SISTEMAS DE INFORMAÇÃO

Glauber Rogério Barbieri Gonçalves

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS

Revisão técnica:

Jeferson Faleiro Leon
Graduado em Desenvolvimento de Sistemas
Especialista em Formação Pedagógica

G643s Gonçalves, Glauber Rogério Barbieri
Sistemas de informação [recurso eletrônico] / Glauber Rogério Barbieri Gonçalves ; [revisão técnica: Jeferson Faleiro Leon]. – Porto Alegre : SAGAH, 2017.

ISBN 978-85-9502-227-0

1. Computação. 2. Sistemas de Informação. I. Título.

CDU 004.78

Catalogação na publicação: Ana Paula M. Magnus – CRB 10/2052

Segurança em TI, crimes, conformidade e continuidade I

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer o impacto na organização de problemas relacionados à segurança da informação.
- Diferenciar os principais termos utilizados na área de segurança da informação.
- Identificar os tipos de ameaças mais comuns à segurança da informação.

Introdução

Antigamente, se você tivesse algumas moedas de ouro, você as colocava em um saco de couro, escolhia um local e as enterrava, marcava o local e pronto, seu tesouro estava seguro. A informação é um precioso ativo da empresa. Quando ela era física, no formato de papel, ainda se conseguia colocar em uma gaveta com chave, fechar e a informação estava segura.

Hoje em dia, com a velocidade em que as informações cresceram, percebemos que seu volume não cabe mais em uma gaveta e, com o advento das melhorias no setor de tecnologia da informação (TI) elas podem e são compartilhadas das mais variadas formas.

Nesse contexto, surgiu a preocupação em como guardar esse bem, uma vez que a conectividade apresenta uma complexidade para que essa tarefa seja bem-feita, tanto para as pessoas físicas como para as empresas. Assim, os sistemas de informação adquirem enorme importância para as organizações, pois são a chave para o sucesso e sobrevivência, devendo ser seguros e protegidos.

Neste texto, você irá estudar como as situações envolvendo a segurança da informação podem afetar negativamente as organizações,

além de analisar como as tecnologias podem auxiliar no planejamento e na construção de um ambiente digital realmente seguro e confiável.

Sistemas de segurança

Os sistemas de segurança evoluíram juntamente a produção da informação pelo homem. Do ponto de vista histórico podemos verificar a existências de relatos de informação e forma para proteger essas informações, que foram passadas de geração em geração.

Veja os seguintes exemplos: o homem pré-histórico, 2000 anos antes de Cristo, se expressava na forma de pinturas em cavernas; posteriormente, para gravar a evolução, haviam os registros em hieróglifos e o papiro, no antigo Egito (3000 AC); os ábacos babilônicos (1800 AC); a produção de papel pelos chineses em 105 DC; as fotografias em 1826; o telégrafo em 1837; e o primeiro computador digital em 1943.

Perceba que, com o passar do tempo, as mudanças ficam cada vez mais curtas, e a necessidade de armazenar e proteger a informação também acompanha essa evolução. Note, ainda, que esse fluxo de informações deve ser protegido, se ele for interrompido ou capturado, pode gerar grandes impactos para pessoas, empresas ou até mesmo povos. Na vertente militar ao longo dos anos existem inúmeros exemplos de que se a informação não tem a segurança necessária e pode ser capturada por adversários e mudar os rumos de batalhas ou guerras.

Para as empresas, atualmente, é necessário que as preocupações sobre escolhas de sistemas de segurança de informações estejam contidas no planejamento estratégico, para que assim fiquem adequadas aos objetivos da empresa, ver Figura 1.

Figura 1. Sistemas de segurança.
Fonte: Alerta Security (2016a).

Para gerenciar, primeiro conhecemos, depois, analisamos, implantamos e administramos o assunto, seguindo assim uma sequência lógica. A importância disso está relacionada ao fato de que os ataques a informação têm crescido nos últimos anos, ocasionando consideráveis prejuízos, por exemplo, ataques do tipo **Denial of Service (DoS)** (negação de serviço) que ocorrem quando um site recebe um grande número de solicitações, além de sua capacidade, fazendo com que ele falhe e não disponibilize as informações aos usuários.

Uma forma de evidenciar esse conceito é utilizando o ciclo planejar, desenvolver, controlar e agir (PDCA, em inglês *plan*, *do*, *check*, *act*), encontrado na literatura da qualidade. Veja o Quadro1, que apresenta um resumo da ferramenta e dessa sequência.

Quadro 1. PDCA.

Planejar	Nesta fase a empresa deve conhecer suas estruturas e informações, realizando uma análise para que, assim, possa dimensionar os sistemas de segurança capazes de dar o suporte necessário as suas atividades com segurança e confiança. Aqui serão identificados os riscos (probabilidade de uma ameaça explorar uma vulnerabilidade) e as ameaças (situação em que alguém ou algo poderá causar danos a um ou vários usuários dentro da organização).
Desenvolver	Nesta fase a empresa realiza a implementação dos atributos de segurança necessários a manter a informação ao alcance de todos os envolvidos no processo, realizando essa implementação nos equipamentos e sistemas de acesso e execução de programas para o desenvolvimento das atividades afins na empresa, como a utilização de contramedidas (recursos de segurança adotados para reduzir os riscos).
Controlar	Nesta fase a empresa controla a utilização e acessos às informações para a verificação das boas práticas e se essas rotinas estão sendo utilizadas para o crescimento da organização.
Agir	Nesta fase a empresa realiza ações de melhorias nos processos ou correções, para que cada vez mais a segurança da informação tenha aderência aos processos da organização.

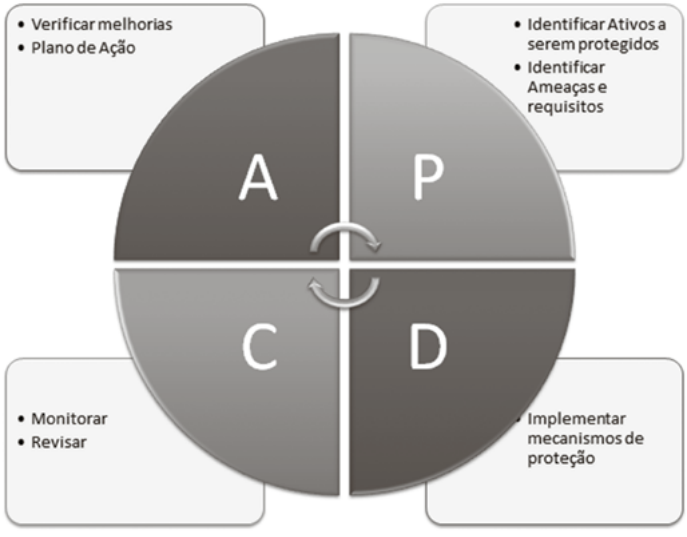

Figura 2. Ciclo PDCA.

Conhecendo a segurança da informação

A segurança da informação tem como meta a proteção da informação, seja ela impressa ou eletrônica, bem como os meios de armazenamento e utilização, por exemplo, os usuários que acessam esses equipamentos. Não basta proteger só os equipamentos se, por exemplo, os usuários liberarem informações sem as devidas permissões a pessoas fora do processo. A segurança da informação está diretamente relacionada com os riscos aos dados, aos sistemas de informação e as redes de comunicação.

Devem ser tomadas medidas para minimizar o comprometimento do vazamento das informações, por exemplo os acessos indevidos e a eliminação da informação de banco de dados. Geralmente, a segurança teve ser reforçada aos próprios funcionários das organizações, pois os maiores riscos e incidentes poder ser causados dentro da empresa.

Tratando as informações como ativos, as empresas irão preservar as informações, para isso, utilizarão os princípios da integridade, confidencialidade e disponibilidade, como você pode ver na Figura 3.

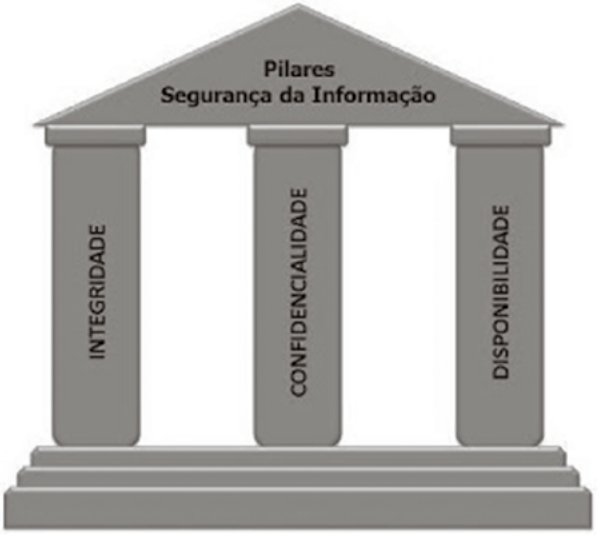

Figura 3. Pilares da segurança da informação.
Fonte: Tenca (2009).

Integridade

Integridade vem do latim *integritate*, que significa a qualidade de alguém ou algo de ser íntegro, de conduta reta, pessoa de honra, ética, educada, cuja natureza de ação nos dá uma imagem de inocência, pureza ou castidade, o que é íntegro, é justo e perfeito. Em segurança da informação, integridade significa ter a disponibilidade de informações confiáveis, corretas e dispostas em formato compatível com o de utilização.

Nesse pilar será garantido o princípio de que a informação não foi alterada de forma não autorizada, ficando, portanto, íntegra. Sendo assim, a organização terá a confiança de que suas informações não foram alteradas de maneira não autorizada ou indevida. A utilização da informação íntegra permitirá que a organização adquira conhecimento empresarial baseado na perfeita comunicação entre receptor e emissor. Se em algum momento houver uma alteração não autorizada, haverá um dano a integridade, e essa informação vai prejudicar as tomadas de decisões, ocasionando perdas para a empresa.

Dos vários aspectos que podem caracterizar a perda da integridade, dois são mais citados: as alterações do conteúdo dos documentos, quando alguém

realiza inserções, substituições ou exclusão de conteúdo ou parte dele; e as alterações nos elementos que oferecem suporte à informação, ou seja, quando há alterações na estrutura física e lógica (dados e rede) em que a informação está armazenada.

Proteger a integridade é proteger a informação, tanto nos agentes da comunicação como nos equipamentos de armazenagem, buscando assegurar o acesso correto dos sistemas e pessoas para visualizações das informações, realizar alterações autorizadas e somente utilizar as informações em prol do desenvolvimento de conhecimento empresarial aliado aos objetivos da empresa.

Confidencialidade

Confidencialidade é a qualidade daquilo que é confidencial (que se diz ou que se faz com confiança e com segurança recíproca entre dois ou mais indivíduos). Para a segurança da informação, confidencialidade é a propriedade da informação que não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização. Em outras palavras, confidencialidade é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

Nesse pilar, o grande objetivo é garantir que somente os sistemas e as pessoas que devem acessar a informação o façam, ou seja, a confidencialidade garante que a informação será utilizada somente por pessoas autorizadas e que têm acesso a ela.

Na empresa, uma ou várias pessoas necessitam, por exemplo, de uma determinada informação para realizar um processo ou fazer algum planejamento, mas essa informação não é necessária para as demais. Um claro exemplo é o custo de aquisição de uma determinada mercadoria que será posta à venda, essa informação é fundamental para o comprador adquirir e para o gestor determinar o preço de venda, mas não é importante para o segurança da empresa ou para o técnico em TI que realiza atividades de atualização do site da empresa.

Obter a confidencialidade significa dizer que o processo de comunicação da informação tem a segurança de que o que foi escrito ou dito por alguém, será recebido, lido ou escutado por quem tiver autorização. A perda de confidencialidade significa perda de segredo e pode ocasionar grandes danos em uma organização. Imagine que um produto a ser lançado é descoberto por um concorrente, ele pode melhorar algum processo e lançar o produto antes da empresa que criou o produto inicialmente, ocasionando, com isso, perdas financeiras em tempo e matérias-primas utilizadas.

Fique atento

A proteção à confidencialidade atualmente é um dos mais complexos desafios organizacionais, pois tem que garantir desde a emissão até a recepção dessa informação, passando pelos agentes e mecanismos utilizados pela empresa no processo.

Uma das formas que as organizações utilizam é a criação de níveis de confidencialidade para as informações que circulam na empresa, por exemplo, ter informações de acesso a todos, informações de acesso a setores e informações de acesso somente da direção da empresa. Dessa forma, quanto maior for o grau de confidencialidade, maior será o nível de segurança necessário para a proteção da informação. Chamamos esse processo de categorizar a informação quanto ao grau de sigilo que ela contém.

Grau de sigilo é uma graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem permissões de acesso à informação. Em geral, no mercado, os graus de sigilo aparecem da seguinte forma: confidencial, restrito, sigiloso e público.

Disponibilidade

O conceito de **disponibilidade** é utilizado em diversas áreas e esferas para fazer referência à possibilidade de que algo, um produto ou serviço, esteja disponível de ser realizado, encontrado ou utilizado. Para a segurança da informação, significa que a informação deve ficar disponível ao uso para quem tem autorização.

Neste pilar, devem ser garantidos os fundamentos de que a informação tem que estar disponível no momento em que se precisa dela. Sendo assim, os recursos tecnológicos utilizados para o acesso e armazenamento devem estar em bom funcionamento e, em caso de incidentes, serem recuperados rapidamente. Assim, o usuário ou o grupo de usuários que necessita da informação terá a garantia de a obter na hora em que precisar para seu trabalho.

A informação adquire permissões à utilização no tempo certo, alcance de todos os envolvidos e acesso quando necessário.

A disponibilidade passa por um bom planejamento em infraestruturas, permitindo a continuidade dos negócios sem prejuízos ao alcance dos objetivos organizacionais. Por exemplo, devem ser garantidos os acessos a informações confidenciais em reuniões de planejamento. Uma empresa não pode parar se

o banco de dados não puder ser acessado na realização dessa reunião ou se as informações foram perdidas por um incêndio nas instalações dos equipamentos de redes.

Partindo desse princípio, a disponibilidade deve ser protegida por meio das várias formas de proteção, como cuidados nas configurações para o trânsito das informações nas comunicações empresariais e cópias de segurança (Backups) nos dados armazenados.

Mecanismos de segurança são medidas que visam controlar o acesso às informações de forma física e lógica. Enquanto os controles físicos limitam o contato direto que um usuário pode ter com a informação e toda a estrutura que a envolve, os controles lógicos trabalham pela integridade da informação de modo que ela não seja acessada e manipulada. Alguns exemplos de mecanismos de segurança são (ALERTA SECURITY, 2016b):

- **Criptografia:** um conhecido meio de converter os dados em um formato que seja impossível decifrá-lo. Imagine que para assegurar que os dados, em idioma português, não sejam compreendidos por meros falantes da língua, as informações sejam convertidas para o hebraico. O raciocínio é muito similar a isso, porém, criptografar é impedir completamente a interpretação das informações, e elas só voltam ao estado inteligível quando uma chave (senha) for inserida.
- **Assinatura digital:** com a assinatura digital é garantida a integridade dos dados por meio de criptografia, ou seja, seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado.
- **Certificação:** uma certificação é como um atestado de autenticidade de um arquivo, uma garantia de que o mesmo é válido.
- ***Honeypot*:** trata-se de um software que age como um antivírus em tempo real, cuja função é proteger os dados de invasores, aplicações maliciosas e estranhas ao sistema. A diferença é que, em vez de mantê-lo em quarentena, por exemplo, o *honeyspot* ludibria esse invasor, fazendo-o acreditar que está tendo acesso real às informações.

Crimes em informática

Os crimes em informática estão crescendo muito, tanto pelo desconhecimento como pelo aumento de usuários na rede. As informações são preciosas para seu autor seja ele uma pessoa física ou uma organização que necessita de suas informações para planejamentos ou para rodar seus processos diariamente.

Há muito tempo, as organizações procuram manter seus segredos industriais fora do alcance de curiosos ou concorrentes. Um caso clássico é a fórmula do refrigerante de cola mais famoso do mundo, a Coca-Cola. No âmbito da TI, um crime muito presente nos dias de hoje, chama-se pirataria de *software*.

Figura 4. Pirataria.
Fonte: Universidade Federal do Sul e Sudeste do Pará (2016).

No Quadro 2, você verá as modalidades desse crime, citados na Lei nº 9.609/1998 (BRASIL, 1998), que estabelece que a violação de direitos autorais de programas de computador é crime, punível com pena de detenção de 6 meses a 4 anos e multa, além de ser passível de ação cível indenizatória.

Quadro 2. Crimes de informática.

Crimes de falsificação	Trata-se de cópia de um software protegido por direitos autorais que é imitado em sua embalagem, etiqueta e demais informações, com visual muito próximo ao original para sua comercialização.
CDROM pirata	Também é um caso de falsificação, só que neste caso o usuário já sabe que está adquirindo uma cópia ilegal do que está procurando, por exemplo, um programa, um filme ou uma música, é encontrado normalmente em pontos de comércio popular, feito em uma mídia regravável, com valor bem abaixo do normal. Em uma única mídia é possível encontrar uma coletânea de mais de um original, por exemplo, todos os lançamentos de um músico.
Revendas de *hardware*	Acontece quando uma empresa ou pessoa vende um computador, seja em uma loja física ou virtual e entrega esse hardware com algum programa instalado pirata ou afirmando ser original, mas sem oferecer ao usuário a licença original ou a documentação técnica. Por exemplo, você compra um notebook já com o programa operacional instalado e não se preocupa em verificar se esse programa foi devidamente licenciado.
Pirataria individual	Ocorre quando uma pessoa, por amizade ou por não entender a gravidade do ato, oferta programas que comprou a colegas ou amigos, ela tem a licença de uso individual, mas realizando esse ato de compartilhar acaba por criar um problema grande não percebendo a gravidade e dimensão que isso pode ocasionar.
Pirataria corporativa	Parte do mesmo princípio da pirataria individual, ocorrendo em progressão geométrica. Imagine em uma empresa, ela compra licença de uso para um computador e instala nos outros 199 que possui. Nesse tipo de pirataria estão concentradas as maiores perdas do setor de software, pois são muitos hardwares funcionando com licenças copiadas. De fato, não são todas as organizações que cometem esse delito, há muitas que tem um rígido controle sobre o uso e adquirem corretamente as licenças para uso de programas.
Pirataria cliente/ servidor	Geralmente ocorre quando uma empresa entra em rede, ou seja, deixa de operar com estações separadas e utiliza um servidor com estações ligadas em rede. Nesse processo pode que ter, mesmo sem saber (quando faz o serviço com terceiros), instaladas cópias piratas ou acessos ilegais a programas compartilhados com um limite maior do que a licença permite, sendo essa prática um crime.
Pirataria *on-line*	Atualmente não há como ficar desconectado, seja em casa ou nos ambientes coorporativos. Com esse advento, a pirataria on-line vem crescendo na mesma proporção, os software são transferidos e instalados ilegalmente e anonimamente.

Fonte: Brasil (1998).

Fique atento

Software são obras intelectuais, e não um produto. Quando adquirimos um software, estamos adquirindo a licença de uso, portanto, quem compra uma cópia pirata está tão sujeito a punições quanto quem comercializa.

Não devemos discutir o valor de cada software, mas sim procurar realizar nossas ações baseadas na ética e na moral, pois esse tipo de crime é muito cultural e deve ser combatido.

Para as empresas, cabe ao empresário responder por qualquer irregularidade que ocorra dentro de sua organização. Mesmo que ele não tenha incentivado a instalação de algum software, é responsável pelo monitoramento de suas estações de trabalho e de praticar ações preventivas e orientações a respeito do tema.

O caminho a percorrer é longo, por tratar-se de um problema cultural, por isso, as empresas estão cada vez mais criando e executando políticas bem claras sobre o tema, com objetivo de minimizar os prejuízos que podem aparecer com esse tipo de crime. Não basta só o amparo legal, é preciso haver uma conscientização coletiva para minimizar os impactos negativos que a pirataria causa.

Lembre-se que qualquer pessoa envolvida com a prática ilícita (pirataria) está sujeita a punições que variam de 6 meses a 2 anos de detenção, além do pagamento de indenizações.

Os sistemas de informação estão sempre sujeitos a sofrerem ameaças, tanto internamente como externamente. Essas tentativas podem ser, como vimos, intencionais, mas também podem não ser intencionais, como uma codificação errada de uma funcionalidade do software por um entendimento incorreto do profissional (programador). É necessário separar esses dois tipos de ameaças.

Saiba mais

O presidente do Fórum Nacional Contra a Pirataria e Ilegalidade (FCNP), Edson Vismona, informou que, em 2015, o Brasil teve perdas da ordem de R$ 115,603 bilhões em **piratarias**, **contrabando** e **sonegações**. O montante contabiliza perdas de setores como vestuário, cigarros e TV por assinatura. Segundo ele "[...] acredito que pode ter sido muito mais, já que não há setores nessa conta, como o automobilístico, por exemplo." (ESTADÃO CONTEÚDO, 2016).

Insegurança na internet

A rede de computadores veio para o auxiliar a disseminação da informação e o acesso mais democrático delas pelas pessoas e empresas que antes não podiam ter acesso. Assim, além dos benefícios vieram também os malefícios da modernidade.

Dentre os fatores que contribuem para a insegurança no acesso, aparece a falta de conhecimento, por parte da maioria dos usuários; o anonimato, que protege os maus usuários; os criminosos; e a pouca disseminação e a própria falta de interesse na segurança por parte do usuário, que acaba por terceirizar a preocupação com segurança a seu provedor de internet. Você deve lembrar que o assunto segurança é de responsabilidade de todos, por exemplo, quando você dirige um carro na preferencial, entende que tem a preferência e, caso ocorra uma colisão, você estará certo e a outra pessoa errada, isso é fato, mas o inconivente de ficar sem carro ou um período até que seja concertado é seu.

Todos estão expostos a um inconveniente, portanto, o melhor é prevenir. Na TI, o nome do criminoso é conhecido como hackers, que são usuários que focam suas ações em praticar atos contra pessoas ou empresas com objetivos próprios e seu favor, sejam por poder ou financeiros.

São muitos os motivos que levam esses criminosos a agir, entre eles:

- **Espionagem:** podem ser militares, de estado ou em empresas industriais, podem ser contratados por concorrentes ou inimigos para roubar ou destruir os dados de outros.
- **Proveito próprio:** quando o ataque objetiva obter proveitos próprios, muitas vezes financeiros, por exemplo: transferências de numerário, resultados de concursos, uso de redes de telefonia ou dados sem os encargos.
- **Vingança:** pessoas comuns, empresas ou até mesmo outro criminoso, pode até ser realizado por um não hacker, pode ser um ex-funcionário que está descontente com a antiga empresa, ou um ex-namorado que sai de um relacionamento e quer prejudicar a outra parte.
- **Status, poder, necessidade de aceitação:** há nitidamente uma concorrência entre esses criminosos, eles querem sempre superar seus pares, sendo reconhecidos nesse submundo.
- **Aventura:** esses criminosos, em maioria, são dotados da necessidade de aventura e desafios, partindo, por exemplo, do grau de dificuldade de invadir determinado sistema, os alvos mais cobiçados são plataformas de governos e instituições de segurança mundial.

- **Maldade:** infelizmente o simples prazer de destruir faz parte do dia a dia desses criminosos, alguns deles têm o ego alto e para satisfazer esse ego cometem os crimes.

No Quadro 3, você verá os principais termos de crimes, ou ações que podem virar crime, que ocorrem na rede.

Quadro 3. Termos de crimes.

***Adware* (junção das palavras em inglês *advertisement*, "anúncio", e *software*, "programa")**	É projetado para apresentar propagandas, tem um formato de dar retorno financeiro para aqueles que desenvolvem software livre ou prestam programas gratuitos, seu mau uso pode vir a acontecer na forma de *spyware*, ou seja, que vire um espião para monitorar os hábitos dos usuários durante a execução ou navegação para direcionar as propagandas de determinados produtos ou serviços.
***Keylogger* (do inglês, "registrador do teclado")**	É um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente é ativado pós o uso por um usuário em um site de comércio eletrônico ou a internet banking, capturando assim as senhas.
***Phishing* (derivada da palavra em inglês *fishing*, que significa "pescaria")**	Trata-se de mensagens não solicitadas, passando-se por empresas conhecidas procurando induzir os usuários ao fornecimento de dados pessoais, de segurança ou financeiros. Podem ainda induzir os usuários a instalarem programas maliciosos para futuras invasões.
***Scam* ou "golpe"**	Termo usado para se referir a comunicações não solicitadas que são enviadas a um grande número de pessoas, aleatórias ou não, com objetivo de originar ganhos financeiros com ações ou delitos.
Vírus	Programa ou parte de programa perigoso ou malicioso que infecta programa ou arquivos em um computador, assim como em humanos ele pode ficar hospedado e um tempo depois ativar dando continuidade ao processo de infecção para destruir ou repassar dados a outros;
Vulnerabilidade	Pode caracterizar-se por falhas em projetos de implementação ou configuração de um sistema operacional, mesmo em sua criação, podendo, assim, originar violação da segurança nas estações de trabalho. Pode ser apresentada na forma de exploração (baseada no uso de ferramentas ou técnicas, com intuído de obter vantagens).
***Worm* (do inglês, "verme")**	É uma espécie de programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Ele se aproveita de vulnerabilidades de segurança ou falhas na configuração de softwares instalados para, posteriormente, ocasionar lesões.

Baseados nessas informações, cada vez mais as pessoas e as empresas têm que criar hábitos para melhorarem o aspecto segurança, criando padrões de proteção aos seus dados e visando à segurança de informações para garantir a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações que irão gerar conhecimento.

A informação é um ativo, sendo importante a qualquer organização e, hoje, até mesmo sendo considerado o ativo de maior importância e mais crítico. Lembre-se que se a informação for adulterada, ou não estar disponível para a tomada de decisão, pode influenciar muito os resultados da organização, gerando inclusive perdas financeiras.

Em um cenário pessimista esse tipo de crime pode levar a empresa a inviabilizar a continuidade de seus negócios se for negligenciada a segurança.

Saiba mais

Os possíveis tipos de *phishing* são (SEU MICRO SEGURO, 2016):

- ***Phishing* tradicional:** esse tipo de ataque é o mais simples na hora de analisá-lo tecnicamente; normalmente está vinculado à cópia de um site conhecido pela vítima no qual é alterado o endereço para onde irão os dados inseridos.
- ***Phishing* redirecionador:** assim como o caso anterior, essa técnica é utilizada em campanhas massivas, apesar do baixo percentual de vítimas, existe uma grande quantidade de usuários afetados e, consequentemente, credenciais comprometidas.
- ***Spear phishing*:** a principal diferença desse tipo é ser direcionado à poucas pessoas ou grupos reduzidos, dessa forma, as campanhas são muito mais personalizadas e com um percentual muito maior de vítimas.
- ***Smishing SMS*:** esse tipo de *phishing* está relacionado ao uso de outro canal digital como os telefones celulares. Normalmente, os cibercriminosos se passam por instituições conhecidas e enviam uma mensagem de texto alertando à vítima que ganhou um prêmio.
- ***Vishing*:** como citado anteriormente, existe o estabelecimento de falsos centros de atendimento telefônico que realizam ligações com o objetivo de cometer uma fraude, relacionando-as com casos de *vishing*. Esse ataque, muitas vezes, está relacionado a outro, de forma que se complementem para conseguir mais credibilidade e, dessa maneira, enganar à vítima de uma forma mais simples e eficaz.

Exercícios

1. As organizações vem se modernizando à medida que as Tecnologias da Informação (TI) sofrem constantes evoluções. Dificilmente, uma empresa moderna sobrevive no mercado sem utilizar recursos tecnológicos na execução de suas tarefas. Contudo, ao mesmo tempo em que ajudam a empresa na sua gestão, as TI podem ser utilizadas por pessoas interessadas em comprometer a segurança das informações organizacionais, tendo como objetivo final o ganho de benefícios indevidos. Em relação à segurança da informação, identifique a afirmação correta.

a) A segurança da informação direciona seus esforços para ataques realizados por cibercriminosos, uma vez que eles ocasionam maiores perdas financeiras.

b) A segurança da informação está diretamente relacionada com os riscos aos dados, aos sistemas de informação e às redes.

c) As novas tecnologias de proteção a dados são, na maioria dos casos, as culpadas por problemas de segurança da informação.

d) Ações reativas não necessitam ser especificadas em um plano de gestão de riscos de TI, pois as ações preventivas são capazes de abordar todos os possíveis problemas.

e) Considerando o baixo potencial de impacto dos atuais vírus de computador, a organização pode priorizar a proteção a outras formas de ataque.

2. A segurança da informação e a segurança de redes corporativas não estão relacionadas apenas ao uso de hardwares e softwares para prevenir ou reagir a incidentes. Na verdade, toda e qualquer defesa tecnológica é importante, mas a proteção aos dados e às operações das empresas requer uma abordagem mais ampla, envolvendo desde a implementação de procedimentos e políticas de uso dos recursos tecnológicos até a garantia do cumprimento de leis e regulamentações governamentais. Nesse contexto, analise as afirmações a seguir.

I. Os maiores riscos e, consequentemente, os maiores incidentes são causados pelos próprios funcionários das organizações.

II. As ameaças à segurança da informação acontecem tanto com o uso de alta tecnologia como pelos crimes tradicionais, como o roubo de um notebook da empresa, por exemplo.

III. É importante tratar a segurança da informação como uma função isolada na organização, pois assim ela será capaz de auxiliar no alcance dos objetivos estratégicos.

Está correto o que se afirma apenas em:

a) I e II.

b) I e III.

c) II e III.

d) I, II e III.

e) Nenhuma das afirmações.

3. A área de segurança da informação utiliza diversos termos técnicos que

devem ser bem compreendidos e diferenciados pelos gestores, especialmente aqueles cuja atuação está diretamente relacionada à proteção dos dados e redes da organização. Esse conhecimento é fundamental para que as ferramentas corretas sejam empregadas em cada situação que envolva a segurança da informação. Analise os termos apresentados a seguir e relacione-os corretamente a seus conceitos.

I. Risco.
II. Ameaça.
III. Contramedida.
IV. Exploração.

( ) Uso de alguma ferramenta ou técnica com o intuito de obter vantagem de uma vulnerabilidade.
( ) Recurso de segurança adotado para reduzir riscos.
( ) Probabilidade de uma ameaça explorar uma vulnerabilidade.
( ) Situação em que alguém ou algo pode causar danos a um ou vários ativos.

Identifique a alternativa que apresenta a relação correta entre os termos e seus respectivos conceitos.

a) II, I, III, IV.
b) III, II, I, IV.
c) III, IV, I, II.
d) IV, I, III, II.
e) IV, III, I, II.

4. Os sistemas de informação estão sujeitos a sofrer diversas ameaças, ocasionadas tanto por agentes internos (funcionários) como por agentes externos, os cibercriminosos, por exemplo. Normalmente, essas ameaças tentam se aproveitar de vulnerabilidades existentes no ambiente tecnológico da organização. Uma classificação comumente encontrada na área de segurança da informação para as ameaças é relacioná-las como intencional ou não intencional, sendo esta última ainda categorizada como erro humano, riscos ambientais ou falhas nos sistemas computadorizados. Analise as afirmações a seguir e identifique aquela que apresenta corretamente um exemplo real de ameaça intencional ou não intencional.

a) dados falsos são inseridos no computador do usuário para que ele seja obrigado a negar essa alteração de arquivos.
b) o usuário abre algum anexo de e-mail infectado com vírus, espalhando essa praga por toda a rede.
c) todos os computadores da empresa são automaticamente desligados por vírus.
d) um servidor ou site recebe um número de solicitações maior do que sua capacidade de resposta, fazendo com que ele falhe.
e) um usuário exclui, deliberadamente, registros de um sistema de informação para prejudicar a execução do serviço por outros usuários.

5. Empresas de monitoramento de redes relatam que o número de ataques vem crescendo nos últimos anos, ocasionando consideráveis prejuízos, especialmente financeiros. Normalmente, os ambientes das grandes empresas e dos governos são os que mais sofrem ataques. Como a variedade de ataques é grande, a tarefa de defender o ambiente virtual é muito complexa

e nem sempre consegue obter sucesso. Um ataque do tipo DoS (Denial of Service – Negação de Serviço) ocorre quando:

a) dados falsos são inseridos no computador do usuário para que ele seja obrigado a negar essa alteração de arquivos.

b) o usuário abre algum anexo de e-mail infectado com vírus, espalhando esta praga por toda a rede.

c) todos os computadores da empresa são automaticamente desligados por vírus.

d) um servidor ou site recebe um número de solicitações maior do que sua capacidade de resposta, fazendo com que ele falhe.

e) um usuário exclui, deliberadamente, registros de um Sistema de Informação (SI) para prejudicar a execução do serviço por outros usuários.

Referências

ALERTA SECURITY. *Entenda as diferenças entre segurança da informação e segurança em TI*. São Paulo, 2016a. Disponível em: <https://www.alertasecurity.com.br/blog/168-entenda-as--diferencas-entre-seguranca-da-informacao-e-seguranca-em-ti>. Acesso em: 13 ago. 2017.

ALERTA SECURITY. *Entenda o que é segurança da informação e reduza riscos na empresa*. São Paulo, 2016b. Disponível em: <https://www.alertasecurity.com.br/blog/117-entenda-o--que-e-seguranca-da-informacao-e-reduza-riscos-na-empresa>. Acesso em: 13 ago. 2017.

BEZERRA, F. *Ciclo PDCA*: conceito e aplicação (guia geral). [S.l.]: Portal Administração, 2013-2015. Disponível em: <http://www.portal-administracao.com/2014/08/ciclo--pdca-conceito-e-aplicacao.html>. Acesso em: 13 ago. 2017.

BRASIL. *Lei nº 9.609, de 19 de fevereiro de 1998*. Brasília, DF, 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 14 ago. 2017.

DEVMEDIA. *Segurança em bancos de dados*: aplicando normas e procedimentos - Revista SQL Magazine 103. Rio de Janeiro, c2017. Disponível em: <http://www.devmedia.com.br/seguranca-em-bancos-de-dados-aplicando-normas-e-procedimentos-revista--sql-magazine-103/25669>. Acesso em: 14 set. 2017.

ESTADÃO CONTEÚDO. *Pirataria e falsificação levaram a perdas de R$ 115,6 bilhões em 2015*. [S.l.]: Brasil Econômico, 2016. Disponível em: <http://economia.ig.com.br/2016-07-01/pirataria-contrabando-sonegacao-prejuizo-2015.html>. Acesso em: 14 ago. 2017.

SEU MICRO SEGURO. *Conheça os 5 tipos mais comuns de phishing*. [S.l.], 2016. Disponível em: <https://seumicroseguro.com/2016/12/06/conheca-os-5-tipos-mais-comuns-de--phishing/>. Acesso em: 13 ago. 2017.

TENCA. *Definição da segurança da informação*. [S.l.]: Segurança da Informação, 2009. Disponível em: <http://segtenca.blogspot.com.br/2009/08/definicao-da-seguranca--da-informacao.html>. Acesso em: 14 set. 2017.

Leituras recomendadas

BRASIL. Departamento de Polícia Rodoviária Federal. *Dia nacional de combate à pirataria*. Brasília, DF, c2017. Disponível em: <https://www.prf.gov.br/portal/noticias/nacionais/dia-nacional-de-combate-a-pirataria>. Acesso em: 13 ago. 2017.

CARNEIRO, A. *Auditoria e controle de sistemas de informação*. Rio de Janeiro: FCA, 2009.

LYRA, M. R. *Segurança e auditoria de sistema de informação*. Rio de Janeiro: Ciência Moderna, 2008.

NONATO, A. A. M. *Os crimes digitais em nosso cotidiano*. [S.l.]: Âmbito Jurídico, c1998-2017. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8890>. Acesso em: 13 ago. 2017.

SANTA CATARINA. Secretaria de Estado do Desenvolvimento Econômico Sustentável. Conselho Estadual de Combate à Pirataria. *Perdas com contrabando chegam a 115 bi, estima fórum antipirataria*. Florianópolis: CECOP, c2017. Disponível em: <http://www.sds.sc.gov.br/cecop/index.php/noticias/255-perdas-com-contrabando-chegam-a-115-bi-estima-forum-antipirataria>. Acesso em: 13 ago. 2017.

UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ. *Instalação de software pirata é crime!* Marabá: CTIC, 2016. Disponível em: <https://ctic.unifesspa.edu.br/index.php/ultimas-noticias/234-instalacao-de-software-pirata-e-crime>. Acesso em: 14 set. 2017.

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS