Ação simultânea
Disponível em: <**http://www.dicio.com.br/sinergia/**>
Acesso em 8 Abr 2013

É importantíssimo haver **sinergia** entre o Departamento de Segurança de Informação e os demais departamentos de uma empresa, devendo funcionar de forma coordenada. Caso ocorra fragmento dentro da organização, o gerenciamento do negócio pode tornar-se inviável e qualquer implementação de segurança da informação estará fadada ao insucesso, prejudicando toda a organização.

Para existir essa segurança da informação, foram estabelecidos princípios conforme pode ser observado a seguir.

1.4 Princípios da segurança da informação

Conforme descrição feita pela norma ISO/IEC 17799, a proteção da informação é vital, sendo caracterizada pela trilogia CID, ou seja, **C**onfidencialidade, **I**ntegridade e **D**isponibilidade.

- **Confidencialidade**

Garante que somente pessoas autorizadas poderão acessar as informações. Trata-se da não permissão da divulgação de uma informação sem prévia autorização.

- **Disponibilidade**

Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema. Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando!

- **Integridade**

Garante que a exatidão e completeza das informações não sejam alteradas ou violadas. Um exemplo, vamos supor que um gerente de uma empresa determina aumento de salário de 2% aos funcionários, para isso, utilizou seu e-mail para o departamento financeiro. Alguém interceptou e alterou de 2% para 20% o aumento!!!

Além da trilogia CID, citados anteriormente, Sêmola (2003) acrescenta outros aspectos da segurança da informação, são eles:

Legalidade: Garantia de que a informação foi produzida em conformidade com a lei;

Autenticidade: garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

Resumo

Nesta primeira aula, procuramos contextualizar o tema Segurança da informação na Sociedade, tendo como foco central sua importância para os negócios. Abordamos também conceitos de segurança, informação e segurança da informação, assim como os princípios básicos que norteiam a segurança da informação.

Atividades de aprendizagem

Discuta com seus colegas as seguintes questões:

4. Identifique os objetivos do Departamento de Segurança da Informação em uma empresa.

5. Quais os princípios da segurança da informação? Defina-os.

6. Relacione a primeira coluna de acordo com a primeira:

(a) Informação	( ) Disponibilidade, Confidencialidade e Integridade.
(b) Segurança da informação	( ) É um conjunto de dados.
(c) Princípios básicos da segurança da informação	( ) Criar, implementar, controlar e monitorar políticas que assegurem os ativos.
(d) Função do Departamento de TI nas empresas	( ) São regras criadas para proteger os ativos de uma empresa.

Caro(a) estudante,

Nesta aula, você estudou conceitos importantes de Segurança da informação que lhe dará subsídios para avançar no conteúdo. Para reforçá-los, retome os tópicos apre¬sentados com a intenção de rever questões que não ficaram claras. Na próxima aula, abordaremos outros problemas de segurança.

Aula 2. Problemas de segurança da informação

Objetivos:

- reconhecer ativos da Informação; e
- identificar problemas de segurança causadores da perda de dados.

Caro/a estudante,

Iniciaremos esta aula com uma definição de Incidente, pois dentro da segurança da informação, vários são os termos aplicados quando se trata de proteger as informações de uma empresa. Além disso, veremos também alguns fatores que acarretam problemas de segurança aos ativos da empresa, assim como suas características e diferenças. Acreditamos que o conteúdo a seguir será de grande auxílio quando você estiver atuando na área para a qual está se qualificando.

2.1 Principais problemas de segurança

Incidente pode ser definido como uma ação que pode interromper os processos normais de negócio, em virtude de alguns aspectos da segurança terem sido violados, seja intencionalmente ou não.

Em segurança de informação, a palavra Ativo refere-se a tudo que representa valor para a organização. Caso esse ativo seja violado, poderá trazer impactos negativos para o prosseguimento das atividades da organização. Podemos citar como ativos as pessoas, os programas, os equipamentos, enfim, tudo que na sua ausência gera transtornos, implicando no bom funcionamento dos negócios.

Quando falamos em problemas de segurança, há inúmeros fatores que acarretam a perda e/ou violação dos dados de uma empresa, como por exemplo,

a má operação do sistema ou mesmo quando a segurança está sofrendo ameaça, risco, vulnerabilidade, falhas e desastres. A seguir abordaremos cada um desses fatores.

2.1.1 Ameaças

Quando um ativo da informação sofre um ataque potencial, podemos entender como ameaça. Este ataque poderá ser efetuado por agentes externos (empresas, pessoas que não são funcionários da organização) ou internos (pessoas pertencentes à organização), se prevalecendo das vulnerabilidades apresentadas no sistema empresa.

As vulnerabilidades são mais nítidas em sistemas de informação online e nos sistemas que utilizam os recursos das telecomunicações, por interligarem seus sistemas em vários locais, as chamadas intranets ou mesmo as extranets. Nesses casos, a exposição é muito grande, pois as ameaças aumentam substancialmente, uma vez que o sistema da empresa está na rede Internet. Muitas pessoas tentarão acessar informações mesmo sem autorização, se houver falhas de segurança.

Esses sistemas que utilizam esses novos padrões de rede ampliam consideravelmente as vulnerabilidades, uma vez que a comunicação pode ser feita também pelas redes de dados sem fio, que por sua vez são difíceis de serem protegidas em virtude dos vários pontos de acesso, possibilitando ainda mais a quebra da confidencialidade das informações.

As redes empresariais precisam de muitos **recursos** tanto **físicos** como **lógicos** para proteger seus ativos das ameaças e fraquezas.

Recurso Físico: É toda segurança que impede acesso físico de pessoas não autorizadas às dependências da empresa, acesso aos computadores, às pessoas, enfim, qualquer proteção física implementada aos ativos físicos da empresa.

Recurso Lógico: Visa proteger os programas de computador da empresa, cujas atividades pertinentes a empresa são realizadas. Exemplos desses recursos lógicos é o uso de anti vírus, firewall, controle do acesso a internet, etc.

Existem diversos tipos de ameaças, Sêmola (2003) classifica-as em categorias, a saber:

Naturais: decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição.

Involuntárias: são inconscientes, podendo ser causadas por acidentes, erros, falta de energia etc.

Voluntárias: são propositais, causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de malwares, incendiários etc.

2.1.2 Riscos

Praticamente, quase toda empresa e/ou usuário doméstico usa a Internet no seu dia a dia, uma ferramenta que possibilita facilidades e oportunidades tanto profissionais como de entretenimento e lazer. Seria muito difícil para estas pessoas viverem sem ela.

Infelizmente, para aproveitar todos esses recursos, são necessários certos cuidados, pois os riscos são inúmeros, como por exemplo:

Ao acessar a Internet, sua máquina já está exposta na rede, você poderá ter seus dados pessoais expostos, e caso sejam acessados por alguém mal intencionado, isso poderá lhe proporcionar grandes transtornos.

Uma pessoa, uma vez com seus dados, poderá querer se passar por você na rede e usar sua identidade até mesmo para lhe expor, colocando em risco a sua reputação, ou cometer crimes como, estelionato, sequestro, pedofilia.

Não é muito prudente você achar que não corre riscos; acreditar que ninguém tem interesse em se apropriar do seu computador, tablet ou celular é mero engano, pois muitos intrusos mal intencionados têm interesse em acessar grandes quantidades de máquinas, não importando quais. Um exemplo que tivemos aqui no Brasil foi o ataque ao site do governo federal, os sites presidencia.gov.br e o brasil.gov.br, deixando-os indisponíveis em função da grande quantidade de acessos, esses acessos poderiam estar sendo feitos pelo seu computador também, os chamados ataques de spam.

As informações na Internet correm numa velocidade muito grande, o que em alguns momentos pode ser benéfico e, em outros, dependendo da situação, pode ser extremamente destrutivo.

Para as empresas, isso não seria diferente, pois todo ativo apresenta algum risco para a organização, podendo gerar um impacto grande ou pequeno aos negócios. Para isso, é necessário fazer um levantamento dos ativos e classificá-los quanto aos riscos, de forma que a facilitar a implementação de uma política de segurança mais eficiente.

Mas para aproveitarmos esses recursos de forma segura, é importante prevenir-se instalando um bom antivírus e claro atualizando-o diariamente, não acessando qualquer site, sem saber exatamente a procedência dos dados, utilizar softwares originais, evitando a pirataria. Oportunamente trataremos

desses aspectos com mais detalhes.

2.1.3 Vulnerabilidades

Podemos entender por vulnerabilidades as falhas que um sistema possui, podendo provocar a indisponibilidade das informações, ou até mesmo a quebra do sigilo e alteração sem autorização, podendo ser decorrente de uma série de fatores, como falta de treinamento, falta de manutenção, falha nos controles de acesso, ausência de proteção de uma determinada área ameaçada. Por exemplo, a criação de contas no sistema sem especificar as restrições e permissões.

A ocorrência de um incêndio poderá também estar associada à vulnerabilidade da empresa quanto a esse tipo de incidente, devido ao fato de a empresa não ter tomado as precauções adequadas contra incêndios.

Podemos classificar as vulnerabilidades em três categorias:

- **Tecnológicas:** compreendem as redes de computadores, os computadores, ameaças por vírus, hacker, enfim, todas as atividades que envolvem tecnologia.

- **Físicas:** representadas pelo ambiente em que se encontram os computadores e periféricos. Exemplo: ausência de gerador de energia, normas para senhas, entre outros.

- **Humanas:** esta categoria envolve o fator humano, considerada a mais difícil de avaliar, por envolver características psicológicas, emocionais, socioculturais, que variam de pessoa para pessoa. Exemplos: falta de treinamento, qualificação, ambiente organizacional inapropriado para desenvolvimento das atividades etc.

Atualmente, quase todas as empresas são informatizadas e possuem um sistema que faz o seu gerenciamento, embora esses softwares auxiliem muito nas tarefas diárias e na tomada de decisão, infelizmente, apresentam muitas vulnerabilidades em relação aos sistemas manuais. Já imaginou a interrupção de energia elétrica por algumas horas, quantos transtornos poderão gerar aos negócios da empresa? Possivelmente, algum dano trará, porque muitos dos recursos de informação estão armazenados em uma base de dados que, por sua vez, só poderão ser acessadas caso haja energia elétrica. Empresas de grande porte, como bancos, companhias aéreas poderão ter

que arcar com prejuízos financeiros grandes, justamente pela indisponibilidade de seus dados.

2.1.4 Falhas

É quando um sistema permite a quebra de alguns dos princípios da segurança da informação. Essas falhas podem ser humanas ou não, intencionais ou não. Mas a maioria dos problemas de segurança da informação está basicamente relacionada às falhas oriundas das fases de implantação e desenvolvimento de uma política de segurança.

Nesse sentido, podemos citar algumas falhas bastante comuns que ocorrem em virtude dessas dificuldades, sendo elas: inexistência de uma política de segurança formalizada, gerenciamento dos acessos efetuados no sistema, backups atualizados, treinamentos e informativos aos usuários sobre como explorar com segurança os recursos tecnológicos e, não menos importante, a definição de uma gerência de Tecnologia da Informação – TI para implementar as regras e fazê-las vivas na empresa.

É sempre importante a empresa manter uma política de segurança bem implementada e usual para que, em um momento de necessidade, não sofra nenhum dano, evitando consequências desastrosas aos negócios.

Para melhor compreensão sobre os riscos da Segurança da Informação, leia a Cartilha de Segurança para Internet proposta pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – Cert.br. Disponível em: <http://cartilha.cert.br/golpes>

Leia sobre ataques promovidos por hackers ocorridos aqui no Brasil. Texto escrito por Sandro Lima, com título "Hackers continuam a atacar *sites* do governo". Disponível em: <http://g1.globo.com/politica/noticia/2011/06/hackers-continuam-atacar-sites-do-governo-diz-serpro.html.>

Leia também este artigo que mostra um caso de falhas em segurança da informação. O artigo escrito por Ana Paulo Lobo, intitulado TCU, detecta falhas no ERP e na segurança da informação dos Correios. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31263&sid=11.>

Resumo

Nesta aula, apresentamos alguns problemas de segurança da informação, que surgem em decorrência da má operação do sistema assim como de ataques. Mostramos como acontecem as ameaças, quando estamos em risco ou vulneráveis e também as falhas. Tratamos também da importância da segurança dos ativos pessoais e empresariais ocasionados por algum incidente de segurança.

Atividades de aprendizagem

1. O que você entende por ativo de uma empresa? Explique.

2. Os incidentes em uma empresa ocorrem quando uma e/ou várias ameaças exploram os pontos fracos da mesma, seja intencionalmente ou não. Cite quais os princípios da segurança da informação foram violados.

3. Quando um ativo da informação sofre um ataque potencial podemos entender como ameaça. Esse ataque poderá ser efetuado por agentes externos ou internos diante das vulnerabilidades apresentadas no sistema da

empresa. Como as ameaças podem ocorrer?

4. Cite alguns riscos aos quais as pessoas estão sujeitas ao utilizar a Internet.

5. Leia as afirmações e assinale a alternativa correta.

a) Quando os princípios da segurança da informação são violados e há interrupção dos processos normais de negócio, denomina-se Incidente.

b) Ativo é conhecido como tudo que tem valor para a organização e, uma vez violados, não trarão impactos relevantes para a empresa.

c) As falhas podem ser apenas humanas e causadas de forma intencional.

d) Quando as atividades são interrompidas na empresa em decorrência de um furacão, essa interrupção é entendida como risco.

7. Explique a importância de um Plano de Recuperação de Desastre para as empresas.

Prezado(a) estudante,

Antes de passarmos para a próxima aula, é importante que você verifique se assimilou os pontos principais do conteúdo como, incidente, ativo e os problemas de segurança da informação. Todos esses aspectos apresentados são importantes para que você consiga identificar as causas de um incidente de segurança.

Não deixe de realizar as atividades de aprendizagem. Elas são ferramentas importantes para você avaliar seu desempenho, caso encontre dificuldades em responder as questões; procure revisar os conteúdos estudados para sanar dúvidas. Este é o momento ideal para você fazer uma revisão daquilo que já foi apresentado. Na próxima aula, abordaremos os mecanismos e tecnologias de segurança. Vamos lá!

Aula 3. Mecanismos e tecnologias de segurança

Objetivos:

- reconhecer a importância da implementação de controles para o pessoal, para infraestrutura e equipamentos;
- Identificar mecanismos de reconhecimento, autenticação e gerenciamento de permissões e restrições de usuários para acessar o sistema; e
- reconhecer a importância da auditoria de acesso as informações.

Caro(a) estudante,

Nesta aula, vamos fazer uma viagem pelos mecanismos de segurança. A falta de segurança em uma empresa pode estar relacionada tanto às tarefas que os funcionários realizam, como ao processo de contratação de novos colaboradores, como aos treinamentos que a empresa realiza e até mesmo aos recursos tecnológicos e às instalações físicas. Os controles de acesso lógico também serão abordados nesta aula e, para finalizar, citaremos outros mecanismos de segurança que visam à redução de vulnerabilidades, tais como programas antivírus, backup, firewall, uso de protocolos seguros, assinatura digital, entre tantos outros que objetivam reduzir as vulnerabilidades existentes em um sistema computacional. Esperamos que seja mais um encontro que contribua para a sua formação profissional.

3.1 Controles de pessoal

A questão da segurança das informações em computadores praticamente é inexistente, pois é uma preocupação diária, minuto a minuto, daí a importância da prevenção de riscos, de forma que venha mitigar ao máximo as vulnerabilidades. Segurança 100% só existe se deixarmos os computadores desligados e desconectados, mas infelizmente, ele perderia sua utilidade.

Por isso, é importante o funcionário conhecer seus deveres na empresa; um cuidado que o departamento de Recursos Humanos deve ter é em relação à contratação de um novo servidor, constatando os documentos e referências apresentados, propor treinamento adequado aos funcionários, deixando claras as diretrizes de segurança da empresa.

3.2 Controles físicos

Muitos acreditam que, quando nos referimos à segurança da informação devemos aplicar normas de segurança somente para quem faz uso do computador, da internet e dos programas que estão instalados, não é mesmo? Mero engano, os procedimentos de segurança devem ser tratados em todos os níveis, sejam físicos, lógicos ou pessoais.

Para assegurar os ativos da informação físicos, são necessários cuidados para prevenir, detectar e solucionar problemas, caso ocorra algum incidente de segurança.

Dessa forma, a proteção física são barreiras que servem para restringir o acesso direto à informação ou infraestrutura, de forma que a garantir a existência da informação.

A Norma ISO/IEC 17799 define perímetro de segurança como sendo: "Alguma coisa que constitui uma barreira, tal como uma parede, um portão de entrada controlado por cartão ou um balcão de recepção com atendentes".

Há alguns controles que merecem cuidados especiais, tais como: identificar quem entra nas dependências da empresa, os trabalhadores da segurança também devem suas regras de trabalho, os locais de carga e descarga também merecem vigilância, para saber quem entrou e como entrou na empresa.

Todos esses aspectos devem ser tratados individualmente e com muita cautela porque muitos crimes ocorrem em virtude da falta de segurança nas dependências da empresa.

3.3 Segurança de equipamentos

Você pode perceber que todos os ativos da empresa merecem cuidados especiais, cada um com suas exigências e restrições de acesso.

Os equipamentos devem ser mais uma preocupação para quem define as diretrizes de segurança de uma empresa, considerando não somente a localização e disposição física, mas também protegendo contra acessos não autorizados, a salvaguarda e descartes de arquivos, manutenção e aquisição de novos equipamentos, falhas de energia, além do cabeamento e toda infraestrutura utilizada.

3.4 Controles de acesso lógicos

Problemas de ordem lógica em uma empresa não se resumem apenas a acessos indevidos, podem ocorrer falhas em algum programa que a empresa utiliza para realizar suas atividades diárias, podendo ficar indisponível para a realização das operações por algumas horas ou mesmo até dias.

Esses problemas geralmente estão relacionados a erros que o próprio programa contém, não garantindo a integridade da base de dados e podem ocorrer também quando o computador está infectado com algum tipo de vírus de computador ou outra forma de ataque.

Os controles nada mais são que barreiras que tentam restringir ou limitar o acesso de pessoas não autorizadas ao sistema da empresa.

Alguns recursos que devem ser protegidos pelo controle de acesso lógico são: os arquivos-fontes, sistemas operacionais e os aplicativos instalados na máquina, sendo definidos pela ISO/IEC 17799.

3.5 Outros mecanismos de segurança

Novas tecnologias são criadas quase que diariamente com o intuito de tentar solucionar os problemas existentes da segurança da informação.

Procuraremos aqui apenas citar alguns mecanismos de segurança aplicados no mercado, mas sem direcionar para uma tecnologia específica, que veremos mais adiante.

3.5.1 Identificação de usuários

A identificação do usuário no sistema pode ocorrer diretamente no provedor de serviços. Neste caso, o usuário terá uma identidade para cada serviço, conhecida como modelo tradicional. O modelo centralizado é o que libera o acesso ao sistema ao usuário uma única vez no servidor que, a partir daí po-

derá utilizar os seus privilégios por tempo determinado. Já o modelo federado permite o acesso dos usuários pela autenticação única, ou seja, uma vez cadastrado em um servidor, o cliente poderá ter sua identidade distribuída a outros servidores, não existindo nenhuma legislação que proíba tal ação e, por fim, o modelo centrado no usuário, no qual quem gerencia a identidade do usuário é o próprio usuário, permitindo ou restringindo determinada informação a um servidor. Essas são as formas de identificação do usuário em um servidor.

3.5.2 Autorização e controle de acesso

Os controles de acesso e autorização geralmente inspecionam o que o usuário vai fazer, desde que devidamente autorizado.

Os mecanismos mais utilizados são os de autenticação, os mais conhecidos são os logins e senhas, não tão seguros, mas atualmente, em mecanismos de autenticação foram criados alguns equipamentos para dar suporte a esse processo, por exemplo, na biometria, nos certificados digitais; vale ressaltar que esses mecanismos são utilizados dentro do ambiente empresa.

Já os mecanismos utilizados para acessar o sistema fora da empresa contam com os firewall, justamente por garantir a proteção de quem acessa tanto de fora como de dentro da empresa.

3.5.3 Programas antivírus

Uma maneira eficaz de se proteger os dados dentro da empresa é justamente utilizar programas antivírus, pois muitos identificam e deletam não somente arquivos infectados no disco, mas também enviados por e-mail e outros meios lógicos que a empresa utiliza para guardar seus dados, dessa forma, esses aplicativos asseguram a integridade dessas informações

Os antivírus, atualmente, utilizam os dois métodos para identificar infecções, sendo denominados híbridos, além de sua atualização diária, pois todos os dias são criados novos vírus.

É importante que o usuário seja devidamente treinado para prevenir e reconhecer possíveis ataques, não bastando apenas a instalação dessas ferramentas de segurança.

3.5.4 Proteção de dados em curso na internet

A tecnologia utilizada para proteger dados que estão trafegando na Internet é a criptografia, cujos dados são codificados, de forma que fiquem totalmente descaracterizados, evitando a sua leitura caso seja interceptado.

3.5.5 Detecção de intrusos

A detecção de intrusos tem por função analisar os acessos efetuados na rede, observando as inúmeras linhas de logs e diagnosticando em tempo real possíveis ataques.

Nesse sentido, os administradores da rede de computadores sabem sobre as invasões que estão ocorrendo ou mesmo as tentativas de invasão ao sistema de computadores, sendo capazes também de identificar possíveis ataques feitos internamente, ou seja, ocorridos na própria empresa, pois essas invasões o firewall não detecta.

3.5.6 Sistema de *backup*

O sistema de backup refere-se à criação de cópias de segurança das informações importantes para os negócios que estão gravados nos servidores e computadores dos usuários.

Para realização do backup, é necessário instalação de ferramentas específicas para essa tarefa, além disso, é importantíssimo ter certeza de que as cópias agendadas tenham sido realizadas corretamente e que as informações estejam íntegras.

O backup deve ser feito periodicamente (diário, semanal, quinzenal, mensal) de forma que, se algum incidente de segurança ocorrer, as informações possam ser recuperadas sem nenhum dano imediatamente.

3.5.7 *Firewall*

É uma junção de hardware e software aplicados em uma política de segurança que gerencia o tráfego de pacotes entre a rede local e a Internet em tempo real. Não vamos nos estender muito sobre esse assunto, porque o mesmo será abordado mais adiante.

3.5.8 Atualização de sistemas operacionais e aplicativos

Atualizar o sistema operacional e os aplicativos da máquina minimizam os riscos e vulnerabilidades, pois os mesmos possuem atualizações que corri-

gem falhas apresentadas nesses aplicativos depois de comercializados. Caso seu aplicativo não seja original ou mesmo de uso livre, você pode estar correndo sérios riscos.

3.5.9 *Honeypot*

É um software que tem por função impedir ou mesmo identificar a ação de um invasor, ou qualquer ação estranha ao sistema. Esse sistema faz o invasor acreditar que realmente está invadindo as vulnerabilidades do sistema.

3.5.10 Sistemas de autenticação

Esta tecnologia faz uso da combinação de logins e senhas, que de certa forma, atualmente, não apresenta tanta dificuldade para descobrir.

Sendo assim, foram integradas a esse sistema de autenticação, soluções melhor elaboradas, dificultando a quebra.

Nesse sentido, instrumentos físicos – hardware – dão suporte a esse mecanismo de segurança. Como exemplos, temos: os recursos da certificação digital, palavras-chaves, cartões inteligentes e os recursos da biometria.

A biometria é uma técnica que utiliza características biológicas como recurso de identificação, como a digital de um dedo ou mesmo da mão, ler a íris, reconhecer a voz, e as próprias empresas já estão se organizando para essa mudança tecnológica. Um exemplo mais próximo foi o que aconteceu nas últimas eleições, cujo recadastramento foi obrigatório em algumas cidades brasileiras para justamente fazer uso nas eleições, agilizando não somente a votação, mas também, a apuração.

Esses mecanismos têm por função gerenciar as permissões que o usuário tem no sistema.

Quanto aos mecanismos de controle efetuados para gerenciar acessos externos, pode ser adquirido pelo uso de um firewall, que é uma barreira lógica na entrada da empresa, impedindo ou permitindo acessos.

3.5.11 Protocolos seguros

É um método que faz uso de protocolos que realmente garantem certo grau de segurança. Atualmente, há inúmeras ferramentas e sistemas disponíveis que têm por objetivo o fornecimento de segurança às redes de computadores. Podemos citar como exemplo os próprios softwares antivírus, os fi-

rewalls, identificadores de intrusos, programas para filtrar spam.

3.5.12 Assinatura digital

Este processo garante que a mensagem realmente veio do remetente, confirmando sua autenticidade, este método utiliza técnicas de criptografia, dessa maneira, garante também a integridade e o não repúdio, que tem como característica provar quem foi o emissor da mensagem.

Basicamente, seu mecanismo gera um resumo criptografado da mensagem utilizando algoritmos complexos, minimizando a mensagem em tamanhos menores, que é denominado hashing ou checagem.

3.5.13 Auditoria de acesso às informações

A auditoria de acesso às informações é um recurso de controle bastante usado, principalmente nas empresas que trabalham com transações financeiras diariamente; pode perfeitamente ser aplicada nos recursos computacionais.

Esse mecanismo de segurança é importante por possibilitar visualizar as atividades efetuadas no computador, assim como identificar quem executou a ação a partir da ID de usuário, além da possibilidade de poder observar o conteúdo que foi tratado nos computadores.

Tem por função, basicamente, registrar todos os acessos efetuadas nas redes de computadores, possibilitando identificar o usuário que acessou a máquina, assim como os recursos utilizados e, caso tenha acessado a internet, é possível saber quais páginas e conteúdos foram acessados, se foram feitos downloads de arquivos.

Esse mecanismo de segurança auxilia na tomada de decisão para uma reformulação da política de segurança, caso a empresa já tenha, ou mesmo dar subsídios na criação de uma política de segurança eficiente.

Atualmente, fala-se muito em computação em nuvem, segundo especialistas, essa tecnologia terá crescimento relevante até 2015 no país.
Saiba mais sobre essa questão, acessando o *site* <**http://www.istoedinheiro.com.br/noticias/105604_COMPUTACAO+EM+NUVEM+CRESCE+NO+BRASIL+MAS+REQUER+CUIDADOS**>

Resumo

Acabamos de estudar algumas das principais maneiras de proteger os ativos de uma empresa, desde cuidados que devemos ter com as pessoas até infraestrutura e equipamentos. Além desses controles, mostramos também as funções de um programa antivírus, firewall, honeypot, assim como, a importância de se fazer backups periodicamente.
Tais informações poderão auxiliá-lo na compreensão das principais ferramentas de segurança da informação e na reflexão sobre o papel da segurança

das informações em uma organização.

Atividades de aprendizagem

1. Que cuidados as empresas devem ter ao contratar um novo funcionário?

2. O que você entende por problemas de acesso lógico?

3. Cite alguns cuidados que o setor de Tecnologia da Informação deve tomar para fazer o reconhecimento e autenticação do usuário no sistema.

4. Por que fazer o controle dos funcionários que gerenciam os privilégios os usuários? Explique.

5. Cite duas tecnologias de identificação e autenticação de usuários.

6. Relacione os termos da primeira coluna de acordo com as definições da segunda coluna:

(A) Assinatura Digital	( )	Aplicativos que identificam e deletam arquivos infectados no disco, arquivos anexos a e-mail e outros meios lógicos que a empresa utiliza para guardar seus dados, dessa forma, esses aplicativos asseguram a integridade dessas informações.
(B) Programas Antivírus	( )	Tem por função analisar os acessos efetuados na rede, observando as inúmeras linhas de *logs* e diagnosticando em tempo real possíveis ataques.
(C) *Honeypot*	( )	Cria cópias de segurança das informações importantes para os negócios que estão gravadas nos servidores e computadores dos usuários.
(D) *Backup*	( )	Processo que garante que a mensagem realmente veio do remetente, confirmando sua autenticidade.
(E) Detecção de Intrusos	( )	Aplicativo que tem por função impedir ou mesmo identificar a ação de um invasor, ou qualquer ação estranha ao sistema.
(F) *Firewall*	( )	Gerencia o tráfego de pacotes entre a rede local e a Internet em tempo real.

Caro(a) estudante,

Com esta aula, esperamos que você tenha compreendido os mecanismos de segurança da informação como de fundamental importância para os negócios. Antes de prosseguirmos, faça uma revisão, caso encontre dificuldades, procure rever novamente o conteúdo para sanar suas dúvidas. Lembre-se que, na educação a distância, a construção do conhecimento ocorre de forma cooperativa e colaborativa; você poderá fazer uso dos recursos tecnológicos proporcionados ao seu curso para compartilhar com colegas suas descobertas.

Aula 4. Conceitos de segurança em rede: criptografia, assinatura e certificado digital

Objetivos:

- reconhecer a criptografia como recurso de segurança;
- identificar as fases da criptografia;
- distinguir as classificações da criptografia;
- reconhecer a assinatura digital como recurso tecnológico seguro; e
- identificar funções e modelos de certificado digital

Você, caro(a) estudante, sabe que a Internet é um dos maiores recursos tecnológicos que oferece grandes oportunidades de negócios e serviços e é, simplesmente, fantástico. As atividades realizadas vão desde compras, operações bancárias até serviços virtuais de informações, só que a segurança também deve ser eficiente, devido a dimensão de serviços ofertados, que envolvem dados pessoais, profissionais e financeiros, sendo estes motivo de preocupação.

Diante dessa nova realidade, controlar acessos a partir de senhas já não é tão seguro, justificando a criação de novas tecnologias e aperfeiçoamento de outras. Sendo assim, a proposta dessa aula é abordar sobre segurança em rede, como a criptografia, assinatura digital e certificado digital. Todos esses métodos de segurança são considerados atualmente os mais eficazes. Vamos então, para mais uma aventura, objetivando compreender as funções desses métodos seguros de rede.

4.1 Criptografia, fases e classificação

A criptografia é um mecanismo de segurança mais eficaz atualmente, podendo ser entendido como a modificação de uma informação em outra,

deixando-a ilegível para pessoas não autorizadas, para obter essas transformações na mensagem, faz-se uso de algoritmos predefinidos e uma chave secreta, que codifica a mensagem em outra e depois é decodificada quando chega ao seu destino com a chave secreta, dessa maneira, procurar-se-á garantir a privacidade e a integridade, impossibilitando que terceiros possam ler a mensagem original ou mesmo alterá-la.

4.1.1 Fases da criptografia

A criptografia, segundo Marçula & Benini Filho (2007), ocorre em fases, iniciando sua transformação antes da transmissão ao destinatário, recebendo uma chave para ser descaracterizada; na segunda fase, a mensagem é transmitida, caso seja interceptada não poderá ser decodificada, pois só será possível com a chave de criptografia e, por fim, na terceira fase, a mensagem já está no seu destino e para ler basta utilizar a chave da codificação. Vejamos o exemplo a seguir:

O remetente deseja enviar a seguinte mensagem: BLADE RUNNER

Primeiramente, será atribuído para cada letra um valor correspondente, sendo 00 para espaço, 01 para a letra A, 02 para a letra B e assim, sucessivamente, para todas as letras. Dessa forma, tem-se:

B	L	A	D	E		R	U	N	N	E	R
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
02	12	01	04	05	00	18	21	14	14	05	18

Os valores são agrupados em conjunto de cinco letras e o final deve ser preenchido com espaços em branco:

02	12	01	04	05		00	18	21	14	14		05	18	00	00	00

Utilizar como chave também um conjunto de cinco números, que deverão ser somados a cada conjunto correspondente da mensagem que deve ser codificada. No exemplo, a chave é 10 08 04 11 02 e o resultado será:

02	12	01	04	05		00	18	21	14	14		05	18	00	00	00	
					+						+						+
10	08	04	11	02		10	08	04	11	02		10	08	04	11	02	
12	20	05	15	07		10	26	25	25	16		15	26	04	11	02	

Com esse conjunto de valores obtidos a partir da soma, utiliza-se novamente a correspondência entre valores e letras. O resultado será:

12	20	05	15	07		10	26	25	25	16		15	26	04	11	02	
↓	↓	↓	↓	↓		↓	↓	↓	↓	↓		↓	↓	↓	↓	↓	
L	T	E	O	G		J	Z	Y	Y	P		O	Z	D	K	B	

A mensagem transmitida é **LTEOGJZYYPOZDKB**

Quando chegar ao destinatário que possui a mesma chave de criptografia utilizada para codificá-la, ele fará o mesmo processo mostrado anteriormente, com a diferença que, ao invés de somar os valores da chave, subtrairá os valores, restituindo a mensagem original.

4.1.2 Classificação da criptografia

Existem dois tipos de chaves para transmitir as mensagens, sendo chamadas de Simétrica e Assimétrica.

A **Criptografia Simétrica** denominada Chave Secreta, para Marçula & Benini Filho (2007, pag.363), é definida como "única e conhecida somente pelo remetente e pelo destinatário das mensagens".

Há alguns algoritmos dessa modalidade de criptografia usados, tais como: Blowfish, RC4, RC5, IDEA, RC6, DES – chave de 40 a 56 bits, 3DES (TRIPLE DES) – 168 bits, e o mais recente AES - chave de 256 bits, todos esses algoritmos já são reconhecidos por normas do IEEE – Instituto de Engenharia Elétrica e Eletrônica e pelo Departamento de Segurança Nacional Americano. Muitos programas podem utilizar esses recursos de criptografia.

A **Criptografia Assimétrica** ou chave pública, segundo Lyra (2008, pag. 37), "é um método que possui duas chaves, a chave pública que fica disponível para todos que queiram enviar mensagens e a chave privada, de exclusividade da pessoa que queira codificar e decodificar mensagens por ele recebidas".

É importante citar que existem outros métodos de criptografia, tais como: ECC (Curvas Elípticas), Diffie-Hellman, DAS, El Gamal e o RSA (**R**onald Rivest, Adi **S**hamir e Leonard **A**dleman, são os fundadores do algoritmo) um dos mais utilizados, esse método baseia-se na fatoração de números primos, utiliza chaves de 256, 512, 1024 e 2048 bits. O Departamento de Defesa

dos Estados Unidos não liberou o uso de chaves com 2048 bits, somente eles têm autorização.

Atividades de aprendizagem:

Para as três primeiras questões, vamos tentar pôr em prática o método de criptografia proposto por Marçula e Benini Filho. Para a solução dos problemas propostos, você deverá utilizar a tabela a seguir para codificar e decodificar as mensagens.

A	B	C	D	E	F	G	H	I	J
01	02	03	04	05	06	07	08	09	10
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
11	12	13	14	15	16	17	18	19	20
U	**V**	**W**	**X**	**Y**	**Z**	**Espaço em Branco**			
21	22	23	24	25	26	00			

1. De férias nos Emirados Árabes, a conselheira Trace recebe uma caixa de seu chocolate Cretariano favorito, juntamente com uma mensagem criptografada do remetente revelando sua identidade. Usando o exemplo de criptografia citado por Marçula & Benini Filho, decodifique a mensagem MPHKCESEVGUGSRKVVECB, cuja chave é: 00 07 05 03 02. Decodifique para saber o nome do remetente.

2. Em seu primeiro contato com um planeta Zomour com que a Retamatemil deseja estabelecer relações diplomáticas, os oficiais da UCorporation foram convidados para um banquete. Infelizmente, há um grupo dissidente no plano Zomour que deseja apoiar os Crodapon e não a Retamatemil. Um espião desta facção é instruído a envenenar um dos oficiais da UCorporation. O traidor é descoberto, mas foge a tempo. Em seu alojamento é encontrada a mensagem codificada KWUXWVVCKN que contém o nome do oficial envenenado e um pedaço de papel com o números 0822031114 usados na codificação. Como o veneno é seu próprio antídoto é preciso saber exatamente quem foi envenenado. Trabalhando contra o tempo, um especialista em segurança verificou que se tratava de um código muito simples, o código proposto por Marçula & Benini Filho. Qual o nome do Oficial envenenado?

3. Você faz parte de uma equipe de segurança de seu país, o Janbolala, e precisa enviar a mensagem ao seu espião secreto que se encontra no país vizinho, o Kongololo. Mas, para isso, a mensagem precisa ser codificada. Usando o método de Marçula e Benini Filho, codifique a mensagem:

Abortar operação. A Chave a ser utilizada para codificar é: 00 07 05 03 01

4.2 Assinatura digital

Assinar documentos é algo muito natural para as pessoas, mesmo aquelas analfabetas, para estes casos, basta a impressão digital de um de seus dedos e pronto, o documento já está assinado.

Agora, já pensou se você tiver que enviar algum documento para um lugar distante, um relatório, por exemplo? Há um tempo fazíamos uso dos correios, o Sedex era uma boa alternativa, só que nesse mundo em que vivemos tudo ocorre de forma muito rápida e aí é que entram as tecnologias e, nesse caso, a assinatura digital. Pois certamente você terá que assinar o relatório para comprovar sua autenticidade. E como é feita essa assinatura digitalmente? Você já parou para pensar nisso?

Para assinar digitalmente um documento, é necessário que o documento primeiramente esteja já digitalizado e esteja de posse da chave pública de quem vai receber o documento, podendo ser pessoa física ou jurídica.

Em seguida, a partir de um programa específico, o documento será criptografado de acordo com a chave pública que você tem para poder enviar o documento, gerando um resumo do mesmo tamanho que será criptografado, denominado hash, garantindo autenticidade e o não repúdio.

Quando a mensagem chegar ao destinatário, o receptor deverá utilizar sua chave privada para decodificar/decriptografar o documento, gerando um novo resumo a partir da mensagem que está armazenada, para em seguida, comparar com a assinatura digital.

Caso o documento tenha sido alterado, a chave privada não vai conseguir decodificar o arquivo, pois consequentemente a assinatura é corrompida, não reconhecendo o documento. Ou seja, se o hash original for igual ao hash gerado na recepção do documento, a mensagem está íntegra.

A função hashing avalia completamente o documento baseado num algoritmo matemático que calcula um valor, tendo como parâmetro os caracteres do documento, obtendo um valor de tamanho fixo para o arquivo, conhecido como valor hash.

Com uso complexo de um algoritmo matemático, é muito difícil desvendar a chave privada através da chave pública, garantindo a segurança e a credibilidade desse processo.

Atividades de aprendizagem

4. Explique como funciona a assinatura digital.

5. O que é hash?

4.3 Certificado digital

Para obtenção de uma assinatura digital, é necessária uma Autoridade Certificadora (AC) que faça esse serviço, tendo como função averiguar a identidade de um usuário e agregar a ele uma chave. Esse conjunto de informações é introduzido em um documento denominado certificado digital. É importante citar que o certificado digital funciona independentemente da assinatura digital.

O certificado digital tem por função atestar a integridade dos negócios, garantindo a legitimidade da operação realizada na Internet, funciona como se fosse um documento usado na Internet para assegurar sua identidade.

No site, o certificado é definido como "documento eletrônico que garante proteção às transações online e a troca virtual de documentos, mensagens e dados, com validade jurídica". Disponível em: <, http://serasa.certificadodigital.com.br/o-que-e/> Acesso em: 12 ag. 2013

Essa tecnologia é composta por um conjunto de informações referentes à entidade para a qual o certificado foi emitido, baseando-se na criptografia de chave pública, garantindo assim outros aspectos da segurança da informação como: autenticação e o não repúdio.

Algumas informações são introduzidas no Certificado Digital para que seja feita a autenticação do remetente, conforme consta no site da SERPRO, tais como:

1-Nome, End. e Empresa do solicitante

2-Chave pública do solicitante

3-Validade do certificado

4-Nome e End. da Autoridade Certificadora (CA)

5-Política de utilização (limites de transação, etc.)

Disponível em: < www.serpro.gov.br/conteúdo-solucoes/serviços/portlet--certificacao-digital> Acesso em:12 ag.2013

4.3.1 Funcionamento do certificado digital

Na identificação digital, é utilizada a técnica de criptografia assimétrica que dispõe de duas chaves relacionadas, uma chave pública e outra privada.

Tanto um nome de usuário como outras informações que identificam o usuário são vinculadas a um par de chaves, e isso funciona como um credenciamento eletrônico que, quando instalado em um navegador da Web, permitem a autenticação.

Em uma única mensagem, podemos anexar várias identificações digitais, formando "uma cadeia de certificados digitais em que cada identificação digital confirma a autenticidade da anterior e essa identificação digital é assinada pela Autoridade Certificadora que a emitiu" (SERPRO).

4.3.2 Modelos de certificado digital

Há necessidade de uma infraestrutura para validar o certificado para as demais entidades. Apresentamos a seguir três modelos:

Modelo Web Oftrust (malha de confiança)

Nesse modelo, seu funcionamento baseia-se na confiança, que é controlada pelos usuários, ou seja, quando um usuário obtém a chave pública de outro usuário poderá verificar a autenticidade da chave recebida por intermédio das outras entidades, sendo então implantada uma rede em que as entidades pertencentes confiem umas nas outras.

Uma das vantagens nesse modelo é que, caso ocorra o comprometimento da chave de uma entidade que autentica o certificado, ela simplesmente será excluída dessa rede, não interferindo nas demais chaves.

E uma desvantagem é que é um modelo menos seguro, porque uma pessoa pode perfeitamente tirar proveito da confiança dos outros usuários.

Modelo Hierárquico

É definido dessa forma por tratar de uma hierarquia de autoridades certificadoras, em que as AC´s certificam os usuários e a autoridade certificadora raiz AC-R faz a certificação de todas as AC´s de sua competência.

Nesse modelo, para ser validado um certificado digital, é necessária a assinatura digital de uma AC. Caso haja dúvidas da sua validade, é necessário consultar na AC se não foi eliminado o certificado usado para a criação de infraestrutura de chaves públicas.

A AC-R, por ser mantida por uma entidade governamental, mostra-se mais segura, possibilitando que a assinatura digital seja juridicamente válida, desde que garantida toda segurança das AC´s e da infraestrutura da AC-R.

Apresenta-se como desvantagem desse modelo o custo de montagem da infraestrutura que é bem superior, em virtude dos procedimentos de segurança aplicado, por exemplo, instalação de sala-cofre; outro fator que é considerado desvantajoso é que, se a chave de uma AC for corrompida, compromete a validade de todos os certificados emitidos por ela.

Modelo de Autoridade Central

Em relação aos dois modelos anteriormente citados, este é o padrão mais usual para certificado digital, quando envolve infraestrutura de chave pública, definido como ITU-T X.509 que sofreu mudanças para ser utilizado na Internet, passando a ser conhecido como PKIX.

É absoluta sua autoridade certificadora, e é assim definido por ser organizado em uma estrutura de diretórios em árvore, cujo certificado digital não pode conter a chave privada do usuário, a mesma é armazenada em tokens ou smart cards.

O padrão X.509, encontra-se na versão 3, padronizando os modelos de chaves públicas e atributos para os certificados, algoritmos para procura do caminho de validação e listas de cancelamento de certificados.

Atividades de aprendizagem

6. De que é composto o certificado digital?

7. Explique o funcionamento do certificado digital.

8. Cite os modelos de certificado digital.

Resumo

Nesta aula, tratamos de conceitos de segurança em rede, iniciando com a criptografia, suas fases e sua classificação; neste tópico, é importante que você compreenda o processo de codificação e decodificação de uma mensagem, dessa forma poderá entender seu funcionamento. Outro assunto abordado foi assinatura digital, mecanismo de segurança muito útil e bastante utilizado, vimos também como é composto um certificado digital, o seu funcionamento e os seus modelos. Acreditamos que esta aula oportunizou ampliar e diversificar os conceitos de segurança em redes de computadores.

Atividades de aprendizagem

9. Relacione os termos da primeira coluna de acordo com as definições da segunda coluna:

(A) Modelo Hierárquico	( )	Seu funcionamento baseia-se na confiança, que é controlada pelos usuários, ou seja, quando um usuário obtém a chave pública de outro usuário, poderá verificar sua autenticidade da chave recebida por intermédio das outras entidades, sendo então implantada uma rede em que as entidades pertencentes confiem umas nas outras.
(B) Modelo de Autoridade Central	( )	Trata de uma hierarquia de autoridades certificadoras, na qual as AC´s certificam os usuários e a autoridade certificadora raiz AC-R faz a certificação de todas as AC´s de sua competência. Nesse modelo, para ser validado um certificado digital, é necessária a assinatura digital de uma AC.

(C) Modelo Web Oftrust	( )	Envolve infraestrutura de chave pública, definido como ITU-T X.509. É absoluta sua autoridade certificadora, e é assim definido por ser organizado em uma estrutura de diretórios em árvore, cujo certificado digital não pode conter a chave privada do usuário, a mesma é armazenada em tokens ou smart cards.

10. Como é classificada a criptografia? E qual a diferença entre elas?

Prezado(a) estudante,

Concluída essa etapa de nossa caminhada, nosso próximo desafio é entender as funções de uma autoridade certificadora, como é feito o processo de autenticação, e quais as funcionalidades de um firewall. Esses mecanismos de segurança vêm complementar esta aula, de forma que você possa agregar mais conhecimento tecnológico em sua formação profissional, e que futuramente auxilie nas atividades profissionais. Caso você tenha dúvidas em relação a algum assunto abordado, é importante que reveja o que já foi apresentado para poder prosseguir com mais segurança.

Aula 5. Conceitos de segurança em rede: Autoridade Certificadora – AC, autenticação e firewall

Objetivos:

- identificar as funções de uma Autoridade Certificadora;
- reconhecer como ocorre o processo de autenticação;
- identificar as funções do firewall;
- distinguir os tipos de firewall; e
- apontar a localização do firewall na rede de computadores

Prezado(a) estudante,

Você terá nesta aula, na verdade, mais um esclarecimento acerca da segurança em redes de computadores, com apresentação das instituições que emitem certificados digitais. Haverá também uma breve abordagem sobre como ocorre a autenticação desses certificados e, claro, trataremos sobre os firewall e suas categorias. Convido você a fazer a leitura do texto para posteriormente resolver as atividades propostas, dessa forma, poderá verificar suas dificuldades e necessidades. Prossiga então.

5.1 Autoridade Certificadora – AC

As autoridades Certificadoras – AC são instituições credenciadas para emitir certificados digitais, associando ao titular pares de chaves criptográficas, gerados sempre pelo titular, que terá acesso exclusivo a sua chave privada, sendo o titular responsável pelo controle, uso e conhecimento, conforme o site do SERPRO. Disponível em: < https://ccd.serpro.gov.br/egba/docs/perguntas.htm#0> Acesso em: 12 ag. 2013

A autoridade certificadora tem como funções a emissão, expedição, distribuição, revogação e gerenciamento dos certificados, assim como disponibili-

za uma lista de certificados revogados aos usuários, além de manter registro de todas as operações.

Para efetuar o cadastro ou identificação junto à autoridade certificadora – AC, pode-se dirigir a uma Autoridade de Registro – AR, que são vinculadas a uma determinada AC, que recebe esses dados cadastrais dos usuários e depois encaminha a solicitação de certificados às ACs, mantendo o registro de suas operações.

O certificado só será válido caso o emissor tenha a chave pública emitida pela AC, comprovando sua origem de emissão. Contudo, existem muitas ACs pelo mundo, inviabilizando a obtenção da chave pública de cada uma.

Para solucionar esse problema, foi criada então a Autoridade Certificadora Raiz (AC-R) da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, ou em inglês PKI (Public Key Infrastructure), assim definido pelo Instituto Nacional de Tecnologia da Informação – ITI. (Fonte SERPRO).

O ICP-Brasil tem por função controlar as ACs, ou seja, o certificado emitido só terá validade diante do governo brasileiro caso seja reconhecido por este órgão brasileiro.

Segundo o Instituto Nacional de Tecnologia da Informação –(ITI):

A Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos. Disponível em: <http://www.iti.gov.br/index.php/icp-brasil/o-que-e> Acesso em: 10 Maio 2013.)

Esses certificados podem ser emitidos pelas ACs para pessoas físicas (e-CPF), para pessoas jurídicas (e-CNPJ), equipamentos ou aplicações (e-SERVIDOR), conforme a necessidade.

Vamos citar algumas ACs do Brasil: Presidência da República, Receita Federal, SERPRO, Caixa Econômica Federal, Serasa, CertiSign, nelas você poderá solicitar seu Certificado Digital.

Atividades de aprendizagem

1. O que é uma autoridade certificadora?

2. Cite algumas funções da autoridade certificadora.

3. Cite pelo menos duas autoridades certificadoras do Brasil.

5.2 Autenticação

O processo de autenticação ocorre quando os usuários sabem que estão acessando as informações desejadas do servidor correto, que os dados enviados chegaram ao destino e não sofreram mudanças, assim como somente o receptor poderá ler as informações. Em contrapartida, o servidor precisa garantir que está se comunicando com o usuário certo e o conteúdo da mensagem e identidade do emissor estão corretos também.

Esse mecanismo pode ser realizado entre as partes envolvidas por meio de uma assinatura digital ou mesmo utilizando o certificado digital, devidamente reconhecido pela AC.

A autenticação faz uso da troca de mensagens entre as partes para existir a autenticação, restringindo o acesso via criptografia.

Acredito sinceramente que esses procedimentos digitais ainda demorarão um pouco para ser introduzidos totalmente no cotidiano das pessoas e empresas, considerando as dificuldades de acesso a internet em algumas regiões do país, seu custo, e claro, a cultura, pois ainda temos o costume de acreditar que um documento é verdadeiro quando vemos o carimbo. Mas observamos também que as empresas que já estão totalmente inseridas nesse processo informatizado, como bancos, grandes indústrias, já fazem uso dessa tecnologia por considerar a segurança de seus dados crucial para a sobrevivência dos negócios.

É sempre importante conhecer mais, por isso vamos indicar alguns *sites* nos quais você poderá obter informações acerca do assunto, por exemplo: métodos de certificação ou como obter um certificado.
Instituto Nacional de Tecnologia da Informação - ITI
http://www.iti.gov.br/certificacao-digital

Serviço Federal de Processamento de Dados – SERPRO
https://www.serpro.gov.br/conteudo-solucoes/servicos/portlet-certificacao-digital

Atividade de aprendizagem

4. Explique como ocorre o processo de autenticação.

5.3 *Firewall*

Esse é um grande recurso de segurança, pois tem a função de fazer análise da passagem de dados entre a rede privada e a rede externa em tempo real,

restringindo ou permitindo o tráfego de dados obedecendo regras preestabelecidas pela gerência de TI da organização.

O *firewall*, na realidade, é um obstáculo entre uma rede privada e uma rede externa, por exemplo, a Internet. Pode ser conhecido como um sistema por ser uma combinação de *hardware* e *software*.

Considerado, atualmente, pelos especialistas em segurança da informação, um dos recursos de proteção de redes corporativas importantes, pois além de controlar também monitora os acessos aos sistemas e aos computadores da organização, filtrando a passagem de dados entre duas redes.

O fato de ter instalado um sistema de firewall na organização não significa que a rede esteja protegida contra invasões, eles protegem apenas contra ataques externos, ficando inertes contra ataques que partem de dentro da própria empresa.

Para que o projeto tenha êxito, é importante fazer o levantamento do perfil da empresa no qual será aplicado esse mecanismo de proteção e, a partir daí, selecionar as funções que ele desempenhará na rede.

5.4 Tipos de *firewall*

Vejamos, agora, algumas categorias de firewall:

- **Filtro de pacotes (*Packet filtering*)**

Os filtros de pacotes inspecionam cada pacote a partir de seu endereço de origem e destino eliminando os que não estiverem de acordo com os parâmetros predefinidos ou permitindo o tráfego na rede. Essas decisões são definidas pelo *firewall* baseado no conteúdo que cada pacote contém.

- **Filtro de pacotes com base no estado da conexão (*Stateful Inspection*)**

Conhecida também como *Dynamic Packet Filtering*, executa sua função a partir do conteúdo da mensagem e dos dados contidos no cabeçalho do pacote, esses dois parâmetros, em conjunto com as regras definidas pelo administrador da rede, permitem ao *firewall* restringir ou dar passagem de um determinado pacote para a rede.

- **Filtro de pacotes na camada de aplicação (*Application Proxy*)**

São mais complexos que os demais filtros apresentados, pois fazem uso de códigos especiais para filtrar a ação desejada, além de registrar todo o conteúdo enviado ou recebido do tráfego.

Nesse sistema de Pacote na Camada de Aplicação, o *firewall* fica interposto entre um computador cliente e um servidor destino durante a comunicação.

5.5 Localização do *firewall*

Depois de selecionada a função do *firewall*, deve-se estabelecer o modelo do sistema, pois sua posição na rede deve obedecer a política de segurança.

Observe algumas topologias em ordem crescente de eficiência:

> ***Basic Border Firewall:*** é o ponto de partida de todos os sistemas de *firewall*. É um único computador interconectado à rede interna da empresa e a alguma rede não confiável em termos de segurança (normalmente a Internet).
>
> ***Untrustworth host*** (servidor não confiável): parecida com a topologia anterior, com o acréscimo de um servidor que está conectado a uma rede não confiável, na qual o *firewall* não pode protegê-lo. Esse servidor é configurado com o mínimo de segurança, desse modo, o *firewall* passa a controlar o tráfego de entrada e saída a partir desse servidor.
>
> ***DMZ Network:*** nesse modelo, o servidor não confiável é conectado ao *firewall*. Apesar disso, ele continua em sua própria rede, ou seja, o *firewall* conecta, agora, três redes diferentes. Isso aumenta a segurança, confiabilidade e disponibilidade apenas do servidor não confiável, e não de toda a rede à qual está conectado.
>
> ***Dual Firewall:*** a rede privada da empresa é ainda mais isolada da rede não confiável pelo acréscimo de mais um *firewall*.
>
> (MARÇULA & BENINI FILHO 2007, p. 368)

Em todos os modelos anteriormente citados, o *firewall* executa suas funcionalidades controlando os acessos no limite da rede, protegendo ao máximo

a rede privada de acessos não autorizados, podem também ser implementados em subredes, aumentando ainda mais a proteção no tráfego.

Atividades de aprendizagem

5. Por que o *Firewall* é importante em uma empresa?

6. Cite os tipos de *firewall*.

7. Quanto à localização do *firewall* em uma rede, cite o modelo mais eficiente, segundo Marçula & Benini Filho.

ALGUMAS APLICAÇÕES PARA FIREWALL

Consulte os *sites* abaixo para conhecer algumas soluções de software para firewall:

Zone Alarm
www.zonealarm.com
www.baixaki.com.br/download/zonealarm-free-firewall.htm

SonicWALL
www.innovision.com.br/

Coleção de softwares para Firewall
pcworld.uol.com.br/downloads/categoria/Segurança/.../Firewall/

NetDefender
netdefender.codeplex.com

Resumo

Nesta aula, mostramos que a evolução tecnológica nos impõe o constante aperfeiçoamento das técnicas de segurança da informação. Também foi abordado sobre a Autoridade Certificadora, instituição responsável pelo credenciamento de assinaturas digitais. Você pôde acompanhar como ocorre o processo de autenticação de uma assinatura digital e, por fim, o *firewall* que é uma barreira interposta entre a rede externa e interna, com suas devidas funcionalidades e categorias. Todos esses assuntos são relevantes quando se trata de assegurar dados, por serem tecnologias criadas para gerenciar acessos não autorizados.

Vamos praticar!

Atividades de aprendizagem

8. Com relação às topologias de Firewall, relacione a primeira coluna, que contém os tipos de *firewall* com a segunda coluna, contendo as definições de cada modelo.

A) Dual Firewall	( )	é o ponto de partida de todos os sistemas de firewall. É um único computador interconectado à rede interna da empresa e a alguma rede não confiável em termos de segurança (normalmente a Internet).
B) Basic Border Firewall	( )	nesse modelo, o servidor não confiável é conectado ao firewall. Apesar disso, ele continua em sua própria rede, ou seja, o firewall conecta, agora, três redes diferentes. Isso aumenta a segurança, confiabilidade e disponibilidade apenas do servidor não confiável, e não de toda a rede à qual está conectado.

C) DMZ Network	( )	a rede privada da empresa é ainda mais isolada da rede não confiável pelo acréscimo de mais um firewall.
D) Untrustworth host (servidor não confiável)	( )	parecida com a topologia anterior ,com o acréscimo de um servidor que está conectado a uma rede não confiável, na qual o firewall não pode protegê-lo. Esse servidor é configurado com o mínimo de segurança, desse modo o firewall passa a controlar o tráfego de entrada e saída a partir desse servidor.

9. Porque o firewall é importante em uma empresa? Explique.

Caro(a) estudante,

Nesta aula, procuramos focar nossos estudos na segurança de redes de computadores, mais especificamente sobre as Autoridades Certificadoras, desde conceitos até suas funções, além disso, abordamos um pouco do processo de autenticação e, por fim, recurso de segurança denominado Firewall, suas funções, classificação e posição em uma rede. Todos esses assuntos darão a você, estudante, embasamento teórico para prosseguimento de sua formação na área que escolheu para se qualificar. Além, é claro, de agregar a essa formação mais respaldo tecnológico, pois sabemos que os grandes profissionais se destacam dos outros também pelo seu conhecimento. Dando continuidade às aulas, trataremos agora da política de segurança da informação.

AULA 6. Controles de segurança da informação: política de segurança da informação

Objetivos:

- conceituar política de segurança da informação;
- distinguir as características de uma política de segurança da informação;
- identificar uma política de uso aceitável; e
- reconhecer plano de contingência e plano de recuperação de desastre.

Prezado(a) estudante,

Na intenção de proporcionar um avanço em seu processo de aprendizagem, apresentaremos nesta aula conceitos de política de segurança da informação, as características que uma política de segurança deve apresentar, especificaremos uma política de uso aceitável e, por fim, trataremos do plano de contingência e de recuperação de desastres. Todos esses cuidados são necessários e essenciais para que as informações estejam sempre garantidas para o bom andamento dos negócios, pois com a crescente disseminação e uso da informática, tanto nas organizações como na nossa vida pessoal há motivos para preocupações e cuidados.

6.1 Política de segurança da informação

Hoje, a informação é considerada um ativo valiosíssimo para as empresas, não importando o ramo de atividade que a mesma exerça, podendo ser comercial, industrial ou financeira, enfim, a informação na hora certa, poderá ajudar na expansão dos negócios, auxiliando na obtenção de maiores lucros, novas perspectivas de negócios e garantindo a sobrevivência dessas organizações.

A política de segurança da informação pode ser entendida como um conjunto de diretrizes, princípios e regras que irão dar suporte para criação e manutenção da segurança, obedecendo aos requisitos do negócio, às leis vigentes e aos regulamentos, pois:

> A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem. Disponível em: < http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf>. Acesso em: 18 jan. 2013.

Ainda segundo orientações do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – Cert.br, é importante fazer um levantamento da informação a ser protegida, a partir de uma análise de riscos que vai diagnosticar onde aplicar a proteção a partir das ameaças e vulnerabilidades.

Após a análise, a norma NBR ISO/IEC 17799, sugere a criação de um documento intitulado "documento da política de segurança da informação", sendo devidamente aprovado pela gerência, publicado e divulgado para todos os funcionários, considerando sua relevância para a organização, deve ser de fácil entendimento pelo público-alvo e acessível.

Neste documento, é importante deixar claros os objetivos, um texto da gerência endossando a importância e princípios da segurança da informação, apresentação de forma detalhada das exigências que deverão ser obedecidas, tais como: respeitar a legislação e contratos firmados no contrato de trabalho, apresentar as consequências e/ou punições que sofrerão caso sejam violadas as políticas de segurança, além disso, é importante também definir as responsabilidades gerais e específicas pela gestão da segurança das informações, juntamente com relatórios de incidentes.

Atividades de aprendizagem

1. O que deve conter a elaboração de uma política de segurança da informação?

2. Qual a importância de se implantar uma política de segurança da informação na empresa?

6.2 Criação de aplicações seguras: características de uma política de segurança

Para uma boa política de segurança, a mesma deve apresentar algumas características segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – Cert.br, consistindo na sua abrangência de atuação, nas normas e regulamentos aos quais estará subordinada, definir quem terá autoridade para sancionar, implementar e fiscalizar o cumprimento da política, estabelecer o período para sua revisão e adequação. Outra preocupação deve estar relacionada à política de senhas, devendo as permissões e restrições estarem de acordo com as atribuições de cada funcionário, além de especificar claramente os direitos e responsabilidades dos usuários, do provedor dos recursos e estabelecer ações caso a política de segurança seja violada.

É importante deixar claro que nem todas as sugestões mencionadas acima são utilizadas, devendo considerar as características de cada empresa, de forma que a política de segurança se adapte às particularidades de cada organização, então, fazer uma análise de riscos e definir a partir daí o que é realmente necessário para assegurar as informações de uma empresa.

Para que essa política de segurança funcione, é necessário que o gestor nomeie alguém para acompanhar sua implementação no ambiente e que periodicamente faça revisões. Isso se deve às constantes mudanças nos processos de negócio, bem como no lançamento de novas tecnologias, fatores que diretamente afetam os aspectos da segurança.

Segundo a NBR ISO/IEC 17799, o profissional responsável por gerir a política de segurança deve periodicamente verificar se a política implementada está em uso, analisar o impacto dos incidentes de segurança registrados, o custo e impacto dos controles na eficiência do negócio e os efeitos das mudanças na tecnologia. Dessa forma, ajudará a reduzir os riscos proeminentes do uso de tecnologias.

Para reforçar essa gerência:

> uma política de classificação de dados é fundamental para proteger as informações de uma organização e estabelecer as categorias responsáveis pela liberação das informações confidenciais.
>
> (MITINIK e SIMON 2003, p. 210)

Esses autores sugerem classicar as informações em:

- **confidencial** - as informações são compartilhadas com um número restrito de pessoas;
- **no modelo particular** - as que se destinam apenas ao uso na organização para fins burocráticos;
- **no modelo interno** - as informações são liberadas para os funcionários; e
- **pública** - cujas informações podem ser liberadas externamente.

Para o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – Cert.br, o sucesso de uma política de segurança se dá quando tem apoio da alta administração, caso contrário, ela rapidamente ficará obsoleta pelos outros setores da organização. Logo, o exemplo deve partir dos gestores para que os funcionários percebam que realmente está funcionando. Também podemos atribuir seu sucesso quando envolve todos os recursos tecnológicos e de informação, atualizada periodicamente, manter um grupo ou pessoa responsável em verificar se a política está sendo respeitada, além de estar disponível facilmente a todos os usuários das tecnologias e da informação.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – Cert.br, apresenta-nos alguns fatores que podem prejudicar a aceitação de uma política de segurança, por exemplo, a política de segurança não deve ser extensa, contendo muitos detalhes, pois dificultará seu entendimento e implementação, não abrir exceções a pessoas ou grupos, deve se dirigir aos programas e equipamentos específicos.

6.3 Política de uso aceitável (AUP – *acceptable use policy*)

É um documento que deve ser público e ficar à disposição dos que utilizam a infraestrutura computacional de uma organização, sendo acordada formalmente entre as partes como os recursos devem ser utilizados. Dessa forma, os usuários externos saberão que, para seu uso, devem obedecer as normas de segurança.

Atividades de aprendizagem

3. Apresente algumas características para a implantação de uma política de segurança da informação.

4. Explique qual deve ser a postura da alta administração em uma organização frente à política de segurança da informação.

6.4 Plano de contingência

Podemos entender como Plano de Contingência a definição das responsabilidades em uma organização em caso de emergência; dessa forma, objetiva uniformizar as ações necessárias para controlar ocorrências anormais.

Segundo o site do Ministério da Integração Nacional, o plano de contingência é um documento elaborado a partir de uma análise de risco de desastre, na qual estabelecem-se os procedimentos para agir caso necessário. Disponível em: < http://www.mi.gov.br/orientacoes-para-elaboracao-de-um-plano-de-contingencia> Acesso em: 09 set. 2013

Para uma boa implementação de um plano de contingência, independentemente do porte da empresa e complexidade dos processos, os gestores de negócios devem ser capazes de detectar os pontos primordiais, cujas atividades não podem sofrer paradas e, caso haja paralisações que resultem em perdas financeiras e/ou operacionais para a organização, o impacto seja reduzido.

Lyra (2008, p. 165) apresenta algumas estratégias de contingência:

Hot-site

Estratégia pronta para entrar em ação imediatamente. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto. Se a aplicássemos em um equipamen-

to tecnológico, um servidor de banco de dados, por exemplo, estaríamos falando de milissegundos de tolerância para garantir disponibilidade do serviço mantido pelo equipamento.

Warm-site

Aplicada em objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade.

Cold-site

Propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, desprovido de recursos de processamento de dados.

Realocação de operação

Visa desviar a atividade atingida pelo evento que provocou a quebra da segurança para outro ambiente físico, equipamento ou link, pertencentes à mesma empresa.

Bureau de serviços

Considera a possibilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado.

Acordo de reciprocidade

Muito conveniente para atividades que demandariam investimentos de contingência inviáveis ou incompatíveis com a importância da mesma, esta estratégia propõe a aproximação e um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes à sua, e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional.

Um bom plano de contingência é capaz de sustentar a missão da empresa, independentemente de quaisquer intempéries da natureza ou alguma recorrência em seu campo de atuação, fazendo parte inclusive do planejamento estratégico.

Atividades de aprendizagem

5. O que você entende por Plano de Contingência?

6. Relacione os termos da primeira coluna à segunda coluna que possui suas devidas definições.

A) Warm-site	( )	Visa desviar a atividade atingida pelo evento que provocou a quebra da segurança para outro ambiente físico, equipamento ou link, pertencentes à mesma empresa.
B) Acordo de reciprocidade	( )	Aplicada em objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade.
C) Realocação de operação	( )	Esta estratégia propõe a aproximação e um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes à sua, e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional.
D) Cold-site	( )	Estratégia pronta para entrar em ação imediatamente. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto.
E) Hot-site	( )	Propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, desprovido de recursos de processamento de dados.

6.5 Plano de recuperação de desastre

Podemos entender por Plano de Recuperação de Desastre um plano de ação para, no menor tempo, colocar os processos do negócio em funcionamento, depois de um desastre natural ou provocado pelo homem.

A criação de um Plano de Recuperação de Desastre se justifica pela necessidade de assegurar a continuidade dos negócios, para isso é importante reduzir os riscos, e eliminar o máximo possível as vulnerabilidades. Sabemos que é uma tarefa difícil, porque há situações que são bem difíceis de serem previstas.

Para se implementar um bom Plano de Recuperação de Desastres, é necessária uma análise sobre o impacto das perdas de dados e a interrupção do sistema da empresa, além da falta de comunicação entre funcionários, fornecedores e clientes. Além disso, devemos identificar quais eventos podem ocasionar possíveis desastres, quais as pessoas responsáveis para diagnosticar o desastre e executar o plano de ação.

Atualmente, há uma preocupação muito grande com segurança da informação. Logo, as empresas procuram criar suas próprias políticas para assegurar seus ativos.
Saiba mais sobre essa questão, acessando os *sites*:
http://www.ibm.com/developerworks/br/cloud/library/cl-cloudsecurepolicy/

http://www.sisp.gov.br/faq_segurancainformacao/one-faq?faq_id=13971979

Resumo

Nesta aula, você estudou que a implantação de uma política de segurança da informação na organização se faz necessária por ditar as regras de uso dos recursos tecnológicos, além disso, podemos identificar as características que uma política de segurança deve conter. Para que uma política de segurança de informação não seja rejeitada em uma organização, é importante obedecer alguns critérios no desenvolvimento e implantação dos mesmos. Foi tratado também o plano de contingência e de recuperação de desastre, objetivando resguardar a empresa de imprevistos, caso ocorram.

Atividades de aprendizagem

7. De que forma uma política de segurança poderá ser recusada pelos funcionários em uma organização?

8. Por que é importante a criação de um plano de recuperação de desastre?

9. Quando abordamos política de classificação de dados, mostramos que elas são divididas em categorias, segundo os autores Mitnik e Simon. Cite-as e defina-as.

Caro(a) estudante,

Como pôde ser visto nesta aula, nossa preocupação foi apontar caminhos para assegurar as informações de uma organização, com a criação de uma política de segurança clara e sucinta que seja entendida por todos os funcionários e que seja funcional na empresa. Esperamos que você tenha assimilado todas as informações do conteúdo a que teve acesso. Até o próximo encontro, no qual abordaremos a criação de aplicações seguras.

Aula 7. Controles de segurança da informação: criação de aplicações seguras

Objetivos:

- identificar alguns cuidados para a criação de aplicações seguras;
- reconhecer um ambiente de desenvolvimento seguro; e
- distinguir as etapas para segurança no ambiente de desenvolvimento.

Prezado(a) estudante,

Convidamos você a refletir sobre controles de segurança da informação durante a criação de uma aplicação. Para tanto, precisamos considerar uma série de fatores que implicam diretamente nos cuidados a serem tomados durante o desenvolvimento de aplicações, cujas responsabilidades é do desenvolvedor ou da equipe de desenvolvedores em manter sigilo dos processos pertencentes a uma empresa. Além dessas pecauções é preciso assegurar que os dados inseridos na aplicação sejam confiáveis e consistentes.Essas questões são o tema desta aula. Continue atento(a) e não deixe de realizar as atividades de aprendizagem.

7.1 Criação de aplicações seguras

Quando se desenvolve uma aplicação, são necessários cuidados relacionados à segurança que envolvem tanto o ambiente como a equipe técnica de desenvolvimento que estará à frente do trabalho. Esses cuidados devem ser redobrados caso a aplicação seja específica para atender uma empresa, pois os dados levantados para o desenvolvimento da aplicação devem ser tratados como sigilosos, por pertencer apenas a ela.

É possível avaliar o nível de segurança de uma aplicação em função dos recursos utilizados para impedir ataques oriundos de agentes maliciosos em seu ambiente de produção.

A norma que especifica as diretrizes para criação de aplicações seguras é definida como Common Criteria, ou Critério Comum, que deu origem à norma ISO/IEC 15408, e tem como objetivo:

> Fornecer um conjunto de critérios fixos que permitam especificar a segurança de uma aplicação de forma não ambígua a partir de características do ambiente da aplicação, e definir formas de garantir a segurança da aplicação para o cliente final. Ou seja, Common Criteria pode ser utilizado para desenvolver um sistema seguro ou avaliar a segurança de um já existente. (LYRA, 2008, p. 173)

A Norma ISO/IEC 15408 apresenta quatro níveis de garantia de segurança (EAL – Evaluation Assurance Level), tais como:

O **nível 1** tem por função testar a funcionalidade do sistema, pois visa atender os requisitos solicitados e identificar as proteções necessárias contra ameaças, além disso, deve haver avaliação na versão final, comparando com os requisitos iniciais sem o auxílio do desenvolvedor.

O **nível 2** tem por função garantir que as aplicações desenvolvidas estejam atendendo aos padrões preestabelecidos, além disso, que seja realizada uma análise para verificar as vulnerabilidades do sistema e aplicar testes para observar a segurança e validação dos dados.

O **nível 3** visa à aplicação de procedimentos de segurança sem que o sistema sofra com mudanças, além de propiciar testes completos do sistema sem precisar da reengenharia.

O **nível 4** objetiva garantir maior segurança durante o desenvolvimento do sistema, aplicando alguns procedimentos de teste e verificação dos resultados.

Para se ter segurança em todo o ciclo de vida do desenvolvimento da aplicação, é importante a adoção de critérios de segurança do mais alto nível, com o uso de ferramentas e de processos também robustos.

7.2 Características de um ambiente seguro

A segurança inicia no ambiente de trabalho com a aplicação de controles relacionados aos acessos físicos, além da proteção lógica dos servidores. Para isso, Melo, em sua palestra postada no site do SERPRO afirma que um am-

biente seguro apresenta como características a divisão entre ambiente de desenvolvimento, teste e construção, essas ações servirão para inibir o roubo de código ou indisponibilidade da equipe de desenvolvimento, outra sugestão é que a equipe de desenvolvimento siga as especificações de segurança para evitar falhas, dessa forma, dará ao cliente garantias de que o sistema é seguro. Disponível em < http://www.softwarelivre.serpro.gov.br/recife/download-plaestras/Apresentacao%20Seguranca%20Desenvolvimento.pdf> Acesso em: 12 ag. 2013

Atividades de aprendizagem

1. Uma aplicação deve assegurar a consistência dos dados introduzidos, para isso, algumas medidas de segurança devem ser tomadas durante o seu desenvolvimento. A Norma ISO/IEC 15408 apresenta quatro níveis de garantia de segurança (EAL – Evaluation Assurance Level). Cite e explique cada uma delas.

2. Aponte uma característica que retrate um ambiente de desenvolvimento seguro.

7.3 Etapas para segurança no ambiente de desenvolvimento

Manter um ambiente seguro é uma tarefa que requer uso de regras formalmente especificadas, de fácil entendimento, que sejam de conhecimento de todos em uma empresa e, claro, que tenha alguém responsável por manter vivas essas regras na empresa, avaliando-as periodicamente e adaptando-as às novas necessidades.

Neste contexto, Lyra (2008, p. 81), baseando-se na norma ISO/IEC 15408, propõe um modelo de segurança no ambiente de desenvolvimento com as seguintes etapas: **Gerência de configuração**; **distribuição**; **desenvolvimento**; **documentação**; **suporte ao ciclo de vida**; **teste de segurança;** e **avaliação de vulnerabilidades**. Vamos então detalhar cada uma delas.

- **Gerência de configuração**

Uma gerência de configuração permanente no ambiente de desenvolvimento é sugerida para o ambiente, pois auxilia na garantia dos aspectos básicos da segurança da informação, como a integridade do sistema.

Essa gerência tem por função prevenir modificações, inserções e deleções sem autorização na documentação do sistema, de forma a auxiliar no processo de desenvolvimento menos frágil a erros ou negligência humana.

- **Distribuição**

Para que o sistema não apresente nenhum problema no processo de mudança entre o desenvolvimento e a produção, é importante garantir que a versão disponibilizada para implantação tenha as características especificadas de segurança.

- **Desenvolvimento**

Deve-se representar, em todos os níveis de abstração, as funcionalidades de segurança, tendo início a partir do projeto lógico até a implementação dos produtos finais.

- **Documentação**

Outro item importante que merece atenção é o manual de auxílio, elaborado tanto para usuários quanto para os administradores. O manual para usuários consiste das instruções de uso, descrição das funções de segurança. Já o manual do administrador é composto de auxílio referente a manutenção, administração e configuração, de forma que garanta o uso correto e seguro do sistema.

- **Suporte ao ciclo de vida**

Os requisitos estabelecidos para assegurar o sistema dependem do modelo do ciclo de vida adotado, pois, caso a seleção não seja adequada com as normas de segurança propostas, poderá comprometer a segurança do produto final.

Para esse caso, a Norma ISO sugere o uso de modelos reconhecidos, como CMMI, RUP, etc. O uso desses modelos garante que os padrões referentes à segurança da informação sejam abordados adequadamente durante as fases de desenvolvimento e manutenção (Lyra, 2008).

- **Testes de segurança**

Alguns mecanismos de testes podem ser criados para garantir que a aplicação esteja atendendo aos pré-requisitos definidos, tais como o uso de ferramentas CASE (*Computer-Aided Software Eninnering*) que disponibiliza processo de teste automatizado, teste de instalação, de aceitação, unidade e integração, conforme afirma Lyra (2008).

- **Avaliação de vulnerabilidades**

Nessa fase de finalização do processo de desenvolvimento, cuidados referentes ao mau uso do sistema, introdução de vulnerabilidades durante o desenvolvimento e aplicação de configurações incorretas são algumas preocupações que merecem atenção nesse momento, devendo ser identificadas e corrigidas.

A Norma ISO sugere a aplicação de um método de desenvolvimento já bem estruturado, que contemple no mínimo as atividades de planejamento, acompanhamento e definição dos testes para verificação.

Atividades de aprendizagem

3. Como devem ser as regras para manter um ambiente de desenvolvimento seguro?

4. A Norma ISO/IEC 15408 propõe um modelo de segurança no ambiente de desenvolvimento a partir de algumas etapas. Cite-as.

5. Gerência de configuração é uma etapa sugerida pela Norma ISO/IEC 15408 para resguardar uma aplicação durante seu desenvolvimento. Qual a função dessa etapa?

7.4 Segurança no ciclo de vida de desenvolvimento da aplicação

A garantia da segurança de um sistema está associada a aplicação de cuidados especiais durante seu desenvolvimento, resultando em um código fonte confiável mais seguro e robusto.

Logo, a produção de códigos seguros torna a aplicação mais lenta, reduzindo sua performance, mas isso não deve ser encarado como problema, pois

pode ser solucionado com um investimento em equipamentos mais rápidos não implicando na redução de desempenho.

Melo, na palestra já citada, disponível no site do SERPRO, define quatro normas e práticas da boa programação:

- Funções intrinsecamente seguras;
- Verificar códigos de erro retornado por função ou método;
- Atentar para tamanho de buffers e arrays do sistema;
- Documentar o código;

Observe a que se refere cada uma dessas normas e práticas:

- **Funções intrinsecamente seguras**

É fazer uso de linguagem que apresenta flexibilidade de programação, na qual o programador poderá criar funções ou mesmo fazer usos de funções que proporcionam essa segurança.

- **Verificar códigos de erro retornado por função ou método**

Sempre que se fizer uma chamada da função, a mesma deve ser testada, dessa forma, caso o resultado não atenda aos requisitos estabelecidos durante o processo de desenvolvimento, o dado gerado deve ser desconsiderado.

A-Z

Buffer: armazenamento temporário. Uma área reservada na memória para armazenar dados enquanto estão sendo processados.

Array: (Matriz) uma combinação de elementos de dados.

- **Atentar para tamanho de *buffers* e *arrays* do sistema**

O ideal é sempre operar o sistema de acordo com as permissões requeridas para executar suas tarefas de forma adequada, pois um erro de buffers ou arrays pode comprometer o desempenho da aplicação.

- **Documentar o código**

Outra etapa importante para garantir a segurança da aplicação é documentar corretamente todo o código, para evitar mal-entendidos na leitura do mesmo ou ainda usá-lo incorretamente .

O que foi exposto acima são alguns cuidados a serem tomados durante a implementação do código, pois durante a fase de implementação de uma aplicação, podemos nos deparar com inúmeras dificuldades, logo, seguir um padrão ajuda consideravelmente na redução de problemas comuns.

Atividades de aprendizagem

6. Quando se desenvolve uma aplicação, devemos nos preocupar em elaborar a documentação para posteriores usos. Por que devemos registrar as ações efetuadas durante o processo de desenvolvimento?

7. Garantir a segurança de uma aplicação durante seu desenvolvimento reduz a performance da aplicação. Explique porque esse fator não deve ser considerado um problema.

8. Especifique quais são as normas e práticas de uma boa programação conforme determinado no site do SERPRO.

Resumo

Nesta aula, você pôde conhecer um pouco mais dos cuidados que devemos ter durante a criação de uma aplicação para assegurar o seu desempenho e credibilidade dos dados gerados quando concluída essa etapa. Também pôde identificar as características de um ambiente seguro, bem como aprender sobre algumas etapas para segurança no ambiente de desenvolvimento, complementada com a apresentação das etapas de segurança em todo o ciclo de vida de desenvolvimento da aplicação. Todas essas precauções durante o processo de desenvolvimento garantirão uma aplicação final com o mínimo ou nenhuma vulnerabilidade ou erros no sistema, resguardando o usuário final e a equipe de desenvolvimento de transtornos futuros.

Sugiro que você faça as atividades de aprendizagem e em seguida confira seu desempenho no guia de soluções a fim de que possa saber se é preciso retomar o estudo dessa aula.

Atividades de aprendizagem

9. Porque devemos ter cuidados especiais durante o processo de desenvolvimento de uma aplicação? Explique.

10. Com relação à segurança no ciclo de vida de desenvolvimento da aplicação, temos algumas etapas sugeridas pelo SERPRO. Você deve relacionar a primeira coluna de acordo com as definições da segunda coluna.

A) Atentar para tamanho de buffers e arrays do sistema.	( )	Sempre que fizer uma chamada da função, a mesma deve ser testada; dessa forma, caso o resultado não esteja atendendo aos requisitos estabelecidos durante o processo de desenvolvimento, o dado gerado deve ser desconsiderado.
B) Verificar códigos de erro retornado por função ou método	( )	É fazer uso de linguagem que apresentam flexibilidade de programação, na qual o programador poderá criar funções ou mesmo fazer usos de funções que proporcionam essa segurança.
C)Funções intrinsecamente seguras	( )	O ideal seria sempre operar o sistema de acordo com as permissões requeridas para executar suas tarefas de forma adequada, pois um erro de buffers ou arrays poderia comprometer o desempenho da aplicação.
D) Documentar o código	( )	Documentar corretamente todo o código, para evitar mal-entendidos na leitura do código ou mesmo usar o código erroneamente.

Caro(a) estudante,

Os assuntos vistos são de suma importancia para o profissional de TI. A seguir, você poderá verificar alguns controles de segurança da informação, em especial a Auditoria em Sistemas Computacionais, que envolve algumas formas de auditar um ambiente informatizado. Vamos lá!

Aula 8. Controles de segurança da informação: auditoria em sistemas computacionais

Objetivos:

- identificar padrões de auditoria a serem seguidos;
- reconhecer as formas de auditoria em sistemas de informação; e
- apontar as etapas de uma auditoria.

Estamos agora na reta final da disciplina e, nesta última aula, centraremos nossos estudos em auditoria. Iniciaremos conceituando, mas também vamos destacar alguns padrões a serem seguidos pelos auditores em sistemas de informação. Abordaremos, ainda, as formas de auditoria e, finalmente, elencaremos algumas etapas para se fazer uma auditoria em um ambiente de sistema de informação.

Bons estudos!

8.1 Auditoria em sistemas computacionais

Muitas mudanças ocorreram nesse último século em todos os ambientes de negócios. Numa velocidade muito grande, as empresas começaram a expandir seus negócios e com isso a complexidade para administrar aumentou.

Nesse contexto, os sistemas de processamento de dados tiveram que acompanhar também esse desenvolvimento. Os equipamentos passaram a ser utilizados para executar desde as tarefas mais simples até as mais complexas. Com isso, a exposição aos riscos aumentou, pois as informações agora são disseminadas na rede de computadores Internet, e podemos afirmar que as vulnerabilidades dos sistemas de processamento eletrônico se difundem na mesma velocidade.

Isso requer dos profissionais de auditoria conhecimento tecnológico e habilidades no trato com esses ambientes informatizados, às vezes bastante com-

plexos, o que gerou a criação de novas técnicas e ferramentas de avaliação de sistemas.

8.2 Conceito de auditoria

Para iniciarmos nossa aventura, vamos então tratar auditoria como um conjunto de atividades para levantar, estudar e avaliar sistematicamente os processos de uma empresa, buscando evidências acerca das ações efetuadas.

No Manual de Auditoria do Tribunal de Contas do Distrito Federal, Auditoria é definida como:

> Processo sistemático de obtenção e avaliação objetiva de evidências sobre ações e eventos econômicos, legais e operacionais para aquilatação do grau de correspondência entre as afirmações e critérios estabelecidos e a comunicação de resultados a usuários interessados. Disponível em < http:www.tc.df.gov.br/app/biblioteca/pdf/PE500418.pdf.> Acesso em: 27 jan. 2013.

8.3 Padrões

Infelizmente, não há padrões para auditores de sistemas, o que há de concreto é uma adaptação dos padrões existentes para auditar ambientes informatizados.

Essa despadronização é justificada porque os sistemas de informação sempre foram vistos como parte de uma auditoria geral, não sendo designada como uma profissão isolada, mas sim como complemento agregado aos trabalhos de auditoria normal.

Contudo, o Comitê de Padrões da Associação de Controle e Auditoria de Tecnologia da Informação e a Associação de Auditores de Sistemas & Controles (ISACA) criaram algumas normas para execução dessa tarefa. Vejamos a seguir:

Responsabilidade, autoridade e prestação de contas

A responsabilidade, a autoridade e a prestação de contas sobre a função de auditor de tecnologia de informação devem ser apropriadamente documentadas numa carta proposta ou de aderência ao escopo.

- **Independência profissional**

Em todas as questões relativas à auditoria, o auditor de tecnologia de informação deve ser independente, seja em atitude ou aparência. No relacionamento organizacional, a função de auditor de tecnologia de informação deve ser suficientemente independente da área sob auditoria para permitir uma conclusão objetiva de auditoria.

- **Ética profissional e padrões**

O auditor de TI deve aderir ao código de ética profissional da Associação de Controle e Auditoria de Tecnologia de Informação, atentando para o cumprimento do zelo profissional. O devido zelo profissional e a observância dos padrões profissionais de auditoria devem ser exercidos em todos os aspectos do trabalho do auditor de tecnologia de informação.

- **Competência**

O auditor de tecnologia da informação precisa possuir habilidades e conhecimentos específicos para executar esse tipo de trabalho, bem como ter competência técnica para sua utilização.

O constante aprimoramento profissional, através da educação continuada, é requisito para manutenção da competência técnica do auditor de tecnologia.

- **Planejamento**

O planejamento das tarefas é indispensável para o direcionamento dos objetivos da auditoria, bem como para seguimento dos padrões profissionais dela. Assim, é necessária uma supervisão da equipe para garantia do alcance dos objetivos, bem como para assegurar que os padrões de auditoria aplicáveis sejam respeitados.

Para o alcance efetivo dos objetivos da auditoria, o auditor de tecnologia da informação precisa conseguir evidência confiável, relevante, suficiente e proveitosa durante o curso da auditoria.

- **Emissão de relatório**

Na conclusão dos trabalhos de auditoria, deve ser providenciado para os destinatários um relatório apropriado. Nesse relatório, devem constar objetivos, escopo, natureza e extensão do trabalho realizado, bem como período de abrangência. É preciso também identificar a organização, as restrições à sua circulação e ainda, os usuários desejáveis. No relatório incluem-se ainda, conclusões, observações, recomendações e qualquer tipo de conceito ou ressalva que o auditor conseguiu durante a auditoria.

- **Atividades de *follow-up***

É função do auditor de tecnologia de informação solicitar e avaliar informações significativas sobre conclusões, pontos e recomendações anteriores, importantes para mostrar se ações adequadas foram implementadas em tempo hábil.

A Associação de Auditores de Sistemas & Controles (ISACA) criou um código de ética profissional para delinear as atividades a serem desenvolvidas.

A-Z

Stakeholders: São todos os envolvidos direta ou indiretamente em interesses da organização, que possuem algum grau de influência (positiva ou não) sobre uma determinada atividade, ação ou projeto, capazes de influenciar a mudança de direção atual ou mesmo uma decisão futura. ALVES,2006, p. 17)

Esse código informa que as funções devem ser exercidas com objetividade, diligência e zelo profissional, procurando manter a confidencialidade e a privacidade das informações obtidas durante o processo de auditoria, exceto se forem solicitadas legalmente. O código ainda sugere que os profissionais da auditoria devem ter tanto habilidade como competência profissional para exercer a função, além de servir aos interesses dos ***stakeholders*** de forma legal e honesta, apoiando a conscientização desses profissionais quanto à importância da segurança das informações na empresa, e ainda apresentar relatório às partes envolvidas com os resultados dos trabalhos, conforme apontado por Imoniana (2005, p. 31).

Atividades de aprendizagem

1. Porque a auditoria de sistemas de informação não é padronizada? Explique

2. O que você entende por auditoria?.

3. O Comitê de Padrões da Associação de Controle e Auditoria de Tecnologia da Informação e a Associação de Auditores de Sistemas & Controles (ISACA) sugeriram algumas etapas para execução de uma auditoria. Cite duas que você considera mais importantes em uma auditoria e justifique sua escolha.

8.4 Formas de auditoria em sistemas de informação

Na auditoria tradicional, os documentos-fontes (documentos que geram todas as transações financeiras, contábeis e econômicas) sempre foram provas reais para os testes de confiabilidade dos registros, ficando à disposição para os gestores da organização tomarem suas decisões, para os auditores analisarem quando a empresa fosse auditada, contudo, a partir da evolução tecnológica, os ambientes corporativos ficaram mais complexos para serem geridos.

Papéis, por exemplo, são pouco utilizados em um ambiente informatizado, os dados estão mesmo armazenados em ambientes informatizados, gerando um problema de segurança, em virtude das vulnerabilidades a que os computadores estão expostos.

Em virtude das características desses novos ambientes corporativos, Imoniana (2005, p. 18), propõe três formas de auditoria de sistemas de informações, nomeadas a seguir:

- Abordagem ao redor do computador;
- Abordagem através do computador;
- Abordagem com o computador.

- **Abordagem ao redor do computador**

Antigamente, esse método era o mais usual, justamente porque eram poucas as empresas que utilizavam esses equipamentos.

Sendo assim, a auditoria era feita analisando os dados que entravam e saíam da máquina, não oferecendo muita atenção às funções de processamento eletrônico de dados porque as tarefas realizadas eram básicas, tais como controles de estoque, por exemplo, além de serem utilizados para imprimir relatórios.

Porém, utilizando essa técnica, não era verificado como os resultados eram calculados; nessa abordagem, os auditores não tinham nenhum contato

mais aprofundado com o processamento dos dados gerados, isso influenciou a qualidade da auditoria com o passar dos anos, pois não havia parâmetros claros e padronizados de que os resultados obtidos eram os mesmos esperados, não apresentando segurança suficiente para a credibilidade dos relatórios gerados.

- **Abordagem através do computador**

Esse modelo já apresentava melhorias em relação à abordagem anterior, sendo possível:

> Uma pessoa requisitar, de muitas maneiras, como é praticada na abordagem ao redor do computador, a verificação dos documentos-fontes com dados intermediários; porém, estabelece o auditor maior ênfase em todas as técnicas que utilizam o computador como uma ferramenta para testar a si próprio e, também, testar a entrada de dados.
>
> O método *test data*, que é o processamento de um dispositivo capaz de simular todas as transações possíveis, era utilizado nesta abordagem. (IMONIANA,2005, p. 20)

Algumas vantagens eram claramente visualizadas no uso deste modelo, no que diz respeito ao preparo do profissional que audita, sendo necessários conhecimentos mais aprofundados das tecnologias da informação e aquisição de aplicativos de auditoria.

Em contrapartida, algumas desvantagens também eram apontadas, tais como: algumas perdas poderiam ocorrer caso a operação fosse realizada incorretamente, essa abordagem foi encarecida em virtude da necessidade de maior preparo dos auditores e investimentos em ferramentas tecnológicas, os aplicativos de auditoria podiam ser contaminados em virtude do contínuo uso em auditorias, a complementação das técnicas de auditoria manuais poderiam ser comprometidas, caso os aplicativos de auditoria gerassem resultados errados.

- **Abordagem com o computador**

Essa abordagem foi proposta por diversos especialistas, trazendo algumas facilidades em seu uso, como a possibilidade de desenvolvimento de aplicações específicas para atender uma necessidade de auditoria, ganho de

tempo diante do uso de aplicações generalizadas de auditoria.

Essas aplicações generalizadas podem ser entendidas como softwares, aplicações que executam tarefas básicas, não focando um processo específico com mais detalhes.

Atividades de aprendizagem

4. Com relação à abordagem através do computador, marque a alternativa incorreta:

a) Método de auditoria mais antigo.

b) A auditoria era feita a partir dos dados que entravam e saiam da máquina, o processamento eletrônico de dados não era considerado para auditar.

c) A qualidade da auditoria realizada com esse modelo era questionado, pois não havia parâmetros claros e padronizados de que os resultados obtidos fossem os mesmos esperados.

d) Com o uso desse modelo, era possível fazer a verificação dos resultados calculados.

5. Dos três modelos apresentados de auditoria, qual o mais eficaz? Justifique.

8.5 Etapas de uma auditoria

Para iniciar uma auditoria, é necessário cumprir algumas etapas para não perder o foco do trabalho e manter o processo organizado e transparente. Vejamos essas etapas a seguir.

Planejamento

Auxilia na orientação das atividades a serem realizadas e deve ser caracterizado para evitar qualquer atividade inesperada na empresa.

Nessa etapa, deve ser elaborada uma "matriz de risco" que seja atualizada sempre, tendo como parâmetro os resultados obtidos nos testes e nas avaliações dos auditores, bem como o impacto recorrente de mudanças ocorridas nos negócios a partir de mudanças estratégicas

empresariais, evoluções tecnológicas, legislações, concorrência, mudanças estatutárias, mudanças nas leis ambientais, sociais, econômicas ou outro fator que reflita nos resultados financeiros, qualidade dos controles, continuidade dos serviços e processos operacionais.

Escolher a equipe

O perfil básico da equipe de auditoria de TI depende dos negócios em que a empresa atua, isso já deve estar bem detalhado no planejamento. Nesse caso, vejamos alguns exemplos de perfil que devemos requerer da equipe de auditoria: formação acadêmica, conhecimento de língua estrangeira caso necessário, conhecimento e experiência da área que vai auditar, disponibilidade para viajar, caso necessário etc.

Programar a equipe

Para esta etapa, já deve haver um encarregado para programar os trabalhos a serem realizados pela equipe, mesmo que a equipe atenda às sugestões de perfil citados anteriormente, não significa assegurar que os riscos de auditoria sejam reduzidos pelos testes de auditoria.

Execução de trabalhos e supervisão

Durante uma auditoria, deve-se garantir a qualidade e certificar que as tarefas foram adequadamente feitas, isso implica na formação do profissional que fará parte da equipe, ou seja, quanto mais experiência e conhecimento técnico no ramo de atividade da empresa auditada, mais fácil será identificar os processos e reconhecer erros caso houver.

Revisão dos papéis de trabalhos

As atividades realizadas pelos auditores devem ser revisadas pelos superiores, de forma que a garantir a qualidade exigida pelas práticas de auditoria.

Nesse caso, os superiores têm a responsabilidade de averiguar se cada passo concluído da auditoria foi cumprido. Se, porventura, for detectada alguma pendência na auditoria, como falhas ou recomendações

para melhorias, procedimentos que não tenham sido cumpridos por restrições do próprio cliente, o revisor poderá solicitar uma nova visita para completar os trabalhos. (IMONIANA, 2005, p. 23)

Atualização do conhecimento permanente

A atualização de informações ditas permanentes poderá ajudar a reduzir horas de auditoria do período seguinte, ou seja, uma vez realizada, ao término é emitido um relatório. Esse relatório contendo todos os dados corretos poderá auxiliar em uma nova auditoria, pois os processos já estarão descritos, não sendo mais necessário estudá-los novamente, bem como o levantamento e avaliação do ambiente de controle, estudo das vulnerabilidades nos controles internos também já estarão citados, entre outros detalhes.

Avaliação da equipe

Ao término de cada auditoria, deve-se avaliar o desempenho da equipe, observando os pontos fracos e fortes do auditor, elogiando quando apresentar eficiência e eficácia e auxiliando-o no desenvolvimento de planos para superar as fraquezas e tornar-se um profissional qualificado e consciente.

Resumo

Nesta última aula, procuramos centrar o estudo dos controles de segurança da informação em Auditoria, por se tratar de um levantamento e estudo sistematizado dos processos internos de uma organização, buscando erros humanos e/ou falhas tecnológicas que deixam vulneráveis o sistema de informação de uma empresa. Apresentamos também as formas de auditoria e as etapas a serem seguidas para auditar.

Todos os aspectos levantados nesta aula são de grande relevância para o profissional de TI, sendo um dos responsáveis por resguardar a empresa das possíveis perdas das informações ocasionadas pela falta de segurança tanto nas aplicações como no aspecto físico.

Atividades de Aprendizagem

6. Relacione a primeira coluna de conceitos de acordo com as definições na segunda coluna.

A) Avaliação da equipe	( )	Auxilia na orientação das atividades a serem realizadas e deve ser caracterizado para evitar qualquer atividade inesperada na empresa.
B) Planejamento	( )	Para esta etapa, já deve haver um encarregado para programar os trabalhos a serem realizados pela equipe.
C) Programar a equipe	( )	Ao término de cada auditoria, deve-se avaliar o desempenho da equipe, observando os pontos fracos e fortes do auditor, elogiando quando apresentar eficiência e eficácia e auxiliando-o no desenvolvimento de planos para superar as fraquezas e tornar-se um profissional qualificado e consciente.
D) Execução de trabalhos e supervisão	( )	O perfil básico da equipe de auditoria de TI depende dos negócios em que a empresa atua, isso já deve estar bem detalhado no planejamento.
E) Escolher a equipe	( )	Durante uma auditoria, deve-se garantir a qualidade e certificar que as tarefas foram adequadamente feitas, isso implica na formação do profissional que fará parte da equipe.

7. Qual a importância de se estabelecer controles de segurança de informação nos processos de negócios de uma empresa?

8. O Comitê de Padrões da Associação de Controle e Auditoria de Tecnologia da Informação e a Associação de Auditores de Sistemas & Controles (ISACA) criaram algumas normas para execução da auditoria. Cite-as.

9. Especifique as etapas de uma auditoria.

Caro(a) estudante,

Chegamos ao final de nossa jornada de estudos nesta disciplina. Nesta aula, não tivemos a pretensão de apresentar um texto conclusivo no conteúdo abordado, mas a intenção de provocar alguns questionamentos e reflexões sobre a auditoria em ambientes informatizados, considerando a rapidez com que as informações se disseminam e o aparecimento de novas formas de comunicação e armazenamento de dados.

Palavras finais

Ufa! Até que enfim, chegamos ao final de mais uma empreitada. Acreditamos que as informações aqui tratadas darão um respaldo a você em sua trajetória profissional. O conteúdo apresentado objetivou torná-lo capaz de identificar os fatores que fazem da segurança da informação uma área gigante ainda em exploração, com temas inesgotáveis, considerando a rápida evolução tecnológica.

Continue estudando, buscando conhecimento e pesquisando sobre as temáticas que envolvem segurança da informação, por se tratar de uma área que requer estudos detalhados e constantes. Lembre-se de que o competitivo mercado de trabalho atual exige profissionais qualificados e sempre em dia com as novas tecnologias.

Guia de Soluções

Aula 1

1. Qual a importância da informação para a sociedade?

Resposta: A informação deve ser encarada como um elemento vital, pois contribui para a formação de um indivíduo mais consciente, participativo em sua sociedade.

2. Conceitue Informação.

Resposta: É considerada um ativo valioso para a empresa e pessoas, para a empresa é um recurso crítico para a realização dos negócios, podendo ser considerada para as pessoas um bem de cunho afetivo, cujo valor é incalculável.

3. Elabore um conceito de Segurança da Informação.

Resposta: São mecanismos de segurança criados para assegurar os ativos tanto de uma empresa como ativos pessoais.

4. Identifique os objetivos do Departamento de Segurança da Informação em uma empresa.

Resposta: Basicamente envolvem a criação, implementação, controle e monitoramento de políticas que objetivam assegurar os ativos de informação de uma empresa ou pessoa.

5. Quais os princípios da segurança da informação? Defina-os.

Resposta:

Confidencialidade: Garante que somente pessoas autorizadas poderão acessar as informações. Trata-se da não permissão da divulgação de uma informação sem prévia autorização.

Disponibilidade: Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema.

Integridade: Garante que a exatidão e completeza das informações não sejam alteradas ou violadas.

Legalidade: refere-se à garantia de que a produção da informação se deu conforme a lei.

Autenticidade: É a garantia de que os remetentes, num processo de comunicação, são exatamente aquilo que dizem ser e que a informação ou mensagem não sofreu alteração depois da sua validação ou envio.

6. Relacione a segunda coluna de acordo com a primeira:

(a) Informação	(C) Disponibilidade, Confidencialidade e Integridade.
(b) Segurança da informação	(A) É um conjunto de dados
(c) Princípios básicos da segurança da informação	(D) Criar, implementar, controlar e monitorar políticas que assegurem os ativos.
(d) Função do Departamento de TI nas empresas	(B) São regras criadas para proteger os ativos de uma empresa.

Aula 2

1. O que você entende por ativo de uma empresa? Explique.

Resposta: Ativo pode ser compreendido como tudo aquilo que se faz necessário ao bom funcionamento dos negócios, caso violados, trarão consequências negativas para a empresa.

2. Os incidentes em uma empresa ocorrem quando uma e/ou várias ameaças exploram os pontos fracos da mesma, seja intencionalmente ou não. Cite os princípios da segurança da informação violados.

Resposta: Os princípios básicos da informação violados que acarretaram incidentes são: confidencialidade, integridade e disponibilidade.

3. Quando um ativo da informação sofre um ataque potencial, podemos entender como ameaça. Este ataque poderá ser efetuado por agentes externos ou internos diante das vulnerabilidades apresentadas no sistema da empresa. Como essas ameaças podem ocorrer?

Resposta: As ameaças podem ocorrer em decorrência de fenômenos naturais, propositalmente ou mesmo inconscientemente.

4. Cite alguns riscos aos quais as pessoas estão sujeitas ao utilizar a Internet.

Resposta: Os dados do computador estarão expostos na rede, caso tenha uma senha, contas em bancos, fotografias elas poderão ser copiadas e, a partir daí, a pessoa que copiou esses dados poderá tirar proveito, pondo em risco sua reputação. Quanto aos dados referentes a uma empresa, o problema não é muito diferente, pois a obtenção de dados sigilosos poderão ocasionar um impacto grande ou pequeno nos negócios.

5. Leia as afirmações e assinale a alternativa correta.

a) Quando os princípios da segurança da informação são violados e há interrupção dos processos normais de negócio, denomina-se Incidente.

b) Ativo é conhecido como tudo que tem valor para a organização e uma vez violados não trarão impactos relevantes para a empresa.

c) As falhas podem ser apenas humanas e de forma intencional.

d) Quando as atividades interrompidas na empresa em decorrência de um furacão são entendidas como risco.

A alternativa correta é a letra A

6. Explique a importância de um Plano de Recuperação de Desastre para a empresa?

Resposta: É uma forma de a empresa não sofrer grandes danos ocasionados por intempéries da natureza ou mesmo eventos ocasionados pelo homem, como greves, manifestações populares etc, pois visa a não interrupção dos negócios a partir da criação de alternativas de trabalho – um plano B, caso as que estejam em uso atualmente faltem.

AULA 3

1. Que cuidados as empresas devem ter ao contratar um novo funcionário?

Resposta: Solicitar documentos e referências e procurar constatar se as informações são legítimas, apresentar formalmente as diretrizes que envolverão suas atribuições.

2. O que você entende por problemas de acesso lógico?

Resposta: É importante compreender que problemas de ordem lógica não significam acessos indevidos somente, podemos definir como sendo ocorrência de falhas em algum programa que a empresa faz uso para realização de suas atividades, ficando o sistema indisponível.

3. Cite alguns cuidados que o setor de Tecnologia da Informação deve tomar para fazer o reconhecimento e a autenticação do usuário no sistema.

Resposta: orientar os usuários a não emprestar suas IDs a outros funcionários, manter atualizado o cadastro de IDs de usuários ativos na empresa para evitar redundâncias, assegurar que o provedor somente permitirá acessos a usuários cadastrados.

4. Por que fazer o controle dos funcionários que gerenciam os privilégios os usuários? Explique.

Resposta: Esse gerenciamento de funcionários evitará uso indiscriminado de privilégios ao sistema, tentando reduzir falhas de sistemas que foram violados.

5. Cite duas tecnologias de identificação e autenticação de usuários.

Resposta: biometria, uso de cartões com chip, verificação de assinatura.

6. Relacione os termos da primeira coluna de acordo com as definições da segunda coluna:

(A) Assinatura Digital	(B)	Aplicativos que identificam e deletam arquivos infectados no disco, arquivos anexos a e-mail e outros meios lógicos que a empresa utiliza para guardar seus dados; dessa forma, esses aplicativos asseguram a integridade dessas informações.
(B) Programas Antivírus	(E)	Tem por função analisar os acessos efetuados na rede, observando as inúmeras linhas de logs e diagnosticando em tempo real possíveis ataques.
(C) Honeypot	(D)	Cria cópias de segurança das informações importantes para os negócios que estão gravadas nos servidores e computadores dos usuários.

(D) Backup	(A)	Processo que garante que a mensagem realmente veio do remetente, confirmando sua autenticidade.
(E) Detecção de Intrusos	(C)	Aplicativo que tem por função impedir ou mesmo identificar a ação de um invasor, ou qualquer ação estranha ao sistema.
(F) Firewall	(F)	Gerencia o tráfego de pacotes entre a rede local e a Internet em tempo real.

Aula 4

Utilize o quadro abaixo para as três primeiras questões.

Vamos tentar pôr em prática o método de criptografia proposto por Marçula e Benini Filho. Para a solução dos problemas propostos, você deverá utilizar a tabela a seguir para codificar e decodificar as mensagens.

A	B	C	D	E	F	G	H	I	J
01	02	03	04	05	06	07	08	09	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	Espaço em Branco			
21	22	23	24	25	26	00			

1. De férias nos Emirados Árabes, a conselheira Trace recebe uma caixa de seu chocolate Cretariano favorito, juntamente com uma mensagem criptografada do remetente, revelando sua identidade. Usando o exemplo de criptografia citado por Marçula & Benini Filho, decodifique a mensagem MPHKCESEVGUGSRKVVECB, cuja chave é: 00 07 05 03 02. Decodifique para saber o nome do remetente.

RESPOSTA DO PROBLEMA 1

Mensagem a ser enviada: Michael seu noivo

QUADRO DE CODIFICAÇÃO:

M	I	C	H	A	E	L		S	E	U		N	O	I	V	O			
13	09	03	08	01	05	12	00	19	05	21	00	14	15	09	22	15	00	00	00
00	07	05	03	02	00	07	05	03	02	00	07	05	03	02	00	07	05	03	02
13	16	08	11	03	05	19	05	22	07	21	07	19	18	11	22	22	05	03	02
M	P	H	K	C	E	S	E	V	G	U	G	S	R	K	V	V	E	C	B

QUADRO DE DECODIFICAÇÃO:

M	P	H	K	C	E	S	E	V	G	U	G	S	R	K	V	V	E	C	B
13	16	08	11	03	05	19	05	22	07	21	07	19	18	11	22	22	05	03	02
00	07	05	03	02	00	07	05	03	02	00	07	05	03	02	00	07	05	03	02
13	09	03	08	01	05	12	00	19	05	21	00	14	15	09	22	15	00	00	00
M	I	C	H	A	E	L		S	E	U		N	O	I	V	O			

2. Em seu primeiro contato com um planeta Zomour com que a Retamatemil deseja estabelecer relações diplomáticas, os oficiais da UCorporation foram convidados para um banquete. Infelizmente, há um grupo dissidente no plano Zomour que deseja apoiar os Crodapon e não a Retamatemil. Um espião desta facção é instruído a envenenar um dos oficiais da UCorporation. O traidor é descoberto, mas foge a tempo. Em seu alojamento, é encontrada a mensagem codificada KWUXWVVCKN que contém o nome do oficial envenenado e um pedaço de papel com o números 0822031114 usados na codificação. Como o veneno é seu próprio antídoto, é preciso saber exatamente quem foi envenenado. Trabalhando contra o tempo, um especialista em segurança verificou que se tratava de um código muito simples, o código proposto por Marçula & Benini Filho. Qual o nome do Oficial envenenado?

RESPOSTA DO PROBLEMA 2

QUADRO DE DECODIFICAÇÃO:

K	W	U	X	W	V	V	C	K	N
11	23	21	24	23	22	22	03	11	14
08	22	03	11	14	08	22	03	11	14
03	01	18	13	09	14	00	00	00	00
C	A	R	M	I	N				

3. Você faz parte de uma equipe de segurança de seu país, o Janbolala, e precisa enviar a mensagem ao seu espião secreto que se encontra no país vizinho, o Kongololo. Mas, para isso, a mensagem precisa ser codificada. Usando o método de Marçula e Benini Filho, codifique mensagem:

Abortar operação. A Chave a ser utilizada para codificar é: 00 07 05 03 01

RESPOSTA DO PROBLEMA 3

QUADRO DE CODIFICAÇÃO:

A	B	O	R	T	A	R		O	P	E	R	A	C	A	O				
01	02	15	18	20	01	18	00	15	16	05	18	01	03	01	15	00	00	00	00
00	07	05	03	01	00	07	05	03	01	00	07	05	03	01	00	07	05	03	01
01	09	20	21	21	01	25	05	18	17	05	25	06	06	02	15	07	05	03	01
A	I	T	U	U	A	Y	E	R	Q	E	Y	F	F	B	O	G	E	C	A

AITUUAYERQEYFFBOGECA

4. Explique como funciona a assinatura digital.

Resposta: A partir de uma mensagem já digitalizada, utiliza-se um aplicativo que vai codificar a mensagem a partir de uma chave pública de uma pessoa ou empresa que irá receber a mensagem, em seguida, quando a mensagem chegar no destinatário, o receptor deverá utilizar sua chave privada para decodificar/decriptografar o documento, gerando um novo resumo a partir da mensagem que está armazenada para, em seguida, comparar com a assinatura digital para ler a mensagem, se não for igual, a mensagem não será aberta.

5. O que é hash?

Resposta: é um resumo gerado quando a mensagem é criptografada, tendo o mesmo tamanho. Dessa forma, garante a autenticidade e o não repúdio.

6. De que é composto o certificado digital?

Resposta: Composto por um conjunto de informações referentes à entidade para o qual o certificado foi emitido, baseando-se na criptografia de chave pública, garantindo assim outros aspectos da segurança da informação como autenticação e o não repúdio.

7. Explique o funcionamento do certificado digital.

Resposta: É utilizada a técnica da criptografia assimétrica, possuindo duas chaves, uma pública e outra privada. Tanto um nome de usuário como outras informações que identificam o usuário são vinculadas a um par de chaves,

e isso funciona como um credenciamento eletrônico que, quando instalado em um navegador da Web, permite a autenticação dos sites.

8. Cite os modelos de certificado digital.

Resposta: Modelo Web Oftrust (malha de confiança), modelo hierárquico e modelo de autoridade central.

9. Relacione os termos da primeira coluna de acordo com as definições da segunda coluna:

(A) Modelo Hierárquico	(C)	Seu funcionamento baseia-se na confiança, que é controlada pelos usuários, ou seja, quando um usuário obtém a chave pública de outro usuário, poderá verificar a autenticidade da chave recebida por intermédio das outras entidades, sendo então implantada uma rede em que as entidades pertencentes confiem umas nas outras.
(B) Modelo de Autoridade Central	(A)	Trata de uma hierarquia de autoridades certificadoras, na qual as AC´s certificam os usuários e a autoridade certificadora raiz AC-R faz a certificação de todas as AC´s de sua competência. Nesse modelo, para ser validado um certificado digital, é necessária a assinatura digital de uma AC.
(C) Modelo Web Oftrust	(B)	Envolve infraestrutura de chave pública, definido como ITU-T X.509. É absoluta sua autoridade certificadora, e é assim definido por ser organizado em uma estrutura de diretórios em árvore, cujo certificado digital não pode conter a chave privada do usuário, a mesma é armazenada em tokens ou smart cards.

10. Como é classificada a criptografia? E qual a diferença entre os dois tipos?

Resposta: em duas categorias, a criptografia simétrica e assimétrica. O que as diferencia é exatamente a chave, pois na criptografia simétrica existe apenas uma chave que servirá para codificar e decodificar e na criptografia assimétrica há duas chaves, uma pública e uma privada. A privada é exclusiva de um usuário e serve para codificar a mensagem e a outra chave, pública, é para o destinatário poder acessar a mensagem.

Aula 5

1. O que é uma autoridade certificadora?

Resposta: São instituições credenciadas para emitir certificados digitais, associando ao titular pares de chaves criptográficas, gerados sempre pelo titular, que terá acesso exclusivo a sua chave privada, sendo o titular responsável pelo controle, uso e conhecimento.

2. Cite algumas funções da autoridade certificadora.

Resposta: A autoridade certificadora tem como funções a emissão, expedição, distribuição, revogação e gerenciamento dos certificados, assim como disponibiliza uma lista de certificados revogados aos usuários, além de manter registro de todas as operações.

3. Cite pelo menos duas autoridades certificadoras do Brasil.

Resposta: Presidência da República, Receita Federal, SERPRO, Caixa Econômica Federal, Serasa, CertiSign, nelas você poderá solicitar seu Certificado Digital.

4. Explique como ocorre o processo de autenticação.

Resposta: O processo de autenticação ocorre quando os usuários sabem que estão acessando as informações desejadas do servidor correto, que os dados enviados chegaram ao destino e não sofreram mudanças, assim como que somente o receptor poderá ler as informações. Em contrapartida, o servidor precisa garantir que está se comunicando com o usuário certo e o conteúdo da mensagem e a identidade do emissor estão corretos também.

5. Porque o Firewall é importante em uma empresa?

Resposta: Porque é um obstáculo entre uma rede privada e uma rede externa, impedindo ou permitindo o tráfego de dados obedecendo regras predefinidas pela gerência de TI da organização. Dessa forma, deixará a rede de computadores da empresa mais segura.

6. Cite os tipos de firewall.

Resposta: Filtro de Pacotes (Packet Filtering), Filtro de Pacotes com base no Estado da Conexão (Stateful Inspection), Filtro de Pacotes na Camada de Aplicação (Application Proxy)

7. Quanto à localização do firewall em uma rede, cite o modelo mais eficiente, segundo Marçula & Benini Filho.

Resposta: O Basic Border Firewall é considerado o mais eficiente, por ser um único computador interconectado à rede interna da empresa e a alguma rede não confiável em termos de segurança (normalmente a Internet).

8. Com relação às topologias de Firewall, relacione a primeira coluna, que contém os tipos de firewall com a segunda coluna, contendo as definições de cada modelo.

A) Dual Firewall	(B)	é o ponto de partida de todos os sistemas de firewall. É um único computador interconectado à rede interna da empresa e a alguma rede não confiável em termos de segurança (normalmente a Internet).
B) Basic Border Firewall	(C)	nesse modelo, o servidor não confiável é conectado ao firewall. Apesar disso, ele continua em sua própria rede, ou seja, o firewall conecta, agora, três redes diferentes. Isso aumenta a segurança, confiabilidade e disponibilidade apenas do servidor não confiável, e não de toda a rede à qual está conectado.
C) DMZ Network	(A)	a rede privada da empresa é ainda mais isolada da rede não confiável pelo acréscimo de mais um firewall.
D) Untrustworth host (servidor não confiável)	(D)	parecida com a topologia anterior com o acréscimo de um servidor que está conectado a uma rede não confiável, na qual o firewall não pode protegê-lo. Esse servidor é configurado com o mínimo de segurança, desse modo o firewall passa a controlar o tráfego de entrada e saída a partir desse servidor.

9. Porque o firewall é importante em uma empresa? Explique.

Resposta: Porque é a barreira entre o mundo externo – Internet e a empresa, dessa forma, tudo que entra e sai da empresa pode ser monitorado. Dessa forma, nada entrará ou sairá sem que esteja devidamente autorizado.

Aula 6

1. O que deve conter a elaboração de uma política de segurança da informação?

Resposta: Os objetivos bem claros, um texto de apresentação da gerência colocando-se favorável sobre a implantação dessa política de segurança, apresentação das exigências de forma detalhada que deverão ser obedecidas, além disso, é importante também, definir as responsabilidades gerais e específicas pela gestão da segurança das informações, juntamente com relatórios de incidentes.

2. Qual a importância de se implantar uma política de segurança da informação na empresa?

Resposta: A política de segurança da informação é um documento valiosíssimo, pois evitará perdas de dados e/ou interrupção dos serviços de informação, dessa forma favorecerá expansão dos negócios, auxiliando na obtenção de maiores lucros, novas perspectivas de negócios e garantindo a sobrevivência dessas organizações.

3. Apresente algumas características para implantação de uma política de segurança da informação.

Resposta: Algumas características que podemos apresentar estão relacionadas à abrangência de atuação nas normas e regulamentos aos quais estará subordinada, nomear um grupo e/ou indivíduo para sancionar, implementar e fiscalizar o cumprimento da política, definir a periodicidade de revisão e adequação caso necessário, definir as permissões e restrições de acordo com as atribuições de cada funcionário.

4. Explique qual deve ser a postura da alta administração em uma organização frente à política de segurança da informação.

Resposta: A gerência deve apoiar a implantação e execução da política de segurança da informação, pois agindo dessa forma, os mesmos estarão endossando as diretrizes estabelecidas.

5. O que você entende por Plano de Contingência?

Resposta: É um documento formal elaborado a partir de uma análise de risco de desastre, no qual estabelecem-se os procedimentos para agir caso ocorra anormalidade.

6. Relacione a primeira coluna com a segunda coluna, que possui as devidas definições.

A) Warm-site	(C)	Visa desviar a atividade atingida pelo evento que provocou a quebra da segurança, para outro ambiente físico, equipamento ou link, pertencentes à mesma empresa.
B) Acordo de reciprocidade	(A)	Aplicada em objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade.
C) Realocação de operação	(B)	Esta estratégia propõe a aproximação e um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes à sua, e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional.
D) Cold-site	(E)	Estratégia pronta para entrar em ação imediatamente. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto.
E) Hot-site	(D)	Propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, desprovido de recursos de processamento de dados.

7. De que forma uma política de segurança poderá ser recusada pelos funcionários em uma organização?

Resposta: poderá ser recusada quando é muito extensa, contendo muitos detalhes, dificultando o entendimento claro das diretrizes, quando se abrem exceções de algumas regras para pessoas ou grupos específicos.

8. Porque é importante a criação de um plano de recuperação de desastre?

Resposta: Um plano de recuperação de desastre se justifica pela necessidade

de assegurar a continuidade dos negócios, propiciando a redução de riscos e eliminação das vulnerabilidades.

9. Quando abordamos políticas de classificação de dados, elas foram divididas em categorias segundo os autores Mitnik e Simon. Cite-as e defina-as.

Resposta: confidencial - na qual as informações são compartilhadas a um número restrito de pessoas, particular – destinam-se apenas ao uso na organização para fins burocráticos, modelo interno - as informações são liberadas para os funcionários e pública - as informações podem ser liberadas externamente.

Aula 7

1. Uma aplicação deve assegurar a consistência dos dados introduzidos, para isso, algumas medidas de segurança devem ser tomadas durante seu desenvolvimento , a Norma ISO/IEC 15408 apresenta quatro níveis de garantia de segurança (EAL – Evaluation Assurance Level). Cite e explique cada uma delas.

Resposta:

Nível 1 - tem por função testar a funcionalidade do sistema, pois visa atender os requisitos solicitados e identificar as proteções necessárias contra ameaças, além disso, deve haver avaliação na versão final, comparando com os requisitos iniciais sem o auxílio do desenvolvedor.

Nível 2 - tem por função garantir que as aplicações desenvolvidas estejam atendendo aos padrões preestabelecidos, além disso, que seja realizada uma análise para verificar as vulnerabilidades do sistema e aplicar testes para observar a segurança e validação dos dados.

Nível 3 - visa a aplicação de procedimentos de segurança, sem que o sistema sofra com mudanças, além de propiciar testes completos do sistema sem precisar da reengenharia.

Nível 4 - objetiva garantir maior segurança durante o desenvolvimento do sistema, aplicando alguns procedimentos de teste e verificação dos resultados.

2. Aponte uma característica que retrate um ambiente de desenvolvimento seguro.

Resposta: deve haver uma proteção lógica dos servidores, divisão entre ambiente de desenvolvimento, teste e construção, é importante que a equipe de desenvolvimento siga as especificações de segurança para evitar falhas.

3. Como devem ser as regras para manter um ambiente de desenvolvimento seguro?

Resposta: As regras devem ser de fácil entendimento, que seja de conhecimento de todos em uma empresa, que tenha alguém responsável por manter vivo na empresa, avaliar periodicamente e adaptar às novas necessidades.

4. A Norma ISO/IEC 15408 propõe um modelo de segurança no ambiente de desenvolvimento a partir de algumas etapas. Cite-as.

Resposta: Gerência de configuração, distribuição, desenvolvimento, documentação, suporte ao ciclo de vida, teste de segurança e avaliação de vulnerabilidades.

5. Gerência de configuração é uma etapa sugerida pela Norma ISO/IEC 15408 para resguardar uma aplicação durante seu desenvolvimento. Qual a função desta etapa?

Resposta: Tem por função prevenir modificações, inserções e deleções sem autorização na documentação do sistema de forma a auxiliar no processo de desenvolvimento menos frágil a erros ou negligência humana.

6. Quando se desenvolve uma aplicação, devemos nos preocupar em elaborar a documentação para posteriores usos. Porque devemos registrar as ações efetuadas durante o processo de desenvolvimento?

Resposta: é uma das etapas da garantia da segurança da informação da aplicação, a documentação torna-se útil quando se vai fazer uma modificação, inserção ou exclusão de rotinas, quando se quer comprovar os requisitos definidos, para evitar mal-entendidos na leitura do código ou mesmo usar o código erroneamente.

7. Garantir a segurança de uma aplicação durante seu desenvolvimento reduz a performance da aplicação. Explique porque esse fator não deve ser considerado um problema.

Resposta: Porque pode ser facilmente solucionado com investimentos em hardware, aquisição de equipamentos mais rápidos para suprir essa necessidade.

8. Especifique as normas e práticas de uma boa programação conforme determinado no site do SERPRO

Resposta: Funções intrinsecamente seguras; verificar códigos de erro retornado por função ou método, atentar para tamanho de buffers e arrays do sistema, documentar o código.

9. Porque devemos ter cuidados especiais durante o processo de desenvolvimento de uma aplicação? Explique.

Resposta: Para evitar que os processos sejam fraudados e manipulados posteriormente por alguém, pertencente ou não à empresa, que queira se beneficiar das vulnerabilidades criadas durante o processo de desenvolvimento da aplicação.

10. Com relação à segurança no ciclo de vida de desenvolvimento da aplicação, temos algumas etapas sugeridas pelo SERPRO. Você deve relacionar a primeira coluna de acordo a definição na segunda coluna.

A) Atentar para tamanho de buffers e arrays do sistema.	(B)	Sempre que fizer uma chamada da função, a mesma deve ser testada, dessa forma, caso o resultado não esteja atendendo os requisitos estabelecidos durante o processo de desenvolvimento, o dado gerado deve ser desconsiderado.
B) Verificar códigos de erro retornado por função ou método	(C)	É fazer uso de linguagem que apresenta flexibilidade de programação, na qual o programador poderá criar funções ou mesmo fazer usos de funções que proporcionam essa segurança.

C) Funções intrinsecamente seguras	(A)	O ideal seria sempre operar o sistema de acordo com as permissões requeridas para executar suas tarefas de forma adequada, pois um erro de buffers ou arrays poderia comprometer o desempenho da aplicação.
D) Documentar o código	(D)	Documentar corretamente todo o código, para evitar mal-entendidos na leitura do código ou mesmo usar o código erroneamente.

Aula 8

1. O que você entende por auditoria? Explique.

Resposta: É um conjunto de atividades para levantar, estudar e avaliar de forma sistemática os processos de uma empresa, buscando comprovar os eventos realizados nos negócios, dessa forma, é possível identificar vulnerabilidades e falhas.

2. Porque a auditoria de sistemas de informação não é padronizada? Explique

Resposta: Ainda não há padrões específicos para auditar um sistema de informação, esse tipo de auditoria é reconhecido como uma parte de uma auditoria normal.

3. O Comitê de Padrões da Associação de Controle e Auditoria de Tecnologia da Informação e a Associação de Auditores de Sistemas & Controles (ISACA), sugeriram algumas etapas para execução de uma auditoria, cite duas que você considera mais importantes em uma auditoria e justifique sua escolha.

Resposta: Planejamento e a Ética profissional e padrões. Todas as etapas são importantes no processo de auditoria, contudo, as duas citadas são a base para fazer uma auditoria completa e satisfatória, pois a etapa de planejamento procura delinear todas as atividades a serem tratadas, pois sem um planejamento prévio a auditoria poderá conter falhas e a etapa Ética profissional e padrões, diz respeito à postura do profissional frente às informações levantadas na organização, uma vez que todo profissional deve assumir uma postura de caráter inquestionável.

4. Com relação à abordagem através do computador, marque a alternativa incorreta.

a) Método de auditoria mais antigo.

b) A auditoria era feita a partir dos dados que entravam e saiam da máquina, o processamento eletrônico de dados não era considerado para auditar.

c) A qualidade da auditoria realizada com esse modelo era questionado, pois não havia parâmetros claros e padronizados que os resultados obtidos fossem os mesmos esperados.

d) Com uso desse modelo, era possível fazer a verificação dos resultados calculados.

A resposta correta é a alternativa D

5. Dos três modelos apresentados de auditoria, qual o mais eficaz? Justifique.

Resposta: Abordagem com o computador. Apresenta algumas facilidades, como a possibilidade de desenvolver aplicações específicas para atender uma necessidade de auditoria, além da redução de tempo frente ao uso de aplicações generalizadas de auditoria.

6. Relacione a primeira coluna de conceitos de acordo com as definições existentes na segunda coluna.

A) Avaliação da equipe	(B)	Auxilia na orientação das atividades a serem realizadas e deve ser caracterizado para evitar qualquer atividade inesperada na empresa.
B) Planejamento	(C)	Para esta etapa, já deve haver um encarregado para programar os trabalhos a serem realizados pela equipe.
C) Programar a equipe	(A)	Ao término de cada auditoria, deve-se avaliar o desempenho da equipe, observando os pontos fracos e fortes do auditor, elogiando quando apresentar eficiência e eficácia e auxiliando-o no desenvolvimento de planos para superar as fraquezas e se torne um profissional qualificado e consciente.

D) Execução de trabalhos e supervisão	(E)	O perfil básico da equipe de auditoria de TI depende dos negócios que a empresa atua, isso já deve estar bem detalhado no planejamento.
E) Escolher a equipe	(D)	Durante uma auditoria, deve-se garantir a qualidade e certificar que as tarefas foram adequadamente feitas, isso implica, na formação do profissional que fará parte da equipe.

Referências

ALVES, Gustavo Alberto. **Segurança da Informação:** uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006.

BRASIL .Ministério da Integração. **Plano de Contingência**. Disponível em: < http://www.mi.gov.br/orientacoes-para-elaboracao-de-um-plano-de-contingencia> Acesso em: 09 set. 2013

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE. INCIDENTES DE SEGURANÇA NO BRASIL – Cert.br. **Cartilha de Segurança para internet.** Disponível em:< http://cartilha.cert.br/glossario> Acesso em: 30 dez. 2012.

_____ – Cert.br. **Práticas de Segurança para Administradores de Redes Internet**. Disponível em:< http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf. > Acesso em: 18 jan. 2013.

DICIONARIO ONLINE DE PORTUGUES. **Significado de paradigma**.Disponível em:< http://www.dicio.com.br/paradigma/> Acesso em; 09 set. 2013.

_____. **Significado de sinergia**. Disponível em: <http://www.dicio.com.brsinergia/> Acesso em: 09 set. 2013

FERREIRA, Fernando N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna. 2003.

FONTES, Edson. **Segurança da Informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação**. São Paulo: Atlas, 2005.

INFORMA BR. Segurança da informação. **Norma ISO/IEC 17799:2000**. Disponível em:< http://www.informabr.com.br/nbr.htm> Acesso em 09 set. 2013

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO .**Infraestrutura de Chaves Públicas Brasileira**. Disponível em:< http://www.iti.gov.br/index.php/icp-brasil/o-que-e> Acesso em: 10 Mai 2013.

_____ **Certificação Digital**. Disponível em:< http://www.iti.gov.br/certificacao-digital> Acesso em : 12 ag. 2013

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

MARÇULA, Marcelo & BENINI FILHO, Pio Armando. **Informática:** conceitos e aplicações. 2 ed. São Paulo: Érica. 2007.

MELO, Araujo Daniel. **Segurança no Desenvolvimento**. Disponível em: < http://www.softwarelivre.serpro.gov.br/recife/download-plaestras/Apresentacao%20Seguranca%20Desenvolvimento.pdf> Acesso em: 09 set. 2013

MITNICK, Kevin D. & SIMONS, William L. **A Arte de Enganar:** ataques de hacker – controlando o fator humano na segurança da informação. São Paulo: Pearson Education. 2003.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma visão executiva. Rio de Janeiro: Campus.2003.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **Certificação Digital**. Disponível em: < https://ccd.serpro.gov.br/egba/docs/perguntas.htm#0> Acesso em: 14 jan.2013.

SISP. Sistema de Administração dos Recursos de Tecnologia da Informação. **Política de Segurança da Informação e da Comunicação**. Disponível em: <http://www.sisp.gov.br/faq_segurancainformacao/one-faq?faq_id=13971979> Acesso em: 12 ag. 2013.

TRIBUNAL DE CONTAS DO DISTRITO FEDERAL. **Manual de Auditoria** . Disponível em: < http://www.tc.df.gov.br/app/biblioteca/pdf/PE500418.pd> . Acesso em: 27 jan. 2013

Obras Consultadas

LIMA, Sandro. **Hackers continuam a atacar sites do governo**. Disponível em: <http://g1.globo.com/politica/noticia/2011/06/hackers-continuam-atacar-sites-do-governo-diz-serpro.html > Acesso em: 12 ag.2013.

LOBO, Ana Paula. **TCU detecta falhas no ERP e na segurança da informação dos Correios**. Disponível em:< http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31263&sid=11.> Acesso em: 12 ag. 2013.

MARCEL, Diego. **Computação em Nuvem cresce no Brasil, mas requer cuidados.** Disponível em: <http://www.istoedinheiro.com.br/noticias/105604_COMPUTACAO+EM+NUVEM+CRESCE+NO+BRASIL+MAS+REQUER+CUIDADOS>. Acesso em: 12 ag. 2013.

Currículo da Professora-autora

Bacharel em Ciência da Computação pela Universidade de Mogi das Cruzes (UMC) desde 2005. Especialista em Metodologia do Ensino Superior pela Universidade Federal de Rondônia (UNIR), Novas Tecnologias na Educação, pela Escola Superior Aberta do Brasil (ESAB), Informática em Saúde, pela Universidade Federal de São Paulo (UNIFESP). Atua como professora de Multimídias Integradas na Rede Pública do Estado de Rondônia (SEDUC) e na Faculdade de Tecnologia – FATEC de Porto Velho – RO, nas áreas de segurança da informação e projeto multimídia.